Timeline/Events

Contains events from EVTX and other sources when a timestamp is provided (NTDS/UAL). You will find the corresponding EVTX files in the results folder.

Time	Source	Headline	Eventdetails
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:24. datatable; belongs to row: DNT_Col 4025;ATT_USER_PRINCIPAL_NAME vkampmann@fuh.lab;RDN Verena Kampmann
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:24. datatable; belongs to row: DNT_Col 4026;ATT_USER_PRINCIPAL_NAME okampmann@fuh.lab;RDN Oliver Kampmann
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:24. datatable; belongs to row: DNT_Col 4023;ATT_USER_PRINCIPAL_NAME ;RDN DESKTOP-MK
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:25. datatable; belongs to row: DNT_Col 4030;ATT_USER_PRINCIPAL_NAME tkampmann@fuh.lab;RDN Tamara Kampmann
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:23. datatable; belongs to row: DNT_Col 4022;ATT_USER_PRINCIPAL_NAME nkampmann@fuh.lab;RDN Nadine Kampmann
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:25. datatable; belongs to row: DNT_Col 4032;ATT_USER_PRINCIPAL_NAME skampmann@fuh.lab;RDN Stefan Kampmann
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:25. datatable; belongs to row: DNT_Col 4031;ATT_USER_PRINCIPAL_NAME qkampmann@fuh.lab;RDN Quinn Kampmann
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:25. datatable; belongs to row: DNT_Col 4029;ATT_USER_PRINCIPAL_NAME ukampmann@fuh.lab;RDN Ulf Kampmann
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:24. datatable; belongs to row: DNT_Col 4027;ATT_USER_PRINCIPAL_NAME rkampmann@fuh.lab;RDN Rudolf Kampmann
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:25. datatable; belongs to row: DNT_Col 4028;ATT_USER_PRINCIPAL_NAME pkampmann@fuh.lab;RDN Peter Kampmann
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:23. datatable; belongs to row: DNT_Col 4014;ATT_USER_PRINCIPAL_NAME ;RDN DESKTOP-WK
0	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from ddMMyy HH:mm:ss (this row) to 17.05.22 14:10:11. datatable; belongs to row: DNT_Col 3831;ATT_USER_PRINCIPAL_NAME ;RDN DC01
3/21/2022 6:11:15 AM	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from 21.03.22 06:11:15 (this row) to 17.05.22 14:10:11. datatable; belongs to row: DNT_Col 4013;ATT_USER_PRINCIPAL_NAME wkampmann@fuh.lab;RDN Werner Kampmann

5/17/2022 11:11:30 AM	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from 17.05.22 11:11:30 (this row) to 17.05.22 14:10:09. datatable; belongs to row: DNT_Col 4021;ATT_USER_PRINCIPAL_NAME mkampmann@fuh.lab;RDN Mark Kampmann
5/17/2022 11:12:06 AM	NTDS.datatable	ATT_BAD_PASSWORD_TIME former timestamp	This attribute has been changed from 17.05.22 11:12:06 (this row) to 17.05.22 14:10:11. datatable; belongs to row: DNT_Col 3802;ATT_USER_PRINCIPAL_NAME ;RDN Administrator
5/17/2022 11:16:03 AM	NTDS.datatable	ATT_LAST_LOGON former timestamp	This attribute has been changed from 17.05.22 11:16:03 (this row) to 17.05.22 14:10:23. datatable; belongs to row: DNT_Col 4021;ATT_USER_PRINCIPAL_NAME mkampmann@fuh.lab;RDN Mark Kampmann
5/17/2022 2:07:58 PM	UAL	LastAccess former timestamp	This attribute has been changed from 17.05.22 14:07:58 (this row) to 17.05.22 14:10:25. UAL; belongs to Line 75;AuthenticatedUserName fuh\wkampmann
5/17/2022 2:08:54 PM	UAL	LastAccess former timestamp	This attribute has been changed from 17.05.22 14:08:54 (this row) to 17.05.22 14:11:11. UAL; belongs to Line 74;AuthenticatedUserName fuh\dc01$
5/17/2022 2:08:55 PM	UAL	LastAccess former timestamp	This attribute has been changed from 17.05.22 14:08:55 (this row) to 17.05.22 14:11:11. UAL; belongs to Line 76;AuthenticatedUserName fuh\dc01$
5/17/2022 2:09:00 PM	dcdiff	begin	The point of time you captured the base-state
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.

