Quest®

Quest® Change Auditor Threat Detection 7.0

Deployment 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

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

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

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

Change Auditor Threat Detection Deployment Guide
Updated - March 2019
Software Version - 7.0

Contents

1

Deploying Threat Detection

- Introduction to Change Auditor Threat Detection
- Who should have input on the deployment plan?
- Components and workflow
- Requirements and prerequisites
- Events to configure
- Deploying a Threat Detection server on ESX
- Deploying a Threat Detection server on Hyper-V
- Upgrading the Threat Detection server
- Creating a Threat Detection configuration
- Reviewing configuration status
- Removing a configuration
- Maintaining the Change Auditor database size
- Historical events and your baseline calculations

Introduction to Change Auditor Threat Detection

To 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. The users with the highest risk scores are then highlighted in the Threat Detection dashboard, enabling you to prioritize your response and adjust policies to strengthen your organization's security and regulatory enforcement.

For details about using the Threat Detection dashboard see the Change Auditor Threat Detection User Guide.

This guide gives information about how Change Auditor integrates with the Threat Detection server to process event data. It is intended for administrators who are responsible for the implementation, deployment, and monitoring of the Change Auditor Threat Detection deployment and configuration.

Who should have input on the deployment plan?

A complete deployment plan requires the combined effort of the resources within your organization who are responsible for information security, such as:

- Chief Information Security Officers who understand the complexities of the enterprise's IT infrastructure and are responsible for the overall handling of key vulnerabilities. Change Auditor provides data to help them deliver security updates and communications.
- Security architects who are responsible for building and overseeing the implementation of the network's security measures. They need to define the threat priorities for their environment.
- Database and network administrators who are responsible for the implementation, deployment, and monitoring of the Change Auditor Threat Detection configuration.
- Auditors and network administrators who are responsible for reviewing the potential threats, optimizing the system by inputting feedback, and prioritizing and investigate the most serious threats.

Components and workflow

Change Auditor sends events in real time to the Threat Detection server to be used for analysis based on calculated user behavior baselines.

See the Change Auditor Threat Detection User Guide for details on Threat Detection concepts and terms.

To enable Threat Detection:

1. Apply the required licenses. (Change Auditor Threat Detection and any required Change Auditor auditing modules.) If you are using more than one coordinator, apply the license to all of them. To verify that a license is applied, right-click the coordinator icon in the system tray and select Licensing.
2. Configure required events for Threat Detection. See Events to configure.
3. Deploy the Threat Detection server on a virtual computer. See Deploying a Threat Detection server on ESX and Deploying a Threat Detection server on Hyper-V.
4. Configure Change Auditor to send collected event data to the Threat Detection server. See Creating a Threat Detection configuration.
5. Login to the Threat Detection dashboard to see the alerts and data. See the Threat Detection User Guide for information about navigating the dashboard and using the data to secure your environment.

Requirements and prerequisites

For a successful deployment, ensure that your environment meets the minimum system requirements.

The Threat Detection server deployed on VMWare ESX is available in both 8 and 16 cores versions.
For a Hyper-v deployment, a single server is available and you select the number of cores during the deployment.

NOTE: The number of cores impact the length of time it takes to process historical audit data and build the baseline. 16 cores is recommended, 8 cores can be used if processing less than 5 million events per day.

Deployment on VMWare ESX

- VMWare ESXI version 5.5 and above which is managed by VMware Vcenter 5.5 and above
- The following vSphere clients are supported:
  - With ESX 5.5 - vSphere Windows client.
  - With ESX 6.0 - vSphere Flash client.
  - With ESX 6.5 - vSphere Flex client, vSphere HTML5 client.
- Small and medium sized enterprise edition OVA:
  - OVA file size: ~10GB
  - CPU: 8 cores, Minimal 2.3 GHz, Recommended 2.4 GHz
  - RAM: 64 GB
  - I/O: 500 MB/sec
  - Disk: SAS 320 GB, SAS 930 GB
- Large sized enterprise edition OVA:
  - OVA file size: ~10GB
  - CPU: 16 cores, Minimal 2.3 GHz, Recommended 2.4 GHz
  - RAM: 64 GB
  - I/O: 500 MB/sec
  - Disk: SAS 320 GB, SAS 930 GB

Deployment on Microsoft Hyper-V

- Hyper-V host which running on Windows server 2016
- Threat Detection server requirements:
  - Template size: ~10 GB
  - CPU: 8 or 16 cores, Minimal 2.3 GHz, Recommended 2.4 GHz.
  - RAM: 64 GB
  - I/O: 500 MB/sec
  - Disk: SAS 320 GB, SAS 930 GB.

