Computer Credential

CET 05202: SERVER ADMINISTRATION

UNIT IV

Ms Jamila L.

Contents

Types of computer credentials:

- User logon
- Application logon
- Network credential

Computer Credential

The credentials used in authentication are digital documents that associate the user's identity to some form of proof of authenticity, such as a

- ✓certificate,
- ✓a password, or
- ✓a PIN.

Computer Logon

Logon is a process of gaining access to local or remote systems using valid credentials. Or

A logon is an event in Windows that shows a user account being granted some access to a workstation/server/computer.

- The user information is validated by **Local Security Authority (LSA),**
- incase of local account it will verify the information from **Security Accounts Manager (SAM)** database and
- incase of domain account it will verify the information from the **Domain Controller.**

The Local Security Authority (LSA)

As per Microsoft docs "The Local Security Authority (LSA) is a protected system process that authenticates and logs users on to the local computer.

- LSA maintains information about all aspects of local security on a computer (these aspects are collectively known as the local security policy), and it provides various services for translation between names and security identifiers (SIDs)."

Logon vs. authentication

A Windows logon occurs on the workstation a user is attempting to access.

However, Windows authentication is performed by the computer where the user account is stored.

Authentication is the process of identifying users that request access to a system, network, or device. Access control often determines user identity according to credentials like username and password.

In Windows-based computers, all authentications are processed as one of the logon types below:

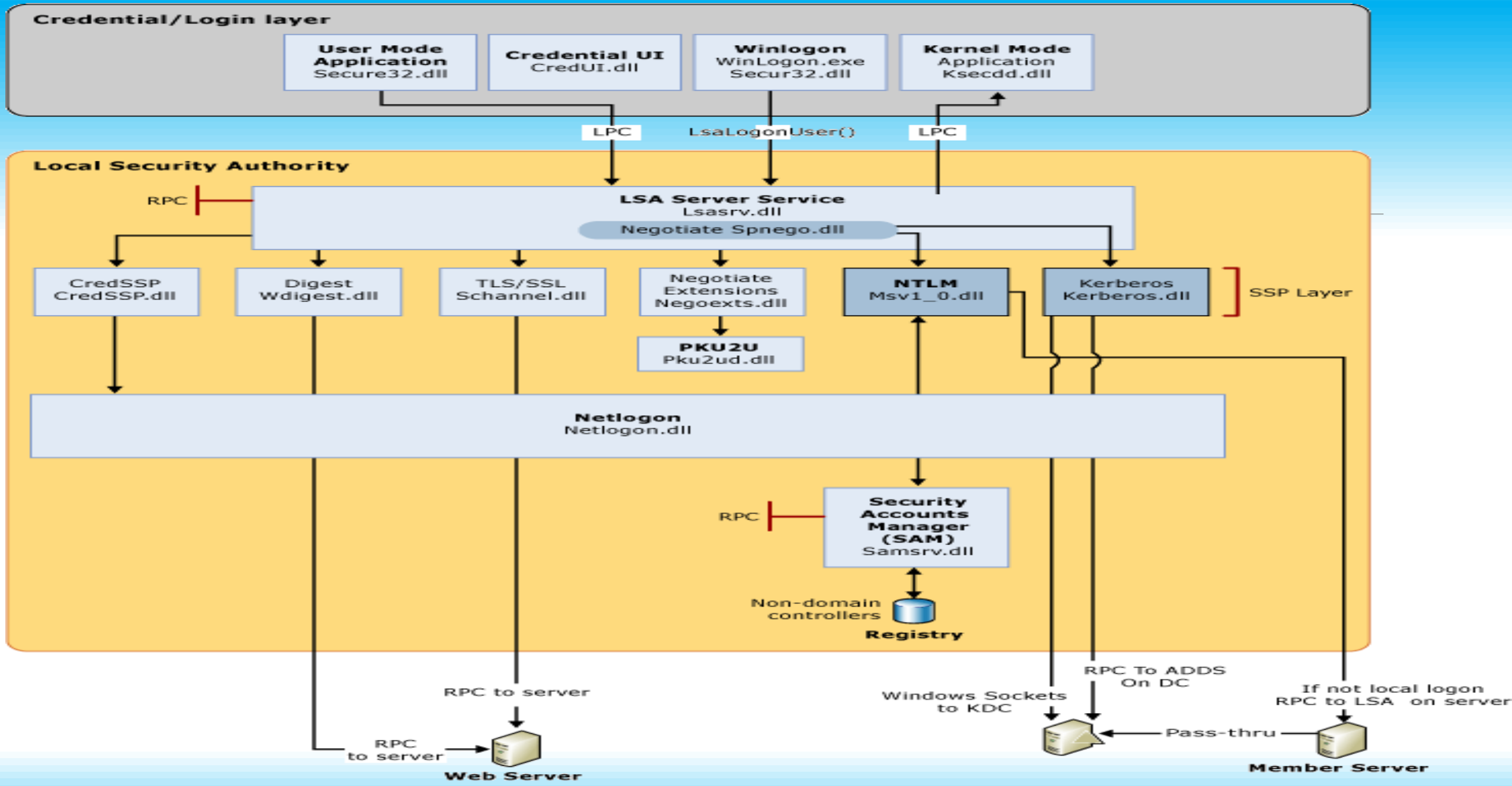
1. Interactive logons with local or domain accounts

This is true regardless of which authentication protocol or authenticator is used.

Interactive logons with local or domain accounts

An interactive logon is a logon whereby a user uses a local keyboard and mouse to enter credentials in the logon screen in Windows.

