RDP Successful Logon

Event ID 1149
Type 10, 7 for Reconnect
"User authentication succeeded"
Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx

Event ID 4624
"An account was successfully logged on"
Security.evtx

Event ID 21
"Remote Desktop Services: Session logon succeeded:"
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

Event ID 22
"Remote Desktop Services: Shell start notification received:"
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

Network Connection  Authentication  Logon

youtube.com/13cubed
RDP Unsuccessful Logon

Event ID 1149

"User authentication succeeded"
Microsoft-Windows-TerminalServices-RemoteConnectionManager%40Operational.evtx

Network Connection

Event ID 4625
Type 10, 7 for Reconnect

"An account failed to log on"
Security.evtx

Authentication
RDP Session Disconnect
(Window Close)

Event ID 24

"Remote Desktop Services: Session has been disconnected:"
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

Event ID 40

"Session <X> has been disconnected, reason code <Z>"
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

Event ID 4779

"A session was disconnected from a Window Station"
Security.evtx

Event ID 4634
Type 10, 7 for Reconnect

"An account was logged off"
Security.evtx

Session Disconnect / Reconnect


youtube.com/13cubed
RDP Session Disconnect
(Purposeful Disconnect via Start > Disconnect)

Event ID 24
“Remote Desktop Services: Session has been disconnected.”
Microsoft-Windows-TerminalServices-LocalSessionManager%40operational.evtx

Event ID 39
“Session <X> has been disconnected by session <Y>.”
Microsoft-Windows-TerminalServices-LocalSessionManager%40operational.evtx

Event ID 40
“Session <X> has been disconnected, reason code <Z>.”
Microsoft-Windows-TerminalServices-LocalSessionManager%40operational.evtx

Event ID 4779
“A session was disconnected from a Window Station”
Security.evtx

Event ID 4634
Type 10, 7 for Reconnect
“An account was logged off”
Security.evtx

Session Disconnect / Reconnect

youtube.com/13cubed
RDP Session Reconnect

Event ID 1149
"User authentication succeeded"
Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx

Event ID 4624 Type 7
"An account was successfully logged on"
Security.evtx

Event ID 25
"Remote Desktop Services: Session reconnection succeeded."
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

Event ID 40*
"Session <X> has been disconnected, reason code <Z>"
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
*Events also indicate/correlate to reconnections

Event ID 4778
"A session was reconnected to a Window Station"
Security.evtx

Network Connection  Authentication  Session Disconnect / Reconnect


youtube.com/13cubed
RDP Session Logoff

Event ID 23

Event ID 4634
Type 16, 7 for Reconnect

Event ID 4647

Event ID 9009

“Remote Desktop Services: Session logoff succeeded.”
Microsoft-Windows-TerminalServices-LocalSessionManager%40Operational.evtx

“An account was logged off”
Security.evtx

“User initiated logoff.”
Security.evtx

“The Desktop Window Manager has exited with code (<X>).”
System.evtx

youtube.com/13cubed