Quest® Change Auditor Threat Detection 7.2

User Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Legend

! **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

i **IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Threat Detection User Guide
Updated - January 2022
Software Version - 7.2

Contents

Introduction to Change Auditor Threat Detection

Overview

Detecting suspicious activity by rogue users is a difficult challenge. The traditional rule-based approach to user threat detection generates too many alerts to investigate. As a result, you waste time with false positives and risk missing the real threats, leaving your organization at risk of a data security breach.

To effectively protect your data and your business, Change Auditor Threat Detection uses advanced machine learning, user and entity behavioral analytics (UEBA), and SMART correlation technology to spot anomalous activity and identify the highest risk users in your environment.

More specifically, Change Auditor provides a threat detection solution that:

- Is automated - The system does not rely on rules and prioritized alerts created by analysts.
- Analyzes historical data to create user behavior baselines, and uses the constant stream of incoming data to update and improve models.
- Correlates events, unifying multiple anomalies and supporting information into a single alert to reduce the volume of alerts and facilitate analysis.
- Provides a manageable number of potential threats, prioritized by risk level, to ensure you can identify and investigate the most serious threats first.
- Presents potential threats in a way that is easy to understand the sequence of events and their relationships, to facilitate quick investigation and response.
- Provides a way to give input that feeds back into the risk scoring and prioritization model.

This guide gives information about the Threat Detection dashboard functions and capabilities for IT and security analysts. It is also relevant to chief information security officers, security architects, network administrators, and auditors responsible for information security in large organizations who need to understand the functionality and abilities made possible using the solution.

Which Change Auditor modules are monitored?

Threat Detection analyzes Change Auditor events to build a user behavior baseline and to detect anomalies and threats. User activity from the following Change Auditor subsystems is streamed to the Threat Detection server for processing to build the global map of users, groups, systems and files in your environment:

- Authentication activity from Change Auditor for Logon Activity
- Active Directory user and group changes from Change Auditor for Active Directory
- File access activity from Change Auditor for Windows File Servers, Change Auditor for EMC, Change Auditor for FluidFS and Change Auditor for NetApp

Threat Detection server events

Threat Detection server activity is also monitored. Events are generated when:

- A risky user is identified.
- Risky user severity is increased or decreased.
- An alert is generated.
- An alert is marked as a risk.

- An alert is marked as not a risk.

To view Threat Detection events in the Change Auditor client:

- Open the Audit Events page on the Administration Tasks tab | Auditing

  The events are listed under the Threat Detection - Risky User" facility and the "Threat Detection - Alert" facility.

  The event details pane contains information to help gain a better understanding of the activities taking place on the Threat Detection server including:

  - The number of alerts and their name, severity, score.
  - User risk score, severity, old and new severity.
  - When the Threat Detection server started processing the alert.
  - Indicators associated with the alert.
  - Contribution to user score.

  For more information on the details displayed for these events, see the Change Auditor Event Reference guide.

Threat detection concepts

The following section describes the terms and concepts used within Change Auditor Threat Detection to help you understand how risk is assessed and alerts are determined.

- Baselines
- Threat indicators
- SMART alerts
- Risk scoring

Baselines

Change Auditor Threat Detection applies machine learning to build behavioral features and a multi-dimensional baseline of typical behavior for each user in your environment. The baseline comprises a unique set of identifiers to ensure that only abnormal behaviors are flagged. For example, the baseline can include information about when a user typically logs on, which workstation they use, whether they tend to log on from remote locations, which files they typically access and so on.

As the baselines are refined over time, the Threat Detection server makes logical assumptions around what to expect, which minimizes the chances for any alarms around normal changes in activity. Change Auditor Threat Detection requires 30 days of audit history to establish the initial user behavior baselines.

Threat indicators

Indicators define risky activity, such as suspicious user logons, brute-force password attacks, unusual Active Directory changes, and abnormal file access. However, threat indicators are not constrained to a specific raw event — they use machine learning to identify patterns of events that together could indicate a threat.

Specifically, as raw events stream in, the Threat Detection server analyzes human actors, accounts, locations and operations to identify behavior that deviates from established baselines.

Abnormal and risky behaviors are evaluated to produce threat indicators. These indicators are based on present and historical patterns, as well as specifically defined risky object attributes. An indicator consolidates all activities that are detected as abnormal.

Anomalous behavior that corresponds with a threat indicator is identified based on the event's rarity and criticality. This strategy ensures that only behavioral changes that are important and potentially indicative of a suspicious activity are highlighted out of the raw events.

Threat indicators are the basis for the formation of alerts. Sorted by severity to reflect the security importance, alerts are managed by the analyst providing investigation and feedback.