- They can log on with a local account against a local SAM (Security Accounts Manager) account database using the computer name in the 'domain' field.
- Users can log on with a domain account by either choosing the Active Directory domain in the domain field or typing in their User Principal Name (UPN) in the username field.
- Smart cards and biometric devices can also be used as authentication methods to log in interactively.


Credential/Login layer
User Mode Application
Secure32.dll
Credential UI
CredUI.dll
Winlogon
WinLogon.exe
Secur32.dll
Kernel Mode
Application
Ksecdd.dll
LPC
LsaLogonUser()
LPC
Local Security Authority
RPC
LSA Server Service
Lsasrv.dll
Negotiate Spnego.dll
CredSSP
CredSSP.dll
Digest
Wdigest.dll
TLS/SSL
Schannel.dll
Negotiate Extensions
Negoexts.dll
NTLM
Msv1_0.dll
Kerberos
Kerberos.dll
SSP Layer
PKU2U
Pku2ud.dll
Netlogon
Netlogon.dll
RPC
Security Accounts Manager (SAM)
Samsrv.dll
Non-domain controllers
Registry
RPC to server
RPC to server
Web Server
Windows Sockets to KDC
RPC To ADDS On DC
Pass-thru
If not local logon RPC to LSA on server
Member Server

Remote interactive logons

When you initiate a Remote Desktop Protocol (RDP) session to another workstation or server, this is a remote interactive login.

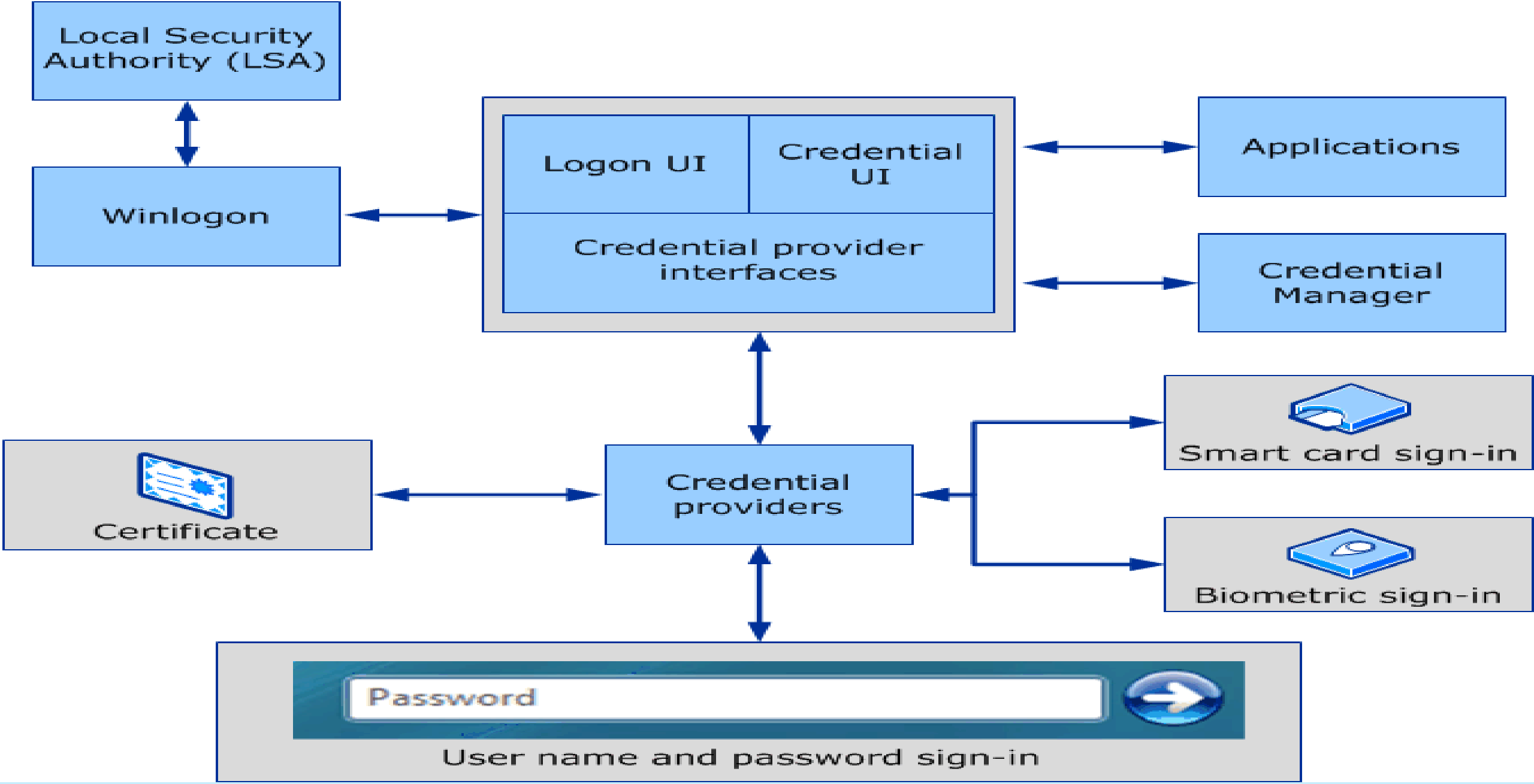
- You are logging in interactively with the remote machine, but you are doing it remotely.
- It is NOT the computer you are using to start that connection.
- This distinction is relatively simple on paper, but there are many nuances in how they are reported, logged in various security event logs, and how they can be exploited or compromised without your knowledge.

Network logons

A network logon is when a user logs on to a machine over the network.

This is commonly for accessing shared network resources.

For example, accessing a shared folder, connecting to a machine via WinRM **(Windows Remote Management protocol),** or a printer.