5/17/2022 2:09:00 PM	Microsoft-Windows-Ntfs/Operational	EventId: 9 NTFS scanned entire volume bitmap.	NTFS scanned entire volume bitmap. Volume correlation Id: {a894cd29-e2f5-45b9-a941-5a75e9e216fb} Volume name: C: Volume label: Device name: \Device\HarddiskVolume3 Device GUID: {7b6f1752-bd95-6e22-e3a5-6ee8419ecad7} Device manufacturer: Device model: VMware Virtual NVMe Disk Device revision: 1.0 Device serial number: VMWare NVME_0000 Bus type: NVMe Adapter serial number: VMWare NVME_0000 Duration (micro seconds): 11543 InputFlags: 0xA Reason: Reload requested because of an exception or configuration change Flags: 0x10
5/17/2022 2:09:00 PM	Microsoft-Windows-Ntfs/Operational	EventId: 10 NTFS cached runs statistics.	NTFS cached runs statistics. Volume correlation Id: {a894cd29-e2f5-45b9-a941-5a75e9e216fb} Volume name: C: Volume label: Device name: \Device\HarddiskVolume3 Device GUID: {7b6f1752-bd95-6e22-e3a5-6ee8419ecad7} Device manufacturer: Device model: VMware Virtual NVMe Disk Device revision: 1.0 Device serial number: VMWare NVME_0000 Bus type: NVMe Adapter serial number: VMWare NVME_0000 Media type: Hard disk Runs cached: 337 Longest run cached: 39.82 GB Most populated bin Count: 123 Most populated bin's minimum length: 16 KB Most populated bin's maximum length: 16 KB
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2051	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:00	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.

PM			
5/17/2022 2:09:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:04 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31EF06 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {3bd45df4-24b5-bd20-c5a0-2998bce061a4} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49865 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:04 PM	Security	EventId: 4769 A Kerberos service ticket was requested.	A Kerberos service ticket was requested. Account Information: Account Name: wkampmann@FUH.LAB Account Domain: FUH.LAB Logon GUID: {23a97c95-a8d8-9c50-197f-a014fb697d67} Service Information: Service Name: DC01$ Service ID: S-1-5-21-1691058862-2640770528-2028557413-1000 Network Information: Client Address: ::ffff:10.0.1.2 Client Port: 49867 Additional Information: Ticket Options: 0x40810000 Ticket Encryption Type: 0x12 Failure Code: 0x0 Transited Services: - This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed; which is often a different machine than the domain controller which issued the service ticket. Ticket options; encryption types; and failure codes are defined in RFC 4120.

5/17/2022 2:09:04 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31EF58 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49866 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:07 PM	Microsoft-Windows-Kernel-IO/Operational	EventId: 1 Windows has started processing the volume mount request.	Windows has started processing the volume mount request. Volume GUID: {00000000-0000-0000-0000-000000000000} Volume Name:
5/17/2022 2:09:07 PM	Microsoft-Windows-Kernel-IO/Operational	EventId: 2 The volume has been successfully mounted.	The volume has been successfully mounted. Volume GUID: {00000000-0000-0000-0000-000000000000} Volume Name:
5/17/2022 2:09:18 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F399 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49869 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:18 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F399 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:18 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F3AE Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49870 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:18 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F3AE Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:18 PM	Directory Service	EventId: 1220 LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate.	LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate. Additional Data Error value: 8009030e No credentials are available in the security package
5/17/2022 2:09:18 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:18 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: Administrator Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:18 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: FUH Logon ID: 0x2FA783 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:18 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F43E Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49873 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:18 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F43E Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:18	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account