SMART alerts

SMART (Significant Multidimensional Anomaly Reduction Technology) is a correlation technology that provides prioritized results for dynamic and frequently changing behaviors. The technology uses statistical and machine learning algorithms to identify unique connections between anomalies, thereby reducing false positives and helping to spot threats.

SMART prioritizes and consolidates threats that reflect a meaningful deviation in user behavior. As a result, while millions of raw events might yield discovery of thousands of threat indicators, only patterns of truly suspicious behavior are scored. This means that fewer alerts are raised in the Threat Detection dashboard, and fewer false positives are identified. Like baselines, SMART alerts improve over time as more log data is processed, so they deliver increasingly accurate user threat detection.

Risk scoring

Each alert is assigned a risk score based on the criticality of its threat indicators. All the alerts that have been identified for each user are combined to produce an overall user risk score that reflects how risky or suspicious that user is. To ensure that only highly suspicious patterns of activity are highlighted and more innocuous alerts are suppressed, risk scoring is applied at four different stages.

Table 1. Event scoring stages

Stage	Description
Stage 1: Event scoring	Each raw event is given an initial risk score that rates the abnormality of its parameters, such as the computer, time or file location.
Stage 2: Threat indicator scoring	Similar events are grouped as threat indicators and scored again to identify abnormal patterns that extend over a period of time, such as an hour.

Table 1. Event scoring stages

Stage	Description
Stage 3: Alert scoring	SMART alerts correlate events and threat indicators into an aggregate alert, which is scored for a third time based on the uniqueness of its composition and the severity of the activities involved. Indicators that are not scored high enough, or that are not correlated with other indicators in the same time period, are eliminated as false positives so that they do not create excessive noise. Only the SMART alerts that are scored as most critical are shown in the dashboard. The final score ranges between 0 and 100, where 0 reflects an event/session/user which is completely adequate with the normal baseline, whereas 100 indicates a very unusual anomaly.
Stage 4: User risk scoring	The user risk score is an aggregate of the contribution to user scores for each alert related to the user. The contribution to the user score value for the alert is dependent on the alert severity. Critical alerts contribute 20, high contribute 15, medium contribute 10, and low contribute 1. The users with the highest risk scores are highlighted in the Threat Detection dashboard.

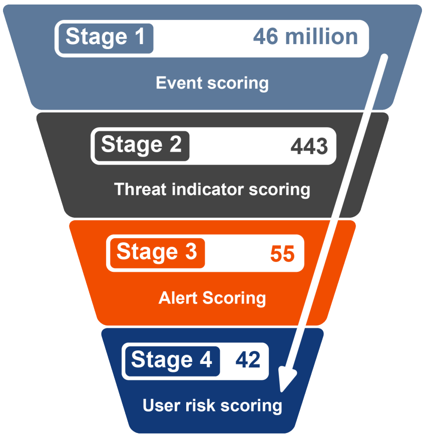


Figure 1. Event scoring stages

Threat Detection process

Threat Detection process includes the following steps:

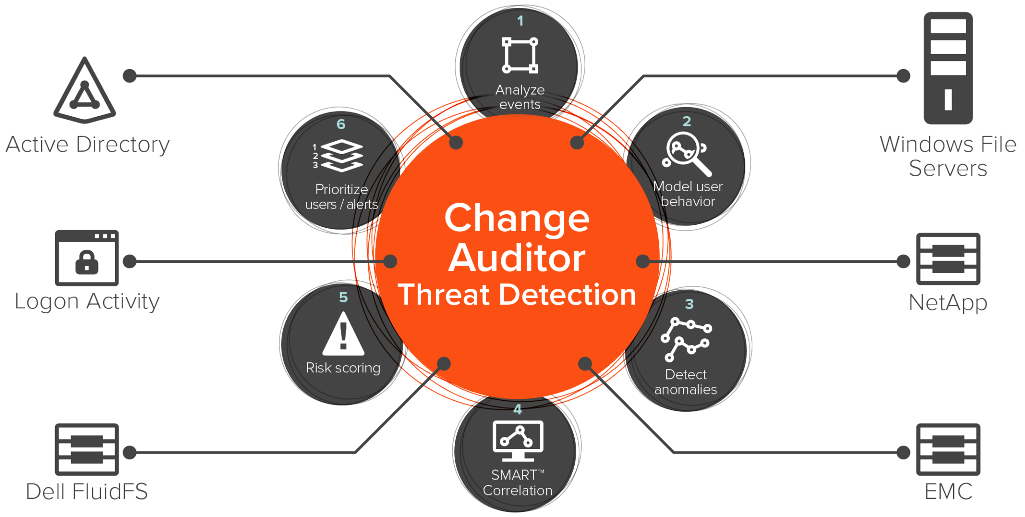


Figure 2. Overview of the Change Auditor Threat Detection input sources and threat assessment process

1 Events are sent to the Threat Detection server to be processed and analyzed.

2 Machine learning and user behavior analytics analyze user actions in the stream of events and builds a multi-dimensional baseline of typical behavior for each user in the environment.