Local Security Authority (LSA)
Winlogon
Logon UI
Credential UI
Credential provider interfaces
Applications
Credential Manager
Credential providers
Certificate
Smart card sign-in
Biometric sign-in
Password
User name and password sign-in

Enabling logon events on Windows

By default, domain controllers will generate a logon event when a domain computer is logged onto.

However, there are more robust events that can be logged:

- Audit account logon events and Audit Logon events.
- You can accomplish this on your domain via Group Policy or on a specific member server or workstation via their respective local security policy.

Enabling logon events on Windows cont...

Domain Environment:

1) Login to Domain Controller

2) Open Group Policy Management Console

3) Expand the Domain Object

4) Expand the Group Policy Objects

5) Right click on the Default Domain Policy and click on Edit (The policy that is applied to all the domain computers. It may differ in your environment)

6) Follow the below path to enable Audit Logon events.

Computer Configuration --> Windows Settings --> Security Settings --> Advanced Audit Policy Configuration --> Audit Policies --> Logon/Logoff --> Audit Logon

7) Select "Configure the following audit events:", "Success" & "Failure" Checkbox

Enabling logon events on Windows cont...

Local Machine:

1) Open Local Group Policy Editor

2) Follow the below path to enable Audit Logon events.

Computer Configuration --> Windows Settings --> Security Settings --> Advanced Audit Policy Configuration --> System Audit Policies - Local Group Policy Object --> Logon/Logoff --> Audit Logon

3) Select "Configure the following audit events:", "Success" & "Failure" Checkbox

Windows logon types

Logon types

Type 0: Used by system

It is used by the system at the time of system start up.

Logon Type 2 : Interactive

This type of logon is generated when a user logs on to the console of a machine.

Once we logon to the machine using Console, we can see in the *Event viewer* that the Logon Type 2 event gets generated.

Authenticators accepted:

You can use the keyboard and mouse, smart cards, and biometric devices. There are new device types introduced in recent years including FIDO2-compatible security devices (Yubikey, etc.).

Logon type 2: Interactive logon cont…



Logon type 3: Network logon

This logon type describes a computer being accessed across the network (LAN/WAN). This is typically used to access file servers, printers, and other network devices.

Authenticators accepted

You can use a keyboard and mouse (password), a Kerberos ticket, and NT hashes are all accepted authenticators for this type of logon.

Examples

A network logon gives the user permission (via token) to access said resources. Local authentication does need to be completed first.

Logon type 4: Batch logon

This logon type typically relates to **scheduled tasks**. Logon type 4 events are usually rather benign, however, a malicious user could try to guess the password of an account here.

Authenticators accepted

A password is the only accepted authenticator as it is local.

Examples

When Windows executes a scheduled task, the service creates a new logon session for the task so that it has the necessary permissions to complete it.

Logon type 5: Service logon:

The next type is called the service logon. When Windows starts a service that is configured to log on as a user, Windows creates a new logon session. Each service is configured to run as a specified user account.

Authenticators accepted

Like batch logons, the service logon type only accepts a password that's usually stored as an LSA secret.

Examples

When setting up a local Apache Tomcat server to host a website, you could configure the Tomcat service to log on as the Administrator (not a good idea), or preferably a domain service account with a very strong password.

Logon type 7: Unlock:

When a user leaves a workstation for a period of time, Windows will lock the computer. This is to protect the workstation, its data, and other potential remote network data from attackers or local hackers. When a user unlocks the computer, this logon type is logged in the local Security event log.

Authenticators accepted

Again, only a password is accepted for this logon type.

Examples

As stated above, after returning to a computer that has been locked by policy, unlocking the computer, by re-entering the password, describes this event.

Logon type 8: Network clear text logon:

This type is similar to a network logon (Type 3), but here the password was sent over the network in cleartext.

The password was passed to the authentication system on the remote system in its unhashed form. Windows always hashes passwords typed in before transmitting them over the LAN.

Authenticators accepted

You guessed it…passwords.

Examples

The only traditional example of this was IIS (**Internet Information Services**) anonymous logins, but even those have become scarce due to the ever-increasing security landscape we live in today.

Logon Type 9: New credentials-based logon:

This logon type describes using RunAs to start a program under a different account than the logged-in account. You use the /netonly switch in Windows to accomplish this.

Authenticators accepted

Only passwords are accepted as authenticators for this logon type.

Examples

When you want to open **Computer Management** as a different domain administrator, you can hold Shift down while you right-click the tool in Administrative Tools, then click **Run As another user**. Here, you are accessing this logon type to open the program under a different account than the one you used to log in to the workstation.

Logon type 10: Remote interactive logon:

This logon type sometimes referred to as "RemoteInteractive," details using Remote Desktop Protocol (or terminal services) to access a remote workstation or server. This type is similar to #2 (Interactive), but again, we are coming from a remote location.

Authenticators accepted

Because we are using RDP, we have similar authenticators possible. We can use smart cards and biometric devices, as long as they are passed through with appropriate settings in the RDP client software.

Examples

The only main example again is using RDP to connect to a remote computer over the network.

Logon type 11: Cached interactive logon

This is very similar, again, to #2 (Interactive), but instead of a 'live' authentication to a domain controller, Windows locally uses previously entered (cached) credentials to grant the user access permissions to the workstation.

Authenticators accepted

In this instance, only passwords are possible. There are no ways to use a cached smart card token, for obvious reasons.

Examples

The most common example here is when your computer or workstation does not have a network (LAN/WAN) connection. Because Windows can't do a real-time authentication request to a domain controller, as long as 'x' number of days haven't passed since your workstation **did talk** to a domain controller, local cached credentials are used to grant local authentication.

