LOGON TYPE CODES

Cheat Sheet

Type 2

Interactive

A logon at the console of a computer, whether with a domain account or a local account from the computer's local SAM. To tell the difference, look for the domain or computer name preceding the user name in the event's description.

Type 3

Network

When accessing a computer from elsewhere on the network. Most commonly connections to shared folders or printers, and other over-the-network logons.

Type 4

Batch

Logon sessions created by Windows when it executes a scheduled task to run it under the authority of the specified user account. Other job scheduling systems may also generate type 4 logon events when starting jobs.

Type 5

Service

Similar to scheduled tasks, each service is configured to run as a specified user account. When a service starts, Windows first creates a logon session which results in a type 5 logon event.

Type 7

Unlock

When a user returns to their workstation and attempts to unlock the console from the password protected screen saver mode, Windows treats this as a logon and logs the event as type 7.

Type 8

NetworkCleartext

Indicates a network logon, like logon type 3, but where the password was sent over the network as clear text. Windows server doesn't allow connection to shared file or printers with clear text authentication. These logons can happen from within an ASP script using the ADVAPI or when a user logs on to IIS using IIS's basic authentication mode. In both cases the logon process in the event's description will list advapi.

Type 9

NewCredentials

If you use the RunAs command to start a program under a different user account and specify the /netonly switch, Windows records a logon/logoff event with logon type 9.

Type 10

RemoteInteractive

When you access a computer through Terminal Services, Remote Desktop or Remote Assistance, Windows logs the logon attempt with logon type 10. (Prior to XP, Windows 2000 doesn't use logon type 10 and Terminal Services logons are reported as logon type 2.)

Type 11

CachedInteractive

Cached logons facilitate mobile users. Windows caches a hash of the last 10 interactive domain logon credentials . Later, when you are not connected to your organization's network and attempt to logon to your laptop with a domain account and there's no domain controller available for verification, Windows uses these hashes to verify your identity.

TechGenix

LOGON TYPE CODES

Cheat Sheet

Type 2

Interactive

A logon at the console of a computer, whether with a domain account or a local account from the computer’s local SAM. To tell the difference, look for the domain or computer name preceding the user name in the event’s description.

Type 3

Network

When accessing a computer from elsewhere on the network. Most commonly connections to shared folders or printers, and other over-the-network logons.

Type 4

Batch

Logon sessions created by Windows when it executes a scheduled task to run it under the authority of the specified user account. Other job scheduling systems may also generate type 4 logon events when starting jobs.

Type 5

Service

Similar to scheduled tasks, each service is configured to run as a specified user account. When a service starts, Windows first creates a logon session which results in a type 5 logon event.

Type 7

Unlock

When a user returns to their workstation and attempts to unlock the console from the password protected screen saver mode, Windows treats this as a logon and logs the event as type 7.

Type 8

NetworkCleartext

Indicates a network logon, like logon type 3, but where the password was sent over the network as clear text. Windows server doesn’t allow connection to shared file or printers with clear text authentication. These logons can happen from within an ASP script using the ADVAPI or when a user logs on to IIS using IIS’s basic authentication mode. In both cases the logon process in the event’s description will list advapi.

Type 9

NewCredentials

If you use the RunAs command to start a program under a different user account and specify the /netonly switch, Windows records a logon/logoff event with logon type 9.

Type 10

RemoteInteractive

When you access a computer through Terminal Services, Remote Desktop or Remote Assistance, Windows logs the logon attempt with logon type 10. (Prior to XP, Windows 2000 doesn’t use logon type 10 and Terminal Services logons are reported as logon type 2.)

Type 11

CachedInteractive

Cached logons facilitate mobile users. Windows caches a hash of the last 10 interactive domain logon credentials . Later, when you are not connected to your organization’s network and attempt to logon to your laptop with a domain account and there’s no domain controller available for verification, Windows uses these hashes to verify your identity.

[print version]

TechGenix