3 Once the baselines are established, predefined threat indicators are used to detect anomalous user activity in real time.

4 SMART technology provides prioritized alerts that reflect a meaningful deviation in user behavior.

5 A risk score is assigned to each alert to identify the level of threat they pose to your environment.

6 A risk score is assigned to each user. This score is a sum of the total alert points assigned to the user using the "contribution to user score'" points associated with each alert. Users with the highest user risk scores are highlighted in the Threat Detection dashboard, creating a dynamic watch list of emerging risky user threats sorted by severity.

2

Using the Threat Detection Dashboard

Deployment and installation

For detailed instructions on how to deploy and properly install Threat Detection, see the Change Auditor for Threat Detection Deployment Guide.

For information about Change Auditor system requirements, see the Change Auditor Release Notes and the Change Auditor for Threat Detection Deployment Guide.

Accessing the dashboard

Once you have deployed the Threat Detection server, configured Change Auditor for Threat Detection, and the system has analyzed 30 days of historical data to create a baseline of user behavior, you can access the Threat Detection dashboard.

To allow access to the Threat Detection dashboard in the Change Auditor client or through Chrome using single-sign on, the Threat Detection server is joined to the coordinator's domain during the initial Threat Detection configuration or manually during an upgrade. See the Change Auditor Threat Detection Deployment Guide for details on creating a configuration or updating the Threat Detection server.

To access the dashboard from Change Auditor

- Select **View | Threat Detection Dashboard**.

  > **NOTE:** The account used to access the dashboard is the user currently logged on to Change Auditor.

To access the dashboard through Chrome

- Use the DNS name for the Threat Detection server provided during deployment. For example: "https://TDServerName.DomainName.Com/caui-webapp/index.html".

> **NOTE:** The following prerequisites are required to enable single-sign on:
>
> - In the Internet Options security settings, add the URL for the Threat Detection dashboard to:
>   - Trusted Sites with the **User Authentication | Logon | Automatic logon with current username and password** option enabled.
>
>   - OR-
>   - Local Internet
> - You must be a member of the Change Auditor Administrators or Operators group in the same domain as the Threat Detection server's domain. To grant access to users from other domains in the same forest, add them to one of the Change Auditor's groups.

Overview tab

The Overview tab provides an initial view of the recent and most important user activities in your environment. At a glance you can see details on the high risk user such as their photo, display or logon name, job title, department, and their address.

Each pane shows either prioritized incidents for investigation or consolidated metrics reflecting potential risks to the enterprise.

- High Risk Users
- SMART Alerts
- All Users

- Alerts Status
- Alerts Severity

High Risk Users

User risk scores are a primary tool for incident prioritization. Using the score, the system highlights specific user accounts that require immediate attention.

The user risk score is the addition of the "contribution to user score" assigned to each alert that is associated with the user and the analysts notes.

> **NOTE:** The Analyst Notes section of the dashboard allows analysts to mark an alert as an Actual Risk or Not a Risk.

Score calculation formula:

User Risk Score = ∑ [Unreviewed (no analyst notes provided) & "Actual Risk"] - ∑ ["Not A Risk"]

The contribution to the user score value for the alert is dependent on the alert severity. The severities are color coded to help identify the severity quickly.

Table 2. Severity color code and contribution to user score values based on alert severity

Severity	Color	Contribution
Critical	Red	+20
High	Yellow	+15
Medium	Blue	+10
Low	Green	+1

The High Risk Users pane lists users with the highest user risk scores, and the following information related to each of those alerts:

- Username: Name of the user.
- User Risk Score: The risk score of the user.

To investigate a user, click anywhere in the user frame to investigate the user’s alerts. See How to perform an alert investigation for more information.

Retired alerts

Alerts and their associated indicators are retired after 90 days and the alert score drops to 0. Once an alert is retired, the risky user is also removed from the dashboard. The retired alerts and indicators remain accessible in the dashboard for an additional 6 months. They will not affect the user score, and they will be grayed-out in the user profile page.

SMART Alerts

The SMART Alerts pane displays a list of alerts, severity level, alert creation date, and number of indicators. The list is comprised of the top ranked SMART alerts in the last 2 months.