Conclusion

Having a good knowledge of the various logon types in Windows helps IT pros in understanding and troubleshooting issues with various logon events in Event Viewer.

And from a security standpoint, you will very likely be analyzing your domain controller Security event logs when trying to track down malicious activity in your Windows domain.

Windows Logon Application (winlogon.exe)

Logon Application In Server OS

The logon application works with *Logon Agent*.

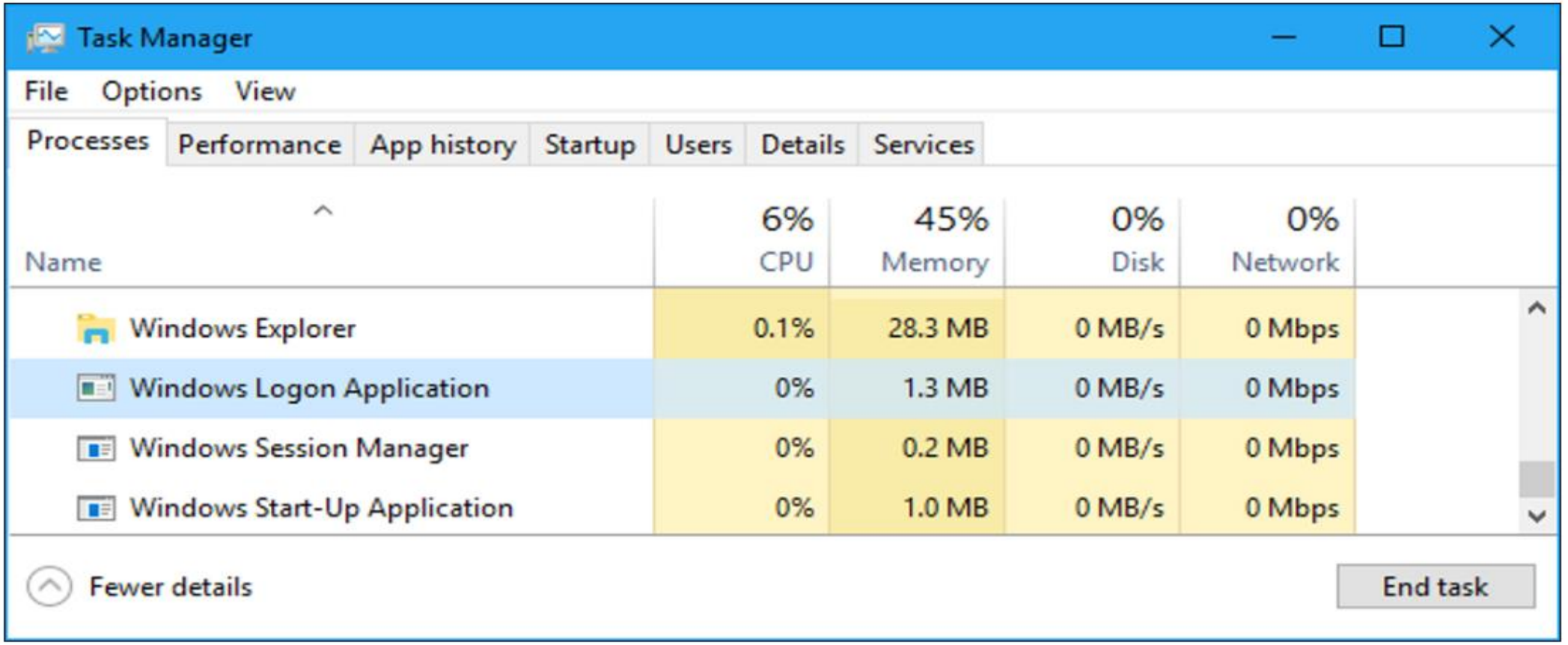
- It runs from a logon script on a domain controller to capture logon sessions as users log on to, or log off of, Windows domains in the network.
- The logon application (LogonApp.exe), runs as a process on *client Windows machines*. It is not installed directly, but rather it is pushed out via Group Policy in Windows domains when employing Logon Agent for user identification.
- At log on, the logon application identifies the user and sends the information to Logon Agent.

Logon Application In client PC

The winlogon.exe process performs a variety of critical tasks related to the Windows sign-in process. For example, when you sign in, the winlogon.exe process is responsible for loading your user profile into the registry.

- This process is always running in the background on Windows, and it's responsible for some important system functions.