PM			Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F455 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49874 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:18 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F455 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:18 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:18 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DC01$ Account Domain: Failure

			Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:18 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F4A6 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49876 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:18 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F4A6 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:18 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F4EF Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49877 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:18 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F4EF Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

5/17/2022 2:09:18 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:18 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: wkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:18 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F7C9 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49879 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:18 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F7C9 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:18 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F7E0 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49880 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:18 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F7E0 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:18 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:18 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-WK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F82A Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49882 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F82A Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F842 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49883 Detailed Authentication

			Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F842 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:19 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: mkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F88C Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49885 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F88C Logon Type: 3 This event is generated when a

			logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F8A3 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49886 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F8A3 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

		internet information server, are not affected by this.	
5/17/2022 2:09:19 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: nkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F8EF Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49888 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F8EF Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F910 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49889 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-

PM			2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F910 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:19 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-MK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F95C Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583}

			Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49891 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F95C Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F973 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49892 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F973 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:19 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: vkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information

			about this specific logon request. - 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.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F9BF Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49894 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F9BF Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31F9D7 Linked Logon ID: 0x0 Network Account Name: -

			Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49895 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31F9D7 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:19 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: okampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon

			Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31EF06 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FA28 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49897 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FA28 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FA3F Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49898 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:19 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FA3F Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon

			ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:19 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:19 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: rkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FA8B Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49900 Detailed Authentication Information: Logon Process: Kerberos

			Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FA8B Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FAA2 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49901 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FAA2 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:20 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: pkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FAEF Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49903 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FAEF Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FB06 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2

			Source Port: 49904 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FB06 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:20 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: ukampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was

			attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FB53 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49906 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FB53

			Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FB6A Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49907 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FB6A Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

		internet information server, are not affected by this.	
5/17/2022 2:09:20 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: tkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FBD8 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49909 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FBD8 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FBEF Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49910 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-

PM			2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FBEF Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:20 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: qkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FC3C Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583}

			Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49912 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FC3C Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FC53 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49913 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FC53 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:20 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: skampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information

			about this specific logon request. - 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.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FC9F Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49915 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FC9F Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FCB7 Linked Logon ID: 0x0 Network Account Name: -

			Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49916 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:20 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FCB7 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:20 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:20 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: Administrator Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon

			Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FD03 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49918 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FD03 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FD1A Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49919 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FD1A Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage

		default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:21 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DC01$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FD69 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49921 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FD69 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FD80 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49922 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FD80 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:21 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: wkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual

			Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FDCE Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49924 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FDCE Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FDE5 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49925 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FDE5 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:21 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-WK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2

			(interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FE33 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49927 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FE33 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account

PM			Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FE4A Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49928 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FE4A Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:21 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: mkampmann Account Domain:

			Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FE96 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49930 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FE96 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FEAD Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49931 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FEAD Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

5/17/2022 2:09:21 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:21 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: nkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FEFA Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49933 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:21 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FEFA Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:21 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FF11 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49934 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FF11 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:22 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:22 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-MK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FF5D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49936 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FF5D Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FF74 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49937 Detailed Authentication

			Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FF74 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:22 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:22 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: vkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FFC1 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49939 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FFC1 Logon Type: 3 This event is generated when a

			logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x31FFD8 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49940 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x31FFD8 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:22 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

		internet information server, are not affected by this.	
5/17/2022 2:09:22 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: okampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320025 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49942 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320025 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32003C Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49943 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-

PM			2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32003C Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:22 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:22 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: rkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320088 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583}

			Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49945 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320088 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32009F Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49946 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32009F Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:22 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:22 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: pkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information

			about this specific logon request. - 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.
5/17/2022 2:09:22 PM	Security	EventId: 4672 Special privileges assigned to new logon.	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: FUH Logon ID: 0x32011D Privileges: SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege SeEnableDelegationPrivilege
5/17/2022 2:09:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: FUH.LAB Logon ID: 0x32011D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {8a474796-ac6b-2925-e837-1675fb839b38} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: ::1 Source Port: 54235 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:22 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: FUH Logon ID: 0x32011D Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022	Security	EventId: 4624 An account	An account was successfully logged on. Subject:

2:09:34 PM		was successfully logged on.	Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3204F4 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49948 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:34 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3204F4 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:34 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32050B Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49949 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:34 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32050B Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:34 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:34 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: ukampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:34 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320558 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49951 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:34 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320558 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon

			ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:34 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32056F Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49952 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:34 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32056F Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:34 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

5/17/2022 2:09:34 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: tkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:34 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3205BB Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49954 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:34 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3205BB Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:34 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3205D2 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49955 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:34 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3205D2

			Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:34 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:34 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: qkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32061F Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation

			Name: - Source Network Address: 10.0.1.2 Source Port: 49957 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:35 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32061F Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320636 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49958 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:35 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320636 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:35 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: skampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320682 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49960 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:35 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320682 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320699 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583}

			Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49961 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:35 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320699 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:35 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: Administrator Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name

			(NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3206E6 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49963 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022	Security	EventId: 4634 An account	An account was logged off. Subject: Security

2:09:35 PM		was logged off.	ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3206E6 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3206FD Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49964 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:35 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3206FD Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

		server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	
5/17/2022 2:09:35 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DC01$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320749 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49966 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:35 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320749 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320761 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49967 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:35 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320761 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:35 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: wkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-

			2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3207AD Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49969 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:35 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3207AD Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3207C4 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49970 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:35 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3207C4 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:35 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:35 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-WK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The

			Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320811 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49972 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320811 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation

			Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320828 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49973 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320828 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:36 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: mkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process

			Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320876 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49975 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320876 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32088E Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49976 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32088E Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36	System	EventId: 36886 No suitable default server credential	No suitable default server credential exists on this system. This will prevent server

PM		exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:36 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: nkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3208DA Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49978 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3208DA Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3208F1 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49979 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3208F1 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:36 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-MK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.

5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32093F Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49981 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32093F Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320956 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49982 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320956 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:36 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: vkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3209A2 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49984 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3209A2 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon

			ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3209B9 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49985 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3209B9 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

5/17/2022 2:09:36 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: okampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320A06 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49987 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320A06 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320A1D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49988 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:36 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320A1D

			Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:36 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:36 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: rkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320A6A Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation

			Name: - Source Network Address: 10.0.1.2 Source Port: 49990 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320A6A Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320A81 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49991 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320A81 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:37 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: pkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320ACE Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49993 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320ACE Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320AE5 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583}

			Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49994 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320AE5 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:37 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: ukampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name

			(NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320B31 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49996 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022	Security	EventId: 4634 An account	An account was logged off. Subject: Security

2:09:37 PM		was logged off.	ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320B31 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320B48 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49997 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320B48 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

		server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	
5/17/2022 2:09:37 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: tkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320B95 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 49999 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320B95 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320BAC Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50000 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320BAC Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:37 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: qkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-

			2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320BF9 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50002 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320BF9 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320C10 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50003 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320C10 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:37 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: skampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The

			Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320C5C Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50005 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320C5C Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation

			Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320C74 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50006 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:37 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320C74 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:37 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:37 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: Administrator Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process

			Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320CC0 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50008 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320CC0 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320CD7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50009 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320CD7 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38	System	EventId: 36886 No suitable default server credential	No suitable default server credential exists on this system. This will prevent server

PM		exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:38 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DC01$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320D24 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50011 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320D24 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320D3B Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50012 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320D3B Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:38 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: wkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.