Clicking on a SMART Alert displays the corresponding alert on the Alert Overview page, allowing for further investigation (see How to perform an alert investigation).

All Users

The All Users pane displays the number of users in each of the Threat Detection predefined groups. The groups are:

- Risky
- Watched
- Admin

See Filters for details on these groups.

To investigate alerts affiliated with a specific group

- Click the group icon.

  This opens the USERS tab with the Tags filter set to the group that you selected. For more information on using the USERS tab, see Users tab.

Alerts Status

The Alerts Status pane displays the number of alerts that have been reviewed and the number that have not been reviewed, for the last month and over the last 2 months.

Alerts are marked as reviewed once analysts notes have been added. See How to perform an alert investigation.

Alerts Severity

The Alerts Severity pane graphically displays the number of alerts, by severity level, generated during the last 2 months.

To investigate further

- Click the portion of the graph on the day that you want to investigate.

  This display the ALERTS tab, based on your selection, with the severity and time filter already set. For more information, see Alerts Tab.

Users tab

The Users tab enables you to use filters to build target lists, to continuously monitor the environment for specific risky behavior patterns.

- Filters
- Users Grid

Filters

You can use alert and indicator filters to only show the users and information that is of interest to you. The Filters pane lists pre-defined filters, with the number of users associated with each in parentheses. Clicking any of these displays all the users that fall into that category. The pre-defined filters are:

- Risky Users: All users with a user risk score greater than 0.
- Watchlist Users: All users who are currently flagged as “Watched”. See Add a user to the watch profile.

- Admin Users: All users who have been previously identified as an administrator through Change Auditor as a member of one of the following groups:
  - Local Administrators
  - Active Directory Administrators
  - Domain Administrators
  - Enterprise Administrators

  ℹ **NOTE:** This is supported in Change Auditor 7.0 and later.

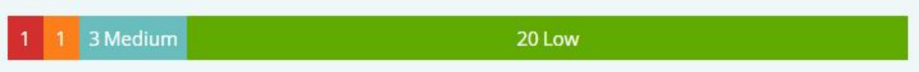
To create a filter

1. Click the filter that you want to modify.
2. Select the desired options from the drop-down list.
3. Click **OK**.

   If required, after creating a filter, you can save it as a favorite, by clicking Save to Favorites**.**

Risk Navigator

The Risk Navigator is the color bar that is displayed at the top of the pane when the Users tab is open. It provides a severity-based breakdown of the target users.



User severity calculation

The severity of the user's aggregate risk score is determined based on a dynamic heuristic which varies based on the scores of the users and number of users scored in the environment.

- A maximum of 5 users will be tagged as critical depending on the spread between their user scores and the scores below them.
- A maximum of 5 users will be tagged as high.
- A maximum of 10% of users will receive a medium severity.
- The remainder will receive a low severity.

The user severity is displayed by the color of the user risk score. You can filter based on the user severity.

Table 3. User severity color code

Severity	Color
Critical	Red
High	Orange
Medium	Blue
Low	Green

Users Grid

At a glance you can see user details such as their photo, display or logon name, job title, department, and address.

> **NOTE:** Alerts generated from Active Roles or GPOADmin events, use the name of the account that initiated the event (rather than the associated Service Account) for the user information in the Threat Detection portal.

The grid includes the following user data:

- Watchlist status
- User risk score
- Number of alerts

Additional grid functions:

- Sort by: Use this function to sort the existing list of users by Risk Score, Name, or Number of Alerts.
- Export: Click to export information for the current list of users to a .csv file. The file will be automatically downloaded.
- Add All to Watchlist: Click to add all users in the current filtered view to the watchlist.
- Search Users List: Enter the name of a user to search for, and select it from the list that is displayed matching your entry.

Alerts Tab

The Alerts tab displays detailed information about all the SMART Alerts found by the system. The Alert List at the top of the central pane displays the number of alerts for each severity level, corresponding to the Alert Filter settings in the left pane.

Alert severity calculation

The severity of the alert is based on the alert score. To see the alert score, hover over the alert severity icon.

- Critical severity has a score of 98 – 100.
- High severity has a score of 93 – 97.
- Medium severity has a score of 85 – 93.
- Low severity has a score of 75 – 84.

Alerts that do not meet the minimum threshold of 75 are discarded as false positives.

- Alert List
- Alert Filter

Alert List

The central pane displays the following information for each alert:

- Severity Icon: An icon next to the alert name that indicates the severity level of the alert. Hover over the icon to see the alert score.
- Alert Name: The name of the alert.
- Entity Name: The name of the entity (for example, user account) that generated the alert.
- Start Time: The date and time when this alert was first detected.
- # Indicators: The number of unique threat indicators associated with the alert.
- Status: Indicates if the alert has been marked as Unreviewed or Reviewed.
- Feedback: Displays as either "No Feedback" "Actual Risk" or "Not a Risk".

