Administrative tools and logon types

Article • 08/15/2022 • 3 minutes to read

This reference information is provided to help identify the risk of credential exposure associated with different administrative tools for remote administration.

In a remote administration scenario, credentials are always exposed on the source computer so a trustworthy privileged access workstation (PAW) is always recommended for sensitive or high impact accounts. Whether credentials are exposed to potential theft on the target (remote) computer depends primarily on the windows logon type used by the connection method.

This table includes guidance for the most common administrative tools and connection methods:

Connection method	**Logon type**	**Reusable credentials on destination**	**Comments**
Log on at console	Interactive	v	Includes hardware remote access / lights-out cards and network KVMs.
RUNAS	Interactive	v	
RUNAS /NETWORK	NewCredentials	v	Clones current LSA session for local access, but uses new credentials when connecting to network resources.
Remote Desktop (success)	RemoteInteractive	v	If the remote desktop client is configured to share local devices and resources, those may be compromised as well.
Remote Desktop (failure - logon type was denied)	RemoteInteractive	-	By default, if RDP logon fails credentials are only stored briefly. This may not be the case if the computer is compromised.
Net use * \\SERVER	Network	-	
Net use * \\SERVER /u:user	Network	-	
MMC snap-ins to remote computer	Network	-	Example: Computer Management, Event Viewer, Device Manager, Services

Connection method	Logon type	Reusable credentials on destination	Comments
PowerShell WinRM	Network	-	Example: Enter-PSSession server
PowerShell WinRM with CredSSP	NetworkClearText	v	New-PSSession server -Authentication Credssp -Credential cred
PsExec without explicit creds	Network	-	Example: PsExec \\server cmd
PsExec with explicit creds	Network + Interactive	v	PsExec \\server -u user -p pwd cmd Creates multiple logon sessions.
Remote Registry	Network	-	
Remote Desktop Gateway	Network	-	Authenticating to Remote Desktop Gateway.
Scheduled task	Batch	v	Password will also be saved as LSA secret on disk.
Run tools as a service	Service	v	Password will also be saved as LSA secret on disk.
Vulnerability scanners	Network	-	Most scanners default to using network logons, though some vendors may implement non-network logons and introduce more credential theft risk.

For web authentication, use the reference from the table below:

Connection method	Logon type	Reusable credentials on destination	Comments
IIS "Basic Authentication"	NetworkCleartext (IIS 6.0+) Interactive (prior to IIS 6.0)	v	
IIS "Integrated Windows Authentication"	Network	-	NTLM and Kerberos Providers.

Column Definitions:

- **Logon type** - Identifies the logon type initiated by the connection.
- **Reusable credentials on destination** - Indicates that the following credential types will be stored in LSASS process memory on the destination computer where the specified account is logged on locally:
  - LM and NT hashes
  - Kerberos TGTs
  - Plaintext password (if applicable).

The symbols in this table defined as follows:

- (-) denotes when credentials are not exposed.
- (v) denotes when credentials are exposed.

For management applications that are not in this table, you can determine the logon type from the logon type field in the audit logon events. For more information, see Audit logon events.

In Windows-based computers, all authentications are processed as one of several logon types, regardless of which authentication protocol or authenticator is used. This table includes most common logon types and their attributes relative to credential theft:

Logon type	#	Authenticators accepted	Reusable credentials in LSA session	Examples

Interactive (also known as, Logon locally)	2	Password, Smartcard, other	Yes	Console logon;
				RUNAS;
				Hardware remote control solutions (such as Network KVM or Remote Access / Lights-Out Card in server)
				IIS Basic Auth (before IIS 6.0)

Network	3	Password, NT Hash, Kerberos ticket	No (except if delegation is enabled, then Kerberos tickets present)	NET USE;
				RPC calls;
				Remote registry;
				IIS integrated Windows auth;
				SQL Windows auth;

Batch	4	Password (stored as LSA secret)	Yes	Scheduled tasks
Service	5	Password (stored as LSA secret)	Yes	Windows services

Logon type	#	Authenticators accepted	Reusable credentials in LSA session	Examples
NetworkCleartext	8	Password	Yes	IIS Basic Auth (IIS 6.0 and newer); Windows PowerShell with CredSSP
NewCredentials	9	Password	Yes	RUNAS /NETWORK
RemoteInteractive	10	Password, Smartcard, other	Yes	Remote Desktop (formerly known as "Terminal Services")

Column definitions:

- **Logon type** - The type of logon requested.
- **#** - The numeric identifier for the logon type that is reported in audit events in the Security event log.
- **Authenticators accepted** - Indicates which types of authenticators are able to initiate a logon of this type.
- **Reusable credentials in LSA session** - Indicates whether the logon type results in the LSA session holding credentials, such as plaintext passwords, NT hashes, or Kerberos tickets that could be used to authenticate to other network resources.
- **Examples** - List of common scenarios in which the logon type is used.

ⓘ Note

For more information about Logon Types, see **SECURITY_LOGON_TYPE enumeration**.

Next steps

AD DS Design and Planning