5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320D87 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50014 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320D87 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320D9E Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50015 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320D9E Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:38 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-WK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320DEB Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50017 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320DEB Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon

			ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320E02 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50018 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320E02 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

5/17/2022 2:09:38 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: mkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320E4E Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50020 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320E4E Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320E67 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50021 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:38 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320E67

			Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:38 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:38 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: nkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:50 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320F49 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation

			Name: - Source Network Address: 10.0.1.2 Source Port: 50023 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:50 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320F49 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:50 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320F60 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50024 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:50 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320F60 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:50 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:50 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-MK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320FAC Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50026 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320FAC Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x320FC3 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583}

			Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50027 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x320FC3 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:51 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: vkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name

			(NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x321011 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50029 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022	Security	EventId: 4634 An account	An account was logged off. Subject: Security

2:09:51 PM		was logged off.	ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x321011 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x321028 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50030 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x321028 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

		server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	
5/17/2022 2:09:51 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: okampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x321075 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50032 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x321075 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32108E Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50033 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32108E Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:51 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: rkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-

			2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3210DA Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50035 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3210DA Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3210F1 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50036 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3210F1 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:51 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: pkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The

			Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32113D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50038 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32113D Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation

			Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x321155 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50039 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x321155 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:51 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: ukampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process

			Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3211A1 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50041 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3211A1 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3211B8 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50042 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:51 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3211B8 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:51	System	EventId: 36886 No suitable default server credential	No suitable default server credential exists on this system. This will prevent server

PM		exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:51 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: tkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022	Microsoft-Windows-	EventId: 2049	dcdiff notice: no details in this event. examine

2:09:53 PM	SystemDataArchiver/Diagnostic		file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.

5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:53 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2049	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:54 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:54 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:54 PM	System	EventId: 7036 The Portable Device Enumerator Service service entered the stopped state.	The Portable Device Enumerator Service service entered the stopped state.
5/17/2022 2:09:54 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:54 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:54 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:09:54 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322541 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50044 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:54 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322541 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:54 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322558 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50045 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:54 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322558 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:54 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:54 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: qkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022	Security	EventId: 4624 An account	An account was successfully logged on. Subject:

2:09:54 PM		was successfully logged on.	Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3225AC Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50047 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:54 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3225AC Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:54 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3225C4 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50048 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:54 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3225C4 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:54 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:54 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: skampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:54 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322616 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50050 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:54 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322616 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon

			ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:54 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32262D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50051 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:54 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32262D Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:54 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

5/17/2022 2:09:54 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: Administrator Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:54 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32267D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50053 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:54 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32267D Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:54 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322694 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50054 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:54 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322694

			Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:54 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:54 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DC01$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:55 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3226E0 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation

			Name: - Source Network Address: 10.0.1.2 Source Port: 50056 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:55 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3226E0 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:55 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3226F8 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50057 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:55 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3226F8 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:55 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:55 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: wkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:55 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322749 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50059 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:55 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322749 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:55 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322760 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583}

			Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50060 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:55 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322760 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:55 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:55 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-WK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name

			(NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:55 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3227B1 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50062 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022	Security	EventId: 4634 An account	An account was logged off. Subject: Security

2:09:55 PM		was logged off.	ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3227B1 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:55 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3227C8 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50063 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:55 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3227C8 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:55 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

		server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	
5/17/2022 2:09:55 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: mkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:55 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322814 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50065 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:55 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322814 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:55 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32282C Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50066 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:55 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32282C Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:09:55 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:09:55 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: nkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:09:56 PM	Security	EventId: 4672 Special privileges assigned to new logon.	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: FUH Logon ID: 0x3228A3 Privileges: SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege

			SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege SeEnableDelegationPrivilege
5/17/2022 2:09:56 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Delegation New Logon: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: FUH.LAB Logon ID: 0x3228A3 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {8a474796-ac6b-2925-e837-1675fb839b38} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: fe80::ed56:d93c:daf8:fd1f Source Port: 54236 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:09:56 PM	DNS Server	EventId: 7648 The DNS server has detected that it is no longer the Key Master for zone fuh.lab. The Key Master role has been seized or transferred to dc01.fuh.lab.	The DNS server has detected that it is no longer the Key Master for zone fuh.lab. The Key Master role has been seized or transferred to dc01.fuh.lab.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022	Microsoft-Windows-	EventId: 2050	dcdiff notice: no details in this event. examine