Click the arrow by each alert to display the following additional details:

- Indicator Name: The name of each unique indicator that is associated with the alert.
- Anomaly Value: The value determined to be abnormal when compared to the baseline. This could be a number, timestamp, or text value. For example, if a user opens the same file numerous times in the same hourly timeframe, it will only display as 1 in the anomaly value.
- Data Source: The data source (authentication, file, or Active Directory) of the risky activity.
- Start Time; The date and time when this indicator was first detected.
- # Events: The number of events in the indicator.

You can export the alert that is currently displayed in the central pane by clicking Export.

Alert Filter

Use the Alert Filter pane to display a subset of alerts. The following is a list of the filter categories and values:

- Severity: Filter the list to include alerts for one or more severity level, including Critical, High, Medium, or Low.
- Feedback: Filter the list to include alerts for one or more feedback type, including Select All, No Feedback, Actual Risk, or Not a Risk. See Alert List for information on providing feedback.
- Entity: Filter the list to include only alerts for a specific username.
- Indicators: Filter the list to include alerts for one or more indicators (For example, Active Directory - Abnormal Logon Time, Authentication - Logged onto Multiple Computers, Multiple File Access Failures, and so on.)
- Date Range: Filter the list to include alerts created during a specific date range, including the Last Week, Last Month, or during a specified range.

The filters are automatically applied as you make your selections. You can clear all currently set filters by clicking Clear.

How to perform an alert investigation

The alert investigation allows you to select existing alerts and indicators for investigation. When investigating a user or an alert for a specific user, you will also see details such as their photo, display name and logon name, email, job title, address, manager and a link to their email address, department, and office.

From the Alerts tab, there are a few options available to start an investigation:

- To investigate a user, click the username in the Entity Name column. This takes you to Alert Overview, where you can investigate the alerts associated with that user.
- To investigate a specific alert for a user, click the alert name in the Alert Name column. This takes you to Alert Overview with the desired alert already selected in the Alerts pane on the left.

  From the Alert Overview pane, you can see a summary of the alert information, including:

  - The alert name.
  - A description of the alert.
  - The time frame of the alert (hourly).
  - The severity level icon.
  - The contribution to the user score value (for example, +20).
  - The sources for the alert (for example, Authentication).
  - Analyst notes.
  - Alerts flow.

  The Alert Flow view provides a timeline of indicators that are related to the formation of the alert. The timeline can help to determine if the alert is an actual risk or not.

  The Analyst Notes section allows you to mark the alert as an Actual Risk or Not a Risk. Additionally, you can add comments about the alert for future reference. When an alert is marked as Not a Risk, the contribution to user score associated with the alert is immediately subtracted from the user risk score.

  Analyst's notes and alert feedback are displayed on the Overview pane. Changes to the user risk score are also listed, and reflect their value at the time of the feedback.
- To investigate a specific indicator that is related to an alert for a user, click the arrow icon next to the alert name. For each indicator you will see:

  - The indicator name.
  - Anomaly value: The value determined to be abnormal when compared to the baseline. This could be a number, timestamp, or text value.
  - Data source of the events found in the indicator.
  - Start time: Date and time the Threat Detection server started processing the alert.
  - Number of events.

  Clicking the indicator name in the Indicator Name column takes you to Alert Overview with the indicator already selected in the Alerts pane and provides the following information:

  - Contribution to SMART: The percentage that each indicator contributed to the SMART alert is calculated based on their assigned score and the number of times they contributed. The total of all contributions is normalized to 100% by dividing the total score for each indicator by the sum of all the scores that contributed to the alert. For example, if an alert had two associated indicators and the score of the first indicator is 50 and the second is 25, and each contributed once to the alert, the contribution for would be 66% for the first indicator and 33% for the second. (50 divided by 75 and 25 divided by 75).
  - The graphic view of the behavioral baseline, with the anomaly highlighted in red.
  - The table containing all the events that took part in this behavioral anomaly.

  To close the indicator view and return to the Alert Overview view, click the X on the top right corner of the pane.
- To switch between the Alert Overview and Indicator views, click the directional symbols (< and >) on the top right corner of the alert view pane.
- To follow the user to make its actions easier to track in the future, click the Watch Profile icon on the top right of the Alert Overview pane.

Common functions

There are many common functions that are used throughout the dashboard. Two of these are listed here for reference:

Search for a user

The Search User tool is located on the upper right corner of the dashboard. Using the tool, you can easily access alert investigations, and instantly drill down into their past behaviors.