For all deployments:

- Obtain a static IP address for Threat Detection server and add DNS (A) record for it.
- Determine the number of historical days to use for your activity baseline. For information on how to determine the best amount for you, see Historical events and your baseline calculations.

Events to configure

NOTE: Consider Maintaining the Change Auditor database size when adding events for Threat Detection auditing.

Events from the following modules are used to build models and generate alerts:

Table 1. Events used for modeling and alerts

Module	Events
Change Auditor for Logon Activity	Authentication Activity events – these are the successful and failed interactive and remote interactive events (all enabled by default). Domain Controller Authentication events – Ensure that you enable the 'User authenticated through Kerberos" event. By default, it is disabled.
Change Auditor for Active Directory	User and group events (all enabled by default).
Change Auditor for Windows File Servers Change Auditor for EMC Change Auditor for FluidFS Change Auditor for NetApp	For optimal Threat Detection results, Quest recommends that you select file, folder, and share events that audit permission changes, create, delete, rename, and open actions during the template creation.

Maintaining the Change Auditor database size

Some of the events required for Threat Detection can be very noisy and take up significant space in the Change Auditor database. Once the events are sent to the Threat Detection server for analysis storage in the Change Auditor database is no longer needed.

To ensure the database maintains a manageable size, Quest recommends that you purge events older than 30 days.

Particularly noisy events are:

- User authenticated through Kerberos
- File and folder open

Deploying a Threat Detection server on ESX

To download the Threat Detection server go to https://support.quest.com/change-auditor/download-new-releases.

The Threat Detection server, which is a a version of Red Hat Enterprise Linux 7 (64 bit), is available as Open Virtual Appliance (OVA) file that must be deployed on VMWare ESXi using VMWare VSphere Client.

NOTE: Depending on the version of the ESXi, the deployment steps may be different. The below steps outline the process for vSphere Client version 6.5.

To deploy the Threat Detection server

1 Open vSphere client.

> **NOTE:** VMWare VSphere Client should be connected to VMWare vCenter not an individual ESXi host.

2 Select **Actions | Deploy OVF Template**.

3 Under **Select template**, choose **Local file**, browse for the OVA template, and click **Next**.

4 Under **Select name and location**, specify the name and inventory location for the deployed template and click **Next**.

5 On **Select a resource**, choose the destination computer for the OVA and click **Next**.

6 Under **Review details**, verify the OVF template details and click **Next**.

7 Under **Select Storage**, select the datastore for the configuration and the disk files and click **Next**. The **Thin Provision** option is recommended.

8 Under **Select networks**, choose a destination network for the virtual computer and select **Next.**

9 Under **Customize template**, enter the deployment properties for the Threat Detection sever.

Property	Description
Hostname	Fully qualified domain name of the Threat Detection server that has been registered in DNS. For example: hostname.yourcompany.com.
IP address	Static IPv4 address of the Threat Detection server.
Subnet mask	Subnet mask. For example: 255.255.255.0
Default gateway	Default gateway IP address.
DNS	DNS server IP address.
Integration password	Password required for the integration between Change Auditor and the Threat Detection server. The integration password is used during the Threat Detection configuration. The password must be 8-24 characters and can only include the following supported values: a-z, A-Z, 1-0, @,$. Maintain this password for use when creating the Threat Detection configuration.
Root password	Root password for the Threat Detection server. It must be 8-24 characters and can only include the following supported values: a-z, A-Z, 1-0, @,$.

10 Click **Next**.

11 Under **Ready to complete**, verify the information and click **Finish.**

12 Once the deployment in complete, power on the Threat Detection server.

Quest recommends that you take a snapshot of the newly deployed virtual server. This allows you to revert to a clean state without redeploying the server if you need to start over or re-create a configuration.