Ctrl+Alt+Delete -> Task manager



Introduction cont…

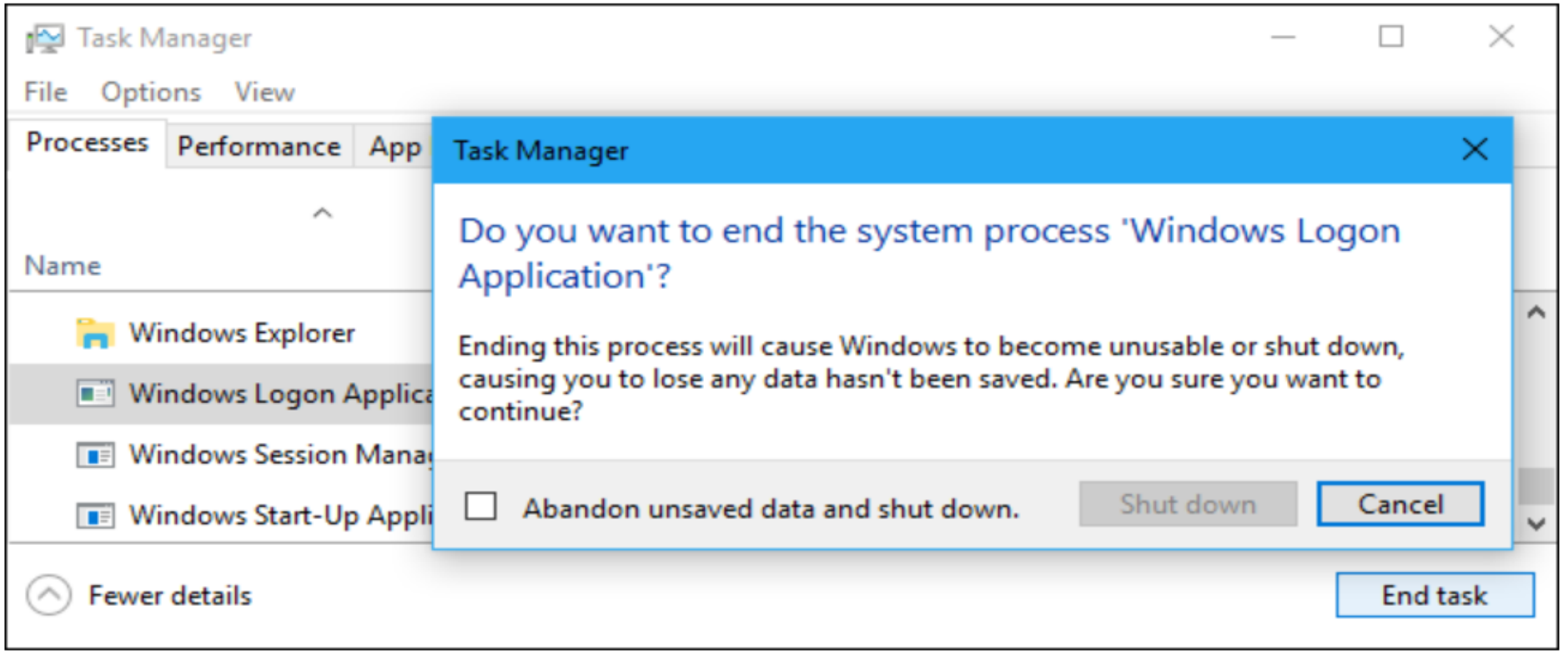
Winlogon.exe has special hooks into the system and watches to see if you press Ctrl+Alt+Delete.

- This is known as the "secure attention sequence", and it's why some PCs may be configured to require you to press Ctrl+Alt+Delete before you sign in.
- This combination of keyboard shortcuts is always caught by winlogon.exe, which ensures you're signing in on a secure desktop where other programs can't monitor the password you're typing or impersonate a sign-in dialog.

The Windows Logon Application also monitors you keyboard and mouse activity and is responsible for locking your PC and starting screen savers after a period of inactivity.

Disabling Windows logon application

You can't disable this process. It's a crucial part of Windows and must be running at all times.

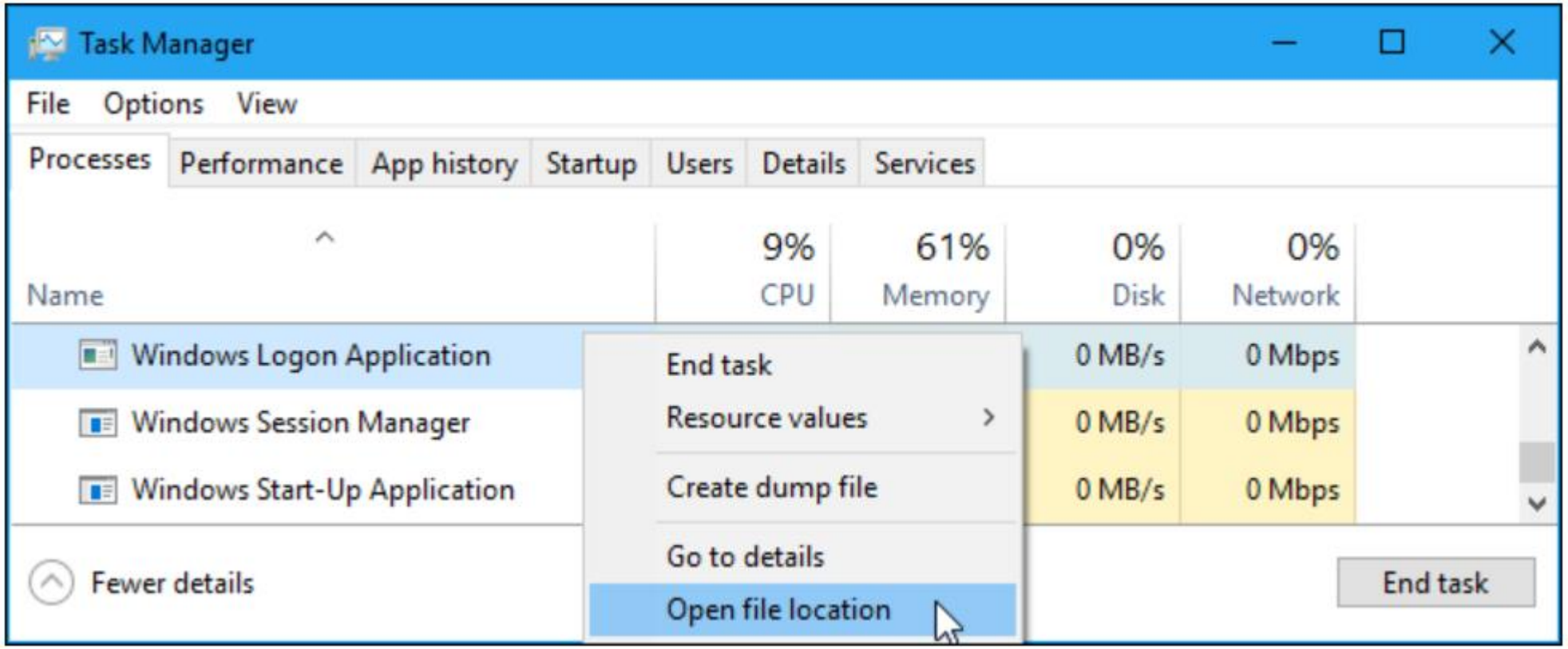


Windows logon application not accessible

Windows will always launch this process when you start your PC.