To search for a user

1. Type letters from the required username into the search field.

   Auto-complete provides suggestions for the user that you are looking for. This includes the user photo, display or logon name, job title, department, and address.

2. Clicking on one of the options provided from the menu redirects you to the specific Alert Overview.

Add a user to the watch profile

If there is a user that you want to follow, you can add them to the list of watched users. You can quickly access the watched users from the Overview pane or by clicking the Watched icon in the All Users pane.

To start watching a user, click Watch Profile from their alert overview. To stop watching a user, click Stop Watching. You can also select to add more than one user by selecting Add all to Watchlist from the Users tab.

3

Alert and indicator reference

Alert types

The following table defines the alerts that can be detected and the related risky behavior.

Table 1.

Alert Type	Description and associated indicators to investigation
Mass Changes to Critical Enterprise Groups	**Details**: An abnormal number of changes made to critical enterprise groups. For details see, Change Auditor for Active Directory Event Reference Guide (Members Added to Critical Enterprise Group event). These groups often manage and control high-value IT assets. If these assets are compromised, attackers can escalate privileges and exploit them to establish persistent control over the domain. **Action to take:** Investigate which elements have been changed, and decide if the changes are legitimate or possibly the result of risky or malicious behavior. **Associated indicators:** This activity is usually associated with the Multiple Member Additions to Enterprise Critical Groups indicator.
Mass Changes to Groups	**Details**: An abnormal number of changes made to groups. **Action to take:** Investigate which elements are changed, and decide if the changes are legitimate or possibly the result of risky or malicious behavior. **Associated indicators:** This activity is usually associated with the Multiple Group Membership Changes indicator.
Elevated Privileges Granted	**Details:** Elevated account privileges are delegated to a user. Attackers often use regular user accounts, granting them elevated privileges, to exploit the network. **Action to take:** Investigate the user that received the elevated privileges, and decide if these changes are legitimate or possibly the result of risky or malicious behavior. **Associated indicators:** This activity is usually associated with the Nested Member Added to Critical Enterprise Group and Member Added to Critical Enterprise Group indicators.
Brute Force Authentication	**Details:** In traditional password cracking attempts, attackers try to obtain a password through guesswork or by employing other low-tech methods to gain initial access. The attacker risks getting caught or being locked out by explicitly attempting to authenticate; but with some prior knowledge of the user's password history, may be able to successfully authenticate. **Action to take:** Look for additional abnormal indications that the account owner is not the one attempting to access this account. **Associated indicators:** This activity is usually associated with the Multiple Failed Authentications indicator.
User Logons to Multiple Domains	**Details:** Domain controllers store credential password hashes for all accounts on the domain, so they are high-value targets for attackers. Domain controllers that are not stringently updated and secured are susceptible to attack and compromise, which could leave the domain and forest vulnerable. User privileges on multiple domains could indicate that a parent domain has been compromised. **Action to take:** Determine if user access to and from multiple sites is legitimate or is an indication of a potential compromise. **Associated indicators:** This activity is usually associated with the Logged into Multiple Domains indicator.

Table 1.

Alert Type	Description and associated indicators to investigation
User Logon to Abnormal Remote Host	**Details:** Attackers often need to acquire credentials and perform other sensitive activities, like using remote access. **Action to take:** Tracing the access chain backwards may lead to the discovery of other computers involved in possibly risky activity. **Associated indicators:** If an attacker's presence is limited to a single compromised host or to many compromised hosts, that activity can be associated with the Abnormal Remote Computer and Abnormal Computer indicators.
User Logon to Abnormal Host	**Details:** Attackers often need to acquire credentials and perform other sensitive functions. **Action to take:** Tracing the access chain backwards may lead to the discovery of other computers involved in possibly risky activity. **Associated indicators:** If an attacker's presence is limited to a single compromised host or to many compromised hosts, that activity can be associated with the Abnormal Remote Computer and Abnormal Computer indicators.
Data Exfiltration	**Details:** Data exfiltration is the unauthorized copying, transfer, or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various techniques, typically by cybercriminals over the Internet or other network. **Associated indicators:** This activity can be associated with the Excessive Number of File Rename Events, Excessive Number of Files Moved from File System, and Excessive Number of Files Moved to File System indicators.
Mass File Rename	**Details:** Ransomware is malware that encrypts desktop and system files, making them inaccessible. Some ransomware, for example, “Locky”, encrypt and rename files as part of their initial run. **Action to take:** Use the indication of mass-file-renaming to determine if your file system has been infected with Ransomware. **Associated indicators:** This activity can be associated with the Multiple File Rename Events indicator.
Snooping User	**Details:** Snooping is unauthorized access to another person's or company's data. Sophisticated snooping uses software programs to remotely monitor activity on a computer or network device. **Associated indicators:** This activity can be associated with the Multiple File Access Events, Multiple Failed File Access Events, Multiple File Open Events, and Multiple Folder Open Events indicators.
Multiple Logons by User	**Details:** All authentication activity, malicious or not, appears as normal logons. Therefore, administrators should monitor unexpected “authorized” activity. The key is that attackers use stolen credentials for unauthorized access, which may provide an opportunity for detection. When an account is being used for unusual activities, such as authenticating an unusual amount of times, then the account may have been compromised. **Associated indicators:** This activity can be associated with the Multiple Successful Authentications indicator.