You are now ready to create a Threat Detection configuration in Change Auditor.

Deploying a Threat Detection server on Hyper-V

To optimize your server utilization and reduce costs, you can choose to deploy a virtual Threat Detection server using a Hyper-V virtual machine deployment.

The Threat Detection server, which is a a version of Red Hat Enterprise Linux 7 (64 bit), is available as .zip file that must be deployed on a Microsoft Hyper-V host environment by running a PowerShell script.

Begin by downloading the Change Auditor Hyper-V template (https://support.quest.com/change-auditor/download-new-releases) to the Hyper-V server.

To deploy the Threat Detection server

1 For remote deployments using an IP address to connect the Hyper-V server (in absence of a Hyper-V server DNS record), perform the following:

- Start the Windows Remote Management (WS-Management) /(WinRM) service.
- Run this PowerShell command as an administrator to add the Hyper-V server IP address to the TrustedHosts list:

```
set-item wsman:\localhost\Client\TrustedHosts -value <Your_Hyper-V_Host_IP_Address>
```

2 From the Change Auditor client browse to the DeployThreatDetectionHyper-VServer.ps1 deployment script. By default it is located here: C:\Program Files\Quest\ChangeAuditor\Client\PowerShell Sample Scripts.

> **NOTE:** You can run the script on the same computer as where you are deploying the Threat Detection server (local deployment) or from any other computer in the network (remote deployment).

3 Right-click the deployment script and select **Run with PowerShell**.

4 Enter the deployment properties for the Threat Detection sever.

Property	Description
Hostname or IP address	The hostname or IP address of the Hyper-V server.
Hyper-V administrator	The account used to deploy the Threat Detection server. The user specified must be a Hyper-V administrator.
Hyper-V password	Password for the Hyper-V administrator.
Threat Detection Hyper-V template location	Location of the Threat Detection Hyper-V template zip file on the Hyper-V server.
Folder for the virtual machine HD files	The path of the folder where the Threat Detection server's hard disk files will be installed on the Hyper-V server during deployment. If the folder does not exist, it will be created.
Folder for the virtual machine configuration files	The path of the folder where the Threat Detection server's configuration files will be installed on the Hyper-V server during deployment. If the folder does not exist, it will be created.
Virtual machine name	The name of the Threat Detection server in the Hyper-V management console.
Number of virtual machine cores	The number of machine cores (8 or 16). **NOTE:** 16 cores is recommended, 8 cores can be used if processing less than 5 million events per day.
Network adapter	The script returns the list of available network adapters for the Threat Detection server. Select one from the list.

Property	Description
Hostname	Fully qualified domain name of the Threat Detection server registered in DNS. For example: hostname.yourcompany.com
IP address	Static IPv4 address of the Threat Detection server.
Subnet mask	Subnet mask for the Threat Detection server. For example: 255.255.255.0
Default gateway	IP address of the default gateway for the Threat Detection server.
DNS	DNS server IP for the Threat Detection server.
Integration Password	Password required for the integration between Change Auditor and the Threat Detection server. The integration password is used during the Threat Detection configuration. The password must be 8-24 characters and can only include the following supported values: a-z, A-Z, 1-0, @,$. Maintain this password for use when creating the Threat Detection configuration.
Root Password	The root password. It must be 8-24 characters and can only include the following supported values: a-z, A-Z, 1-0, @,$.

5 Review and confirm the Threat Detection server settings. To continue enter **Yes**. To change the properties, enter **No**.

The Hyper-V Threat Detection server will now be deployed. This may take several minutes.

6 If you are using System Center Virtual Machine Manager (SCVMM) to manage your Hyper-V hosts, refresh the Virtual Machine Manager (VMM) dashboard to display the Threat Detection server.

a Open the Virtual Machine Manager (VMM) dashboard. Under **VMs and Services**, select **All Hosts.**

b Right-click the Hyper-V host where the Threat Detection server is hosted and click **Refresh Virtual Machines**.

Quest recommends that you take a checkpoint of the newly deployed virtual server. This allows you to revert to a clean state without redeploying the server if you need to start over or re-create a configuration.

You are now ready to create a Threat Detection configuration in Change Auditor. See Creating a Threat Detection configuration.