If Windows can't launch winlogon.exe, csrss.exe, or other critical user system processes, your PC will blue screen with error code 0xC000021A.

- The real winlogon.exe file is located in the C:\Windows\System32 directory on your system.
- To verify the real Windows Logon Application is running, right-click it in Task Manager and select "Open file location".


Task Manager
File
Options
View
Processes
Performance
App history
Startup
Users
Details
Services
Name
9%
CPU
61%
Memory
0%
Disk
0%
Network
Windows Logon Application
Windows Session Manager
Windows Start-Up Application
0 MB/s
0 Mbps
0 MB/s
0 Mbps
0 MB/s
0 Mbps
End task
Resource values
Create dump file
Go to details
Open file location
Fewer details
End task

Checking User Login History in Windows Active Directory

IT administrators often need to know who logged on to their computers and when for security and compliance reasons.

Although you can use the native auditing methods supplied through Windows to track user account logon and logoff events, you may end up having to sift through thousands of records to reach the required log.

Once you've found the required log, getting the required information for compliance and security reports is not an easy process.

Enable Native Auditing for User Logon/Logoff Events

You can do this through two GPO settings:

1. Audit Logon Events: This setting generates events for starting and ending logon sessions. These events happen on the machine where you log in.

2. Audit Account Logon Events: This setting generates events on the computer that validates logons. When a domain controller authenticates a domain user account, events are generated and stored on that domain controller.

Enable Native Auditing for User Logon/Logoff Events

Below are the steps to enable auditing of user Logon/Logoff events:

Step 1 – Open the "Group Policy Management" console by running the "gpmc.msc" command.

Step 2 – If you want to configure auditing for the entire domain, right-click on the domain and click "Create a GPO in this domain, and Link it here…".

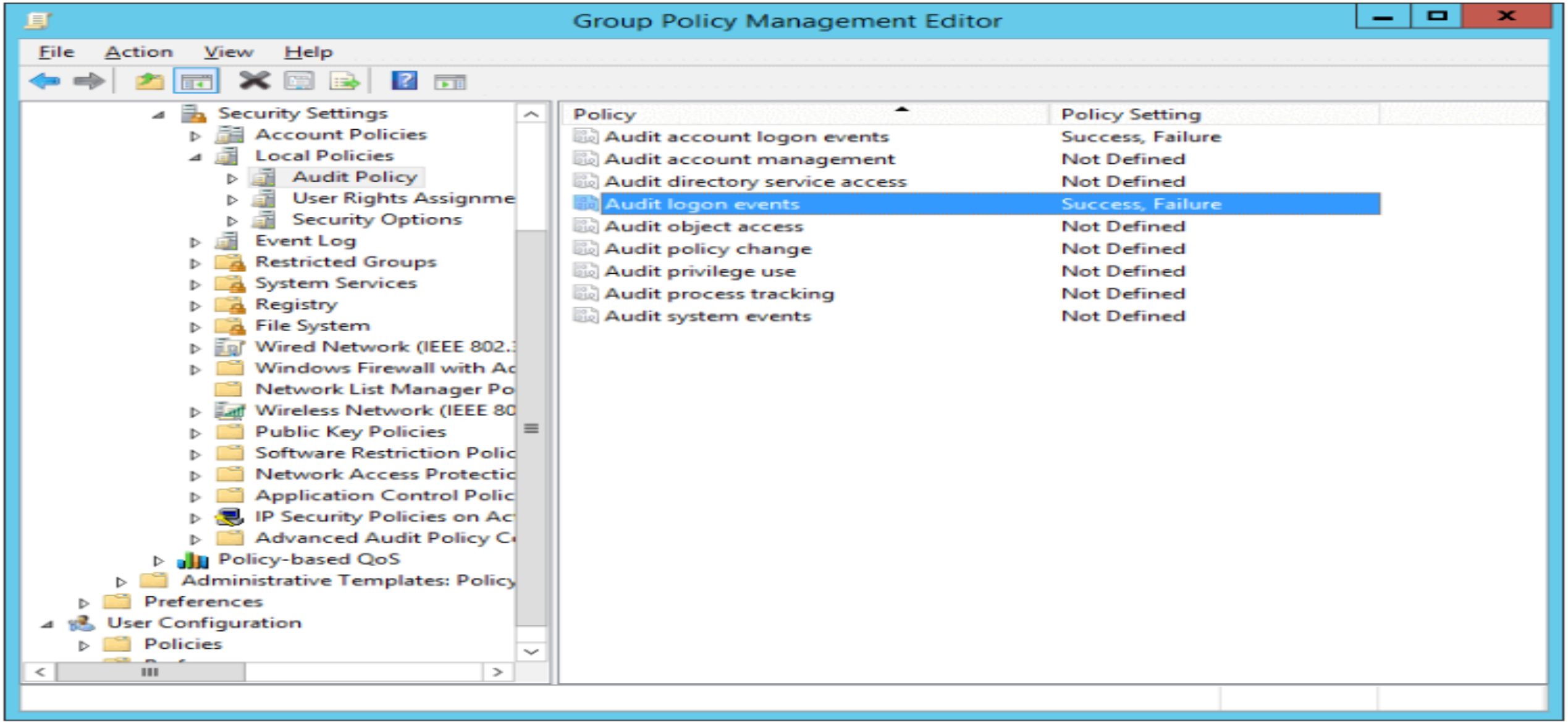
Step 3 – Create a new GPO dialog box that appears on the screen. Enter a new GPO name.