2:10:00 PM	SystemDataArchiver/Diagnostic		file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2051	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050	dcdiff notice: no details in this event. examine file with eventviewer.
5/17/2022 2:10:00 PM	Microsoft-Windows-SystemDataArchiver/Diagnostic	EventId: 2050 Cannot retrieve event message text.	Cannot retrieve event message text.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322EAD Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50068 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322EAD Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322EC5 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50069 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322EC5 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:07 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:07 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-MK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID:

			S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322F11 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50071 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322F11 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322F28 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50072 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322F28 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:07 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:07 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: vkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and

			process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322F75 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50074 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322F75 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual

			Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322F8D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50075 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322F8D Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:07 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:07 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: okampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status:

			0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322FD9 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50077 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322FD9 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x322FF0 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50078 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x322FF0 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022	System	EventId: 36886 No suitable	No suitable default server credential exists on

2:10:07 PM		default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:07 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: rkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32303D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50080 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32303D Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:07 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323054 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50081 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:07 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323054 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:07 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:07 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: pkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.

5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3230A0 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50083 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3230A0 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3230B7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50084 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3230B7 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:08 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: ukampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323104 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50086 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323104 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon

			ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32311B Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50087 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32311B Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

5/17/2022 2:10:08 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: tkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323167 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50089 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323167 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32317E Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50090 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32317E

			Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:08 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: qkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3231CD Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation

			Name: - Source Network Address: 10.0.1.2 Source Port: 50092 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3231CD Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3231E4 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50093 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3231E4 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:08 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: skampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323231 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50095 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323231 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323248 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583}

			Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50096 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323248 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:08 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: Administrator Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name

			(NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323297 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50098 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022	Security	EventId: 4634 An account	An account was logged off. Subject: Security

2:10:08 PM		was logged off.	ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323297 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3232AE Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50099 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:08 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3232AE Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:08 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

		server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	
5/17/2022 2:10:08 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DC01$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3232FA Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50101 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3232FA Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323312 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50102 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323312 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:09 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: wkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-

			2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323361 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50104 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323361 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323378 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50105 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323378 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:09 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-WK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The

			Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3233C5 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50107 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3233C5 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation

			Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3233DC Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50108 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from 17.05.22 11:11:30 to 17.05.22 14:10:09 (this row). datatable; belongs to row: DNT_Col 4021;ATT_USER_PRINCIPAL_NAME mkampmann@fuh.lab;RDN Mark Kampmann
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3233DC Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:09	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain:

PM			- Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: mkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32342B Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50110 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32342B Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323447 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50111 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323447 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively

			correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:09 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: nkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323494 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50113 Detailed Authentication

			Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323494 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3234AB Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50114 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:09 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3234AB Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:09 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:09 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-MK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:09 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3234FF Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50116 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3234FF Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323517 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation

			Name: - Source Network Address: 10.0.1.2 Source Port: 50117 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323517 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:10 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: vkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is

			generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323564 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50119 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann

			Account Domain: FUH Logon ID: 0x323564 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32357B Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50120 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32357B Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).

		credentials, such as the internet information server, are not affected by this.	
5/17/2022 2:10:10 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: okampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3235C8 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50122 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3235C8 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3235DF Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50123 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022	Security	EventId: 4634 An account	An account was logged off. Subject: Security

2:10:10 PM		was logged off.	ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3235DF Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:10 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: rkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32362B Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID:

			{a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50125 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32362B Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323642 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50126 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323642 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:10 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: pkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication

			information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32368F Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50128 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32368F Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3236A6

			Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50129 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3236A6 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:10 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: ukampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872

			Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3236F6 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50131 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3236F6 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32370D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50132 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:10 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32370D Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:10 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage

		default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:10 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: tkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:11 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32375B Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50134 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32375B Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323772 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50135 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323772 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:11 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: qkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:11 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual

			Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3237BF Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50137 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3237BF Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3237D6 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50138 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3237D6 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:11 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: skampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2

			(interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:11 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323824 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50140 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323824 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account

PM			Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x32383B Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50141 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x32383B Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:11 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from 17.05.22 11:12:06 to 17.05.22 14:10:11 (this row). datatable; belongs to row: DNT_Col 3802;ATT_USER_PRINCIPAL_NAME ;RDN Administrator

5/17/2022 2:10:11 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: Administrator Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:11 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323888 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50143 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323888 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3238A0 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50144 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:11 (this row). datatable; belongs to row: DNT_Col 3831;ATT_USER_PRINCIPAL_NAME ;RDN DC01

5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3238A0 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:11 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DC01$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:11 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x3238EC Linked Logon ID: 0x0 Network Account Name: -

			Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50146 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x3238EC Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323903 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50147 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:11 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323903 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:11 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from 21.03.22 06:11:15 to 17.05.22 14:10:11 (this row). datatable; belongs to row: DNT_Col 4013;ATT_USER_PRINCIPAL_NAME wkampmann@fuh.lab;RDN Werner Kampmann
5/17/2022 2:10:11 PM	System	EventId: 36886 No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.	No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials; such as the internet information server; are not affected by this. The SSPI client process is lsass (PID: 700).
5/17/2022 2:10:11 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: wkampmann Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2

			(interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:22 PM	Security	EventId: 4672 Special privileges assigned to new logon.	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: FUH Logon ID: 0x323BC9 Privileges: SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege SeEnableDelegationPrivilege
5/17/2022 2:10:22 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: DC01$ Account Domain: FUH.LAB Logon ID: 0x323BC9 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {8a474796-ac6b-2925-e837-1675fb839b38} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: ::1 Source Port: 54237 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:22	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-18 Account Name: DC01$ Account

PM			Domain: FUH Logon ID: 0x323BC9 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:23 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323D26 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50149 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:23 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323D26 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:23 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323D3D Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583}

			Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50150 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:23 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323D3D Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:23 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:23 (this row). datatable; belongs to row: DNT_Col 4014;ATT_USER_PRINCIPAL_NAME ;RDN DESKTOP-WK
5/17/2022 2:10:23 PM	Security	EventId: 4625 An account failed to log on.	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: DESKTOP-WK$ Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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 was requested. The most common types are 2

			(interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - 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.
5/17/2022 2:10:23 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323D8A Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50152 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:23 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323D8A Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:23	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account

PM			Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323DA1 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50153 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:23 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323DA1 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:23 PM	NTDS.datatable	ATT_LAST_LOGON new timestamp	This attribute has been changed from 17.05.22 11:16:03 to 17.05.22 14:10:23 (this row). datatable; belongs to row: DNT_Col 4021;ATT_USER_PRINCIPAL_NAME mkampmann@fuh.lab;RDN Mark Kampmann
5/17/2022 2:10:23 PM	Security	EventId: 4776 The computer attempted to validate the credentials for an account.	The computer attempted to validate the credentials for an account. Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon Account: mkampmann Source Workstation: DESKTOP-WK Error Code: 0x0
5/17/2022 2:10:23 PM	Security	EventId: 4672 Special privileges assigned to new logon.	Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1105 Account Name: mkampmann Account Domain: FUH Logon ID: 0x323DE5 Privileges: SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege

			SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege SeEnableDelegationPrivilege
5/17/2022 2:10:23 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1105 Account Name: mkampmann Account Domain: FUH Logon ID: 0x323DE5 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: DESKTOP-WK Source Network Address: 10.0.1.2 Source Port: 49872 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V2 Key Length: 128 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.
5/17/2022 2:10:23 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323E1A Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50155 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:23 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323E1A Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:23 PM	Security	EventId: 4624 An account was successfully logged on.	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH.LAB Logon ID: 0x323E31 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {a8daaafc-ceac-c5db-2cf4-2bdc2ee90583} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: 10.0.1.2 Source Port: 50156 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos 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.
5/17/2022 2:10:23 PM	Security	EventId: 4634 An account was logged off.	An account was logged off. Subject: Security ID: S-1-5-21-1691058862-2640770528-2028557413-1103 Account Name: wkampmann Account Domain: FUH Logon ID: 0x323E31 Logon Type: 3 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
5/17/2022 2:10:23 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:23 (this row). datatable; belongs to row: DNT_Col 4022;ATT_USER_PRINCIPAL_NAME nkampmann@fuh.lab;RDN Nadine Kampmann
5/17/2022 2:10:24 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:24 (this row). datatable; belongs to row: DNT_Col 4023;ATT_USER_PRINCIPAL_NAME ;RDN DESKTOP-MK
5/17/2022 2:10:24 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:24 (this row). datatable; belongs to row: DNT_Col 4025;ATT_USER_PRINCIPAL_NAME vkampmann@fuh.lab;RDN Verena Kampmann
5/17/2022 2:10:24 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:24 (this row). datatable; belongs to row: DNT_Col 4026;ATT_USER_PRINCIPAL_NAME okampmann@fuh.lab;RDN Oliver Kampmann
5/17/2022 2:10:24 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:24 (this row). datatable; belongs to row: DNT_Col 4027;ATT_USER_PRINCIPAL_NAME rkampmann@fuh.lab;RDN Rudolf Kampmann
5/17/2022 2:10:25 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:25 (this row). datatable; belongs to row: DNT_Col 4028;ATT_USER_PRINCIPAL_NAME pkampmann@fuh.lab;RDN Peter Kampmann
5/17/2022 2:10:25 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:25 (this row). datatable; belongs to row: DNT_Col 4029;ATT_USER_PRINCIPAL_NAME ukampmann@fuh.lab;RDN Ulf Kampmann
5/17/2022 2:10:25 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:25 (this row). datatable; belongs to row: DNT_Col 4030;ATT_USER_PRINCIPAL_NAME tkampmann@fuh.lab;RDN Tamara Kampmann
5/17/2022 2:10:25 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:25 (this row). datatable; belongs to row: DNT_Col 4031;ATT_USER_PRINCIPAL_NAME qkampmann@fuh.lab;RDN Quinn Kampmann
5/17/2022 2:10:25 PM	NTDS.datatable	ATT_BAD_PASSWORD_TIME new timestamp	This attribute has been changed from ddMMyy HH:mm:ss to 17.05.22 14:10:25 (this row). datatable; belongs to row: DNT_Col 4032;ATT_USER_PRINCIPAL_NAME skampmann@fuh.lab;RDN Stefan Kampmann
5/17/2022 2:10:25 PM	UAL	LastAccess new timestamp	This attribute has been changed from 17.05.22 14:07:58 to 17.05.22 14:10:25 (this row). UAL; belongs to Line 75;AuthenticatedUserName fuh\wkampmann
5/17/2022 2:10:36	dcdiff	end	The point of time you captured the final-state

PM			
5/17/2022 2:11:11 PM	UAL	LastAccess new timestamp	This attribute has been changed from 17.05.22 14:08:55 to 17.05.22 14:11:11 (this row). UAL; belongs to Line 76;AuthenticatedUserName fuh\dc01$
5/17/2022 2:11:11 PM	UAL	LastAccess new timestamp	This attribute has been changed from 17.05.22 14:08:54 to 17.05.22 14:11:11 (this row). UAL; belongs to Line 74;AuthenticatedUserName fuh\dc01$