Auditing

- Auditing, on page 1
- View Auditing Policies, on page 1
- View Security Log, on page 2
- Real-Time Alerts, on page 2
- SQL Server Auditing Policies, on page 2
- Active Directory Auditing Policies, on page 2
- Configuration Auditing, on page 3

Auditing

You can set auditing policies to track significant events, such as account logon attempts. Always set Local policies.

Note Domain auditing policies always overwrite local auditing policies. Make the two sets of policies identical where possible.

To set local auditing policies, select **Start** > **Programs** > **Administrative Tools** > **Local Security Policies**.

View Auditing Policies

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Local Security Policies**.

The Local Security Settings window opens.

Step 2 In the tree in the left pane, select and expand **Local Policies**.

Step 3 In the tree under Local Policies, select **Audit Policy**.

The different auditing policies appear in the left pane.

Step 4 View or change the auditing policies by double-clicking the policy name.

View Security Log

After setting auditing policies, view the security log once a week. Look for unusual activity such as Logon failures or Logon successes with unusual accounts.

To view the Security Log:

Procedure

Choose **Start** > **Programs** > **Administrative Tools** > **Event Viewer**.

Real-Time Alerts

Windows provides the SNMP Event Translator facility. This facility lets you translate events in the Windows eventlog into real-time alerts by converting the event into an SNMP trap. Use evntwin.exe or evntcmd.exe to configure SNMP traps.

For more information about configuring the translation of events to traps, see the Microsoft TechNet articles on the **Evntcmd**.

Refer to the *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* guide for information about configuring SNMP trap destinations.

SQL Server Auditing Policies

For general SQL Server auditing policies, see the Microsoft documentation .

SQL Server C2 Security Auditing

C2 security is a government rating for security in which the system is certified for discretionary resource protection and auditing capability.

Cisco does not support C2 auditing for SQL Server in the Unified ICM/Unified CCE environment.

Active Directory Auditing Policies

Routinely audit Active Directory account management and logins. Also monitor audit logs for unusual activity.

The following table contains the hardened and default DC Audit policies.

Table 1: Active Directory Audit Policy Settings

Policy	Default setting	Hardened setting	Comments
Audit account logon events	No auditing	Success and Failure	Account logon events are generated when a domain user account is authenticated on a Domain Controller.
Audit account management	Not defined	Success	Account management events are generated when security principal accounts are created, modified, or deleted.
Audit directory service access	No auditing	Success	Directory services access events are generated when an Active Directory object with a System Access Control List (SACL) is accessed.
Audit logon events	No auditing	Success and Failure	Logon events are generated when a domain user interactively logs on to a Domain Controller. Logon events are also generated when a network logon to a Domain Controller is performed to retrieve logon scripts and policies.
Audit object access	No auditing	(No change)	
Audit policy change	No auditing	Success	Policy change events are generated for changes to user rights assignment policies, audit policies, or trust policies.
Audit privilege use	No auditing	(No change)	
Audit process tracking	No auditing	(No change)	
Audit system events	No auditing	Success	System events are generated when a user restarts or shuts down the Domain Controller. System events are also generated when an event occurs that affects either the system security or the security log.

Configuration Auditing

Unified CCE captures a history of all system configuration changes in the Config_Message_Log table. However, the information that is captured in the Config_Message_Log table is encrypted. To display the table in a meaningful format, use the dumpcfg utility, which is a database administration tool. You can use the information that is retrieved for auditing purposes.

To run the utility, on the command prompt use the following command:

dumpcfg *<database></@server>|[</bd begin date>]|[</bt begin time]>|[</ed enddate]>| [</ed endtime>]|[</nd number_of_days>]|[<low recovery key>]|[<high recovery key>]*|.

Where:

1. *database* is the case-sensitive name of the logger database.
2. *@server* is the hostname of the AW or logger database.
3. *<database></@server>|[</bd begin date>]|[</bt begin time]>|[</ed enddate]>| [</ed endtime>]|[</nd number_of_days>]|[<low recovery key>]|[<high recovery key>]|* are the time range for which the information is required.

   RecoveryKey is a value that the software uses internally to track virtual time.

The *dumpcfg* command displays the following output details:

- **LogOperation**: Indicates the type of the configuration operation. For example, *Add* and *Update*.
- **TableName**: Represents the name of the table that the configuration operation had impacted.
- **DateTime** Indicates the date and time of the configuration operation.
- **ConfigMessage**: Lists all the configuration messages for a configuration operation.

For example, if you add a skill group and then run the following command:

For example, if you add a skill group and then run the command:**dumpcfg ucce_sideA@uccergr100a /bd 09/27/2018**

The output displays the following details:

LogOperation - **Add**.

TableNames -skill_target and t_skill_group.

DateTime - the exact timestamp when the skill group was added.

ConfigMessage - the field names impacted, such as **Peripheral Name**, **Enterprise Name**, and so on.