Step 4 – Go to the new GPO, right-click on it, and select "Edit" from the context menu.

Step 5 – "Group Policy Management Editor" window appears on the screen.

Step 6 – In the navigation pane, go to "Computer Configuration" ➔ "Policies" ➔ "Windows Settings" ➔ "Security Settings" ➔ "Local Policies" ➔ "Audit Policy".

Figure: Configuring audit logon events policy



Steps cont…

Step 7 – In the right pane, double-click the "Audit logon events" policy to open its properties window.

Step 8 – Select the "Success" and "Failure" checkboxes, and click "OK".

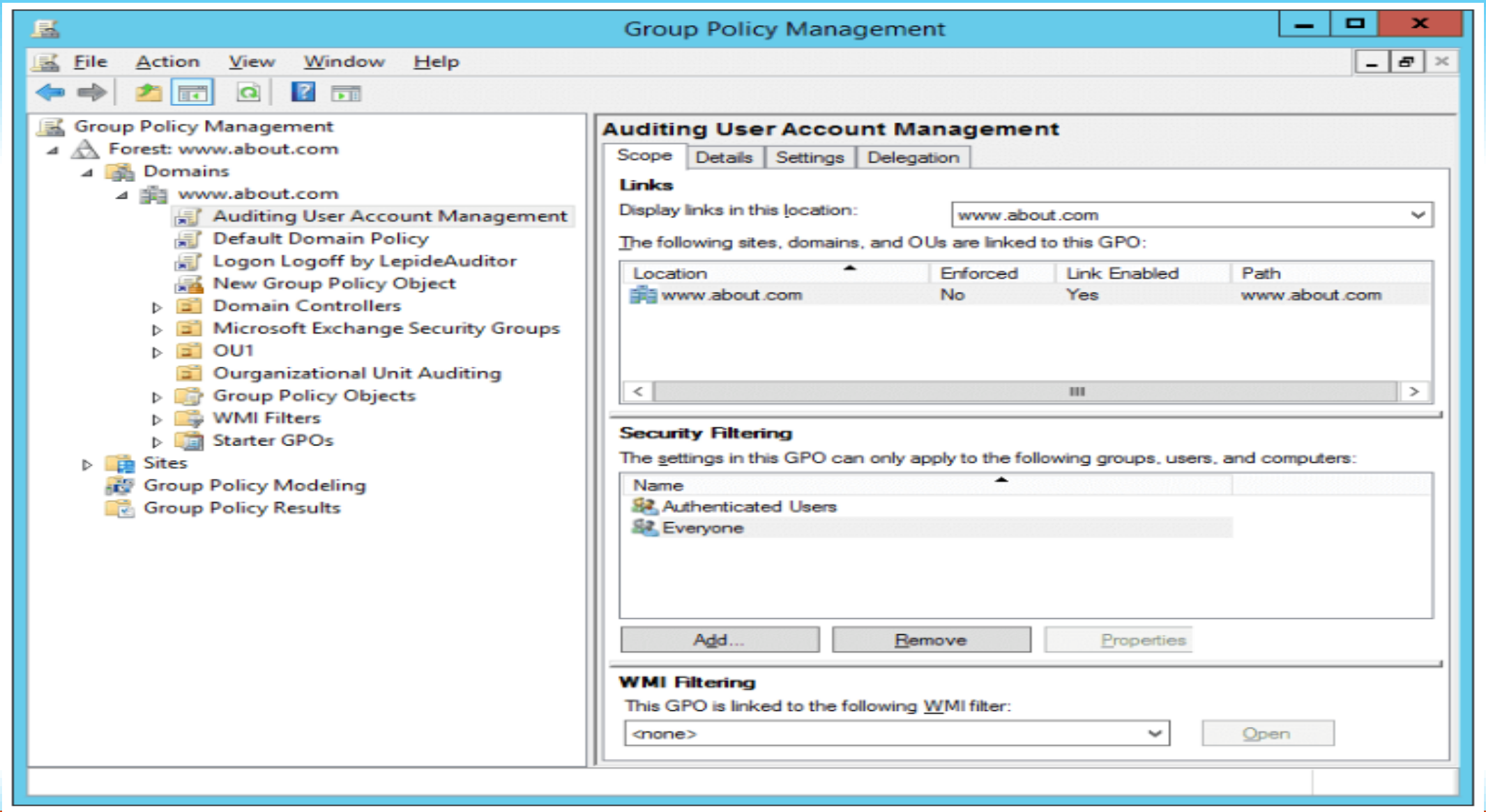
Step 9 – Similarly, you have to enable "Success" and "Failure" for "Audit Account Logon Events".

Step 10 – Close "Group Policy Management Editor".

Step 11 – Now, you have to configure this new Group Policy Object (containing this audit policy) on all Active Directory objects including all users and groups. Perform the following steps.

- In In "Group Policy Management Console", select the new GPO (containing the above change).
- In the "Security Filtering" section in the right panel, click "Add" to access the "Select User, Computer or Group" dialog box.
- Type "Everyone". Click "Check Names" to validate this entry. Click "OK" to add it and apply it to all objects.

Figure : Applied the Group Policy Object to everyone



Steps cont…

Step 12 – Close "Group Policy Management Console".

Step 13 – Now, run the following command to update GPO.