Table 1.

Alert Type	**Description and associated indicators to investigation**
User Logons to Multiple Hosts	**Details**: Attackers typically need to reacquire credentials periodically. This is because their keychain of stolen credentials naturally degrades over time, due to password changes and resets. Attackers frequently maintain a foothold in the compromised organization by installing backdoors and maintaining credentials from many computers in the environment. **Associated indicators:** This activity can be associated with the Logged onto Multiple Computers indicator.
Admin Password Change	**Details:** Shared long-term secrets, such as privileged account passwords, are frequently used to access anything from print servers to domain controllers. **Action to take:** To contain attackers, that seek to leverage these accounts, pay close attention to password changes by admins, and ensure they have been made by trusted parties and have no additional abnormal behavior associated with them. **Associated indicators:** This activity can be associated with the Admin Password Change indicator.
Mass Permission Changes	**Details:** Some credential theft techniques, such as Pass-the-Hash, use an iterative, two-stage process. First, an attacker obtains elevated read/write permission to privileged areas of volatile memory and file systems, which are typically accessible only to system-level processes on at least one computer. Second, the attacker attempts to increase access to other computers on the network. **Action to take:** Investigate if abnormal permission changes have taken place on the file systems to ensure that they were not compromised by an attacker. **Associated indicators:** This activity can be associated with the Multiple File Access Permission Changes, Multiple Failed File Access Permission Changes, and Abnormal File Access Permission Change indicators.
Abnormal AD Changes	**Details:** If an attacker gains highly privileged access to an Active Directory domain or domain controller, that access can be leveraged to access, control, or even destroy the entire forest. If a single domain controller is compromised and an attacker modifies the Active Directory database, those modifications replicate to every other domain controller in the domain and, depending on the partition in which the modifications are made, the forest as well. **Action to take:** Investigate abnormal changes conducted by administrators and non-administrators in Active Directory to determine if they represent a possible true compromise to the domain. **Associated indicators:** This activity can be associated with the Abnormal Active Directory Change, Multiple Account Management Changes, Multiple User Account Management Changes, and Multiple Failed Account Management Changes indicators.

Table 1.

Alert Type	Description and associated indicators to investigation
Abnormal Site Access	**Details:** An Active Directory site can be defined as a physical location or network. It can be separate building, separate city, or even in separate country. In an Active Directory infrastructure setup, the domain represents the logical topology while sites and subnets represent the physical topology. Access from abnormal sites could indicate an account is used by users across multiple geographies, and possibly indicate the account has been hijacked. **Action to take:** Determine if user access to and from multiple sites is legitimate or is an indication of a potential compromise. **Associated indicators:** This activity can be associated with the Abnormal Site Access and Logon Attempts from Multiple AD Sites indicators.
Sensitive User Status Changes	**Details:** A domain or enterprise administrator account has the default ability to exercise control over all resources in a domain, regardless of whether it operates with malicious or benign intent. This control includes the ability to create and change accounts; read, write, or delete data; install or alter applications; and erase operating systems. Some of these activities trigger organically as part of the account’s natural life cycle. **Action to take:** Investigate these security sensitive user account changes, and determine if it has been compromised. **Associated indicators:** This activity can be associated with the User Account Enabled, User Account Disabled, User Account Unlocked, User Account Type Changed, User Account Locked, User Password Never Expires Option Changed, User Password Changed by Non-Owner, and User Password Change indicators.
Abnormal File Access	**Action to take:** Monitor for abnormal file access to prevent improper access to confidential files and theft of sensitive data. By selectively monitoring file views, modifications and deletions, you can detect possibly unauthorized changes to sensitive files, whether caused by an attack or a change management error. **Associated indicators:** This activity can be associated with the Abnormal File Access Event and Multiple File Delete Events indicators.
Non-Standard Hours	**Details:** All authentication activity, malicious or not, appears as normal logons. Therefore, administrators should monitor unexpected “authorized” activity. The key is that attackers use these stolen credentials for unauthorized access, which may provide an opportunity for detection. When an account is being used for unusual activities, e.g. authenticating at non-standard time, then the account may have been compromised. **Action to take:** Use the indication of an abnormal activity time to determine if the account has been taken over by an external actor. **Associated indicators:** This activity can be associated with the Abnormal File Access Time, Abnormal Active Directory Change Time, and Abnormal Logon Time indicators.

Threat indicators

The following tables contain indicators (and the alert that they are associated with) available for each Change Auditor subsystem:

Table 2. Change Auditor for Windows File Servers, Fluid File System, NetApp, and EMC

Indicator Name	Alert Name	Description
Abnormal File Access Time	Non-Standard Hours	A user accessed a file at an abnormal time.
Abnormal File Access Permission Change	Mass Permission Changes	A user changed multiple share permissions.
Abnormal File Access Event	Abnormal File Access	A user accessed a file abnormally.
Multiple File Access Permission Changes	Mass Permission Changes	A user changed multiple file share permissions.
Multiple File Access Events	Snooping User	A user accessed multiple file share permissions.
Multiple Failed File Access Permission Changes	Mass Permission Changes	A user failed multiple times to change file access permissions.
Multiple Failed File Access Events	Snooping User	A user failed multiple times to access a file.
Multiple File Open Events	Snooping User	A user opened multiple files.
Multiple Folder Open Events	Snooping User	A user opened multiple folders.
Multiple File Delete Events	Abnormal File Access	A user deleted multiple files.
Multiple File Rename Events	Mass File Rename	A user renamed multiple files.
Excessive Number of Files Moved from File System	Data Exfiltration	A user moved multiple files from a shared drive.
Excessive Number of Files Moved to File System	Data Exfiltration	A user moved multiple files to a shared drive.

Table 3. Change Auditor for Active Directory

Indicator Name	Alert Name	Description
Abnormal Active Directory Change Time	Non-Standard Hours	A user made Active Directory changes at an abnormal time.
Abnormal Active Directory Change	Abnormal AD Changes	A user made an abnormal change to AD attribute.
Abnormal Site	Abnormal Site Access	A user logged on from a computer in an abnormal site.
Multiple Member Additions to Enterprise Critical Groups See the list of groups in the Change Auditor for Active Directory Event Reference Guide for "Member Added to Critical Enterprise Group”.	Mass Changes to Critical Enterprise Groups	A user successfully made multiple changes to sensitive groups.

Table 3. Change Auditor for Active Directory

Indicator Name	Alert Name	Description
Multiple Group Membership Changes	Mass Changes to Groups	A user successfully made multiple changes to groups.
Multiple Account Management Changes	Abnormal AD Changes	A user successfully made multiple Active Directory changes.
Multiple User Account Management Changes	Abnormal AD Changes	A user successfully made multiple sensitive Active Directory changes.
Multiple Failed Account Management Changes	Abnormal AD Changes	A user failed to make multiple Active Directory changes.
Admin Password Changed	Admin Password Change	An admin's password was changed.
User Account Enabled	Sensitive User Status Changes	A user enabled another user account.
User Account Disabled	Sensitive User Status Changes	A user disabled another user account.
User Account Unlocked	Sensitive User Status Changes	A user unlocked another user account.
User Account Type Changed	Sensitive User Status Changes	A user account type was changed by another user account.
User Account Locked	Sensitive User Status Changes	A user locked another user account.
User Password Never Expires Option Changed	Sensitive User Status Changes	A user password policy was changed by another user account.
User Password Changed by Non-Owner	Sensitive User Status Changes	A user's password was changed by non-owner.
User Password Changed	Sensitive User Status Changes	A user changed the password for another user account.
Member Added to Critical Enterprise Group	Elevated Privileges Granted	A user was added to a privileged group.

Table 4. Change Auditor for Logon Activity

Indicator Name	Alert Name	Description
Abnormal Logon Time	Non-Standard Hours	A user logged on at an abnormal time.
Abnormal Remote Computer	User Login to Abnormal Remote Host	A user attempted to remotely access an abnormal computer.
Abnormal Computer	User Login to Abnormal Host	A user attempted to access an abnormal computer.
Multiple Successful Authentications	Multiple Logons by User	A user logged on multiple times.
Multiple Failed Authentications	Multiple Failed Logons	A user failed to log on multiple times.
Logged into Multiple Domains	User Logins to Multiple AD Sites	A user attempted to log on to multiple domains.
Logged onto Multiple Computers	User Logged into Multiple Hosts	A user attempted to log on from multiple computers.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.