NOTE: The Threat Detection server uses Dynamic MAC address for its network adapter. If you are using SCVMM to manage your Hyper-V hosts and you plan to move the Threat Detection server from one Hyper-V server to another, ensure that after moving, the server is allocated an unused MAC address or alternatively change the address to a static MAC address.

Hyper-V resource control settings

After you have deployed the Threat Detection server, you can select to adjust the Hyper-V processor settings to reserve an amount of processor capacity for a specific virtual machine or, alternatively, configure which virtual machine is given priority in your environment.

Change Auditor's deployment of a Threat Detection server uses the system defaults unless otherwise specified. To change the values for these properties, open the virtual machine's setting, select the Processor, and configure the associated resource control setting.

Table 2. Hyper-V CPU settings

Property	Description	Best Practice
Reserve	The percentage of logical processor resources that are reserved for the Threat Detection server. For example, if the host machine has 8 logical CPUs, then setting this value to 25% would reserve 2 of those CPUs for the Threat Detection server. The default value is dynamic based on the CPU.	Set this value to 100% to ensure the Threat Detection server will have access to the resources that it requires.
Relative Weight	Determines how the CPU is distributed when you want to set which virtual machine takes priority when there is contention for the processor. For example, a virtual machine with a relative weight of 200, receives twice as much processor time than one set to 100. The default value for all virtual machines is 100.	The weight ranges from 1-10000. To give the Threat Detection server priority, assign it with a higher weight than all other computers in your environment.

Upgrading the Threat Detection server

For the Threat Detection system to function properly, the Threat Detection server must be compatible with the installed version of Change Auditor. To see if your Threat Detection server is compatible or if an upgrade is required see Reviewing configuration status.

You can upgrade your existing Threat Detection server by running an update script and a series of configuration commands on the Threat Detection server. This will ensure that your existing configuration and Threat Detection information is maintained.

To upgrade the Threat Detection server:

- Download the update package (UpdateTDServer-<Change Auditor version>.zip) from https://support.quest.com/change-auditor/download-new-releases.
- Log on to the Threat Detection server and upload the update package to the server. For details see, Upload the update package the Threat Detection server.
- Upgrade the Threat Detection server by running the update script. For details see, Upgrade the Threat Detection server.
- Join the Threat Detection server to the coordinator's domain to enable single sign-on capability to the Threat Detection dashboard. For details see, Join the Threat Detection server to the coordinator's domain.
- Configure a service account that is used by the Treat Detection server for communicating with Active Directory to verify single-sign on user access to the dashboard. For details see, Configure the service account.

IMPORTANT: Quest recommends that you take a snapshot (for ESX deployments) and a checkpoint (for Hyper-v deployments) of the Threat Detection server before beginning the upgrade process. This allows you to revert to the initial state.

For details see the vSphere documentation and the Microsoft documentation.

Upload the update package the Threat Detection server

To upload the update package the Threat Detection server

1. Log on to the Threat Detection server through your preferred SFTP client with the username ‘presidio’ and the integration password specified during the Threat Detection server configuration.

   NOTE: Ensure your SFTP client transfer setting is set to Binary before uploading the zip package.

2. Upload the UpdateTDServer-<Change Auditor version>.zip file to the ‘/home/presidio’ directory.

Upgrade the Threat Detection server

To upgrade the server:

1. Log on to the Threat Detection server with the username ‘presidio’ and the integration password specified during the Threat Detection server configuration.
2. Run ‘cd /home/presidio/’ to change the directory to the presidio home directory.
3. Run 'unzip UpdateTDServer-<Change Auditor version>.zip' to unzip the update package.
4. Run ‘cd /home/presidio/UpdateTDServer-version’ to change to the unzipped directory.
5. Run ‘./update.sh’ to run the upgrade script.
6. When prompted, enter the integration password.

   The server will now be upgraded; this could take up to 15 minutes to complete.

   A log file detailing the results of the update is generated after the update is complete. The log file is located here: /home/presidio/update logs and is called UpdateTDServer-YYYY-MM-DD.log. (Where the date is the date of the update.).

Join the Threat Detection server to the coordinator’s domain

To join the server to the coordinator’s domain:

1. While logged on to the Threat Detection server, open a command prompt.
2. Run ‘cd /opt/quest/bin’ to change the directory to the Quest tools directory.
3. Run 'sudo ./vastool -u < User SamAccountName> join <domain FQDN>' to join the server to the coordinator’s domain.

   NOTE: The user must be a domain administrator or have been delegated the following tasks using the Active Directory Delegation Control wizard:

   - Create, delete, and manage user account.
   - Join a computer to the domain.

4. When prompted for the “Password for presidio”, enter the integration password.
5. When prompted for the password for the domain, enter the password of the user account specified in step 3.

   The Threat Detection server will now be joined to the domain.

6 Run './vastool info domain' to verify that the server is joined to the domain. The command will return the domain for the Threat Detection server.

Configure the service account

To configure the service account:

1 While logged on to the Threat Detection server with the username 'presidio' and the integration password specified during the Threat Detection server configuration open a command prompt.

2 Run 'cd /opt/quest/sbin' to change the directory to the Quest sbin tools directory.

3 Run 'sudo ./setup-mod_auth_vas4' to create the service account.

You will now be prompted with a series of questions, accept the default answers for the prompts.

4 When prompted for a sufficiently privileged domain account, enter the domain administrator account (SAMAccountName).

5 Accept the default answer to change group of /etc/opt/quest/vas/HTTP.keytab to Apache.

6 Specify any SPN aliases (if required) or Enter to finish.

7 Run 'sudo service httpd restart' to restart the httpd service to finish the configuration.

The service account will now be created in Active Directory.

8 Verify that the service account has been created in the Computers container in the same domain as the Threat Detection server. The service account will be a user account with the same name as the Threat Detection server with "HTTP" appended to it.

Creating a Threat Detection configuration

A Threat Detection configuration must be created to view activity, receive alerts, and analyze anomalies on the dashboard.

When a configuration is created, the Threat Detection server is automatically joined to your coordinator's domain and an associated service account is created. This is required to enable single-sign on to the Threat Detection dashboard.

To create a Threat Detection configuration

1 From Change Auditor select **Administration Tasks | Configuration | Threat Detection**.

2 Enter the Threat Detection server fully qualified domain name and integration password you created when deploying the Threat Detection server.

3 Enter the account used to join the Threat Detection server to your coordinator's domain. (Use this format for the account: <Domain>\<User Name>.)

> **NOTE:** The user must be a domain administrator or have been delegated the following tasks using the Active Directory Delegation Control wizard:
>
> - Create, delete, and manage user account.
> - Join a computer to the domain.

4 Select how many days of historical events should be sent to Threat Detection server. For information on how to determine the best amount for you, see Historical events and your baseline calculations.

5 Select **Apply Changes**.

Reviewing configuration status

The status of the Threat Detection configuration is displayed on the configuration page.

To see the Threat Detection configuration status

1 Select **Administration Tasks | Configuration | Threat Detection**.

2 Click **Refresh**.

Table 3. Available configuration states

State	Description
Configured	The Threat Detection server is properly configured.
Not configured	The Threat Detection server is not configured. See Creating a Threat Detection configuration. **NOTE:** If you see this status after removing a configuration and want to configure Threat Detection again, see Removing a configuration for details.
Update is required	An update is required on the Threat Detection server. See Upgrading the Threat Detection server.
License required	A valid Threat Detection license has not been applied.
License expired	The Threat Detection license has expired.

Configured server deployment details

For a configured server, the following deployment details are displayed:

- State of the configuration.
- How many historical events have been sent to Threat Detection server.
- Status of the Threat Detection server.
- Status of the data processing. For example, building baseline.
- Threat Detection server version.
- Threat Detection subscription ID.
- Starting point in time for events to send.
- Subsystems that contain the event data that is being sent.
- Whether the Threat Detection subscription is enabled.
- How often how often (in milliseconds) events are sent.
- Interval (in milliseconds) that a heartbeat check is made for the configuration.
- Batch size. (The maximum number of events to include in a single notification message.)
- Url for notifications.
- Url for heartbeat notifications.
- When the last event was sent.
- Last event response (For example OK, HTTP 429 - Too many events being sent, and HTTP 401 - Unauthorized access.)
- When the last heartbeat was sent.

- When the last heartbeat response. (For example OK, HTTP 429 - Too many events being sent, and HTTP 401 - Unauthorized access.)
- Number of events sent.
- Number of batches sent.
- Number of heartbeats sent.
- Time of the event that was last sent.
- List of coordinators permitted to send events.
- The coordinator that is sending events. If the subscription is disabled, this is the last coordinator that sent events.

Removing a configuration

Deleting the configuration only removes configuration information from Change Auditor. It does not remove data or configuration on the Threat Detection server.

If you are removing the configuration as a part of a clean up process, you can delete the Threat Detection server after removing configuration.

If you are removing the configuration and plan to start over, you can either revert to a snapshot from a previously deployed (but not configured) Threat Detection server or deploy a new Threat Detection server.

NOTE: When you join the server to the domain during configuration, Change Auditor creates a computer and service account in the domain required for Integrated Windows Authentication. The computer and service account must be removed manually from the domain when a configuration is removed.

To remove a Threat Detection configuration

1. Select **Administration Tasks | Configuration | Threat Detection**.
2. Click **Remove Configuration**.

   This removes the Threat Detection configuration from Change Auditor.

Historical events and your baseline calculations

Before the Threat Detection server can generate alerts, it needs to establish user behavior baseline. The baseline is built by processing 30 days of historical or real time events. Refer to the Change Auditor Threat Detection User Guide for information about baseline modeling.

When you create the Threat Detection configuration, you can specify how many days of historical events should be sent to the Threat Detection server to create the baseline.

NOTE: The baseline is more accurate if it is built using the exact configuration of events that you plan to analyze on an ongoing basis. If a new event is enabled after the initial baseline has been built (for instance, the User authenticated through Kerberos event) it may initially be treated as an anomaly as there is no history of it in the baseline.

Table 4. How to determine which type of events to use for a baseline

Type of events to use	When to use...
Real-time events (0 days) **NOTE:** It will take at least 30 days before you start seeing alerts in the Threat Detection dashboard.	• For a new installation of Change Auditor where no events have been collected. • If you just enabled events that need to be analyzed by Change Auditor Threat Detection.
Historical events (more than 0 days)	• If you have been collecting all events supported by Change Auditor Threat Detection. • If you are not purging any of the events supported by Change Auditor Threat Detection.

Use the following as guidance on the number of days to specify when you create your Threat Detection configuration:

- You should not specify more days than the number of days of events that exist in the Change Auditor database.
- You can enter between 1 and 90 days.
- If you specify less than 30 days, Threat Detection uses real time events to continue to build a baseline until 30 days of event have been analyzed.
- If you specify more than 30 days, the Threat Detection server starts generating alerts for any abnormal activity that happened after 30 days.

2

Threat Detection configuration commands

- Adding the PowerShell module
- Viewing available commands and help
- Connecting to Change Auditor
- Managing a Threat Detection configuration

Adding the PowerShell module

Change Auditor comes with a PowerShell module for you to use to manage your Threat Detection deployment. It is installed when you install the Windows client or a coordinator.

NOTE: Windows PowerShell version 3.0 or higher is required.

To import the Change Auditor PowerShell module:

1. Open a Windows PowerShell window and type the following at the Windows PowerShell command prompt:

   ```
   Import-Module <path>
   ```

   Where "<path>" is the file path for the ChangeAuditor.PowerShell.dll assembly found in the Change Auditor Windows client or Change Auditor coordinator folder.

2. To ensure that the module was added, type the following at the Windows PowerShell command prompt:

   ```
   Get-Module -All
   ```

   The registered PowerShell modules are listed.

Viewing available commands and help

- To view all available Change Auditor commands, enter:

  ```
  Get-Command -Module ChangeAuditor.PowerShell
  ```

- To view help on each command including the syntax, enter:

  ```
  Get-Help cmdletName
  ```

- To view an interactive command browser that shows you the layout of commands and the help for the commands, enter:

  ```
  Show-Command cmdletName
  ```

Threat Detection sample scripts

Change Auditor includes the following sample scripts to help you configure and manage Threat Detection:

- CreateThreatDetectionConfiguration.ps1
- GetThreatDetectionConfiguration.ps1
- ModifyThreatDetectionConfiguration