Step 14 – **gpupdate /force**

Check Login History by Tracking Logon/Logoff Events in Windows Event Viewer

After you have configured log on auditing, whenever users logon into network systems, the event logs will be generated and stored. To find out the details, you have to use Windows Event Viewer. Follow the below steps to view logon audit events:

Step 1 – Go to Start ➔ Type "Event Viewer" and click enter to open the "Event Viewer" window.

Step 2 – In the left navigation pane of "Event Viewer", open "Security" logs in "Windows Logs".

Step 3 – You will have to look for the following event IDs for the purposes mentioned herein below.

Use Lepide Active Directory Auditor to Check User Login History

Using **Lepide Active Directory Auditor**, you can easily monitor AD users' login history by tracking their logon and logoff activities in real-time.

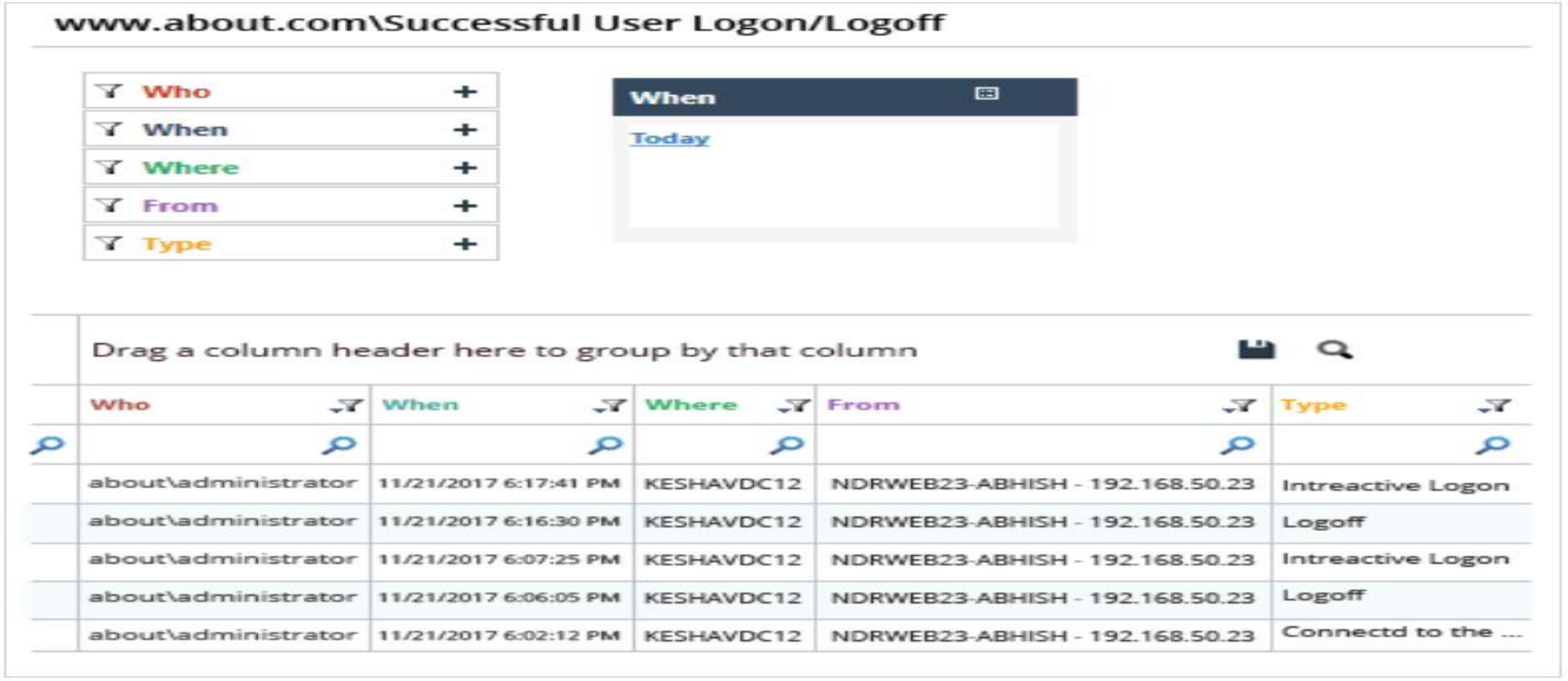
The solution collects log on information from all added domain controllers automatically.

Its report contains details on logon or logoff events, including when users logged in, from which computer, and when.

You get accurate and instant reports on the login details of users in the network.

Figure: Successful User logon/logoff report

The following screenshot shows a successful user logon report event captured by Lepide Active Directory Auditor:



Responsibilities of Winlogon

Window station and desktop protection: Winlogon sets the protection of the window station and corresponding desktops to ensure that each is properly accessible.

Standard SAS recognition: Winlogon has special hooks into the User32 server that allow it to monitor CTRL+ALT+DEL *secure attention sequence* (SAS) events.

SAS routine dispatching: When Winlogon encounters a SAS event or when a SAS is delivered to Winlogon by the GINA, Winlogon sets the state accordingly, changes to the Winlogon desktop, and calls one of the SAS processing functions of the GINA.

User profile loading: When users log on, their user profiles are loaded into the registry. In this way, the processes of the user can use the special registry key HKEY_CURRENT_USER.

Responsibilities of Winlogon

Assignment of security to user shell: When a user logs on, the GINA is responsible for creating one or more initial processes for that user.

Screen saver control: Winlogon monitors keyboard and mouse activity to determine when to activate screen savers. After the screen saver is activated, Winlogon continues to monitor keyboard and mouse activity to determine when to terminate the screen saver.

Multiple network provider support: Multiple networks installed on a Windows system can be included in the authentication process and in password-updating operations.

Thank you!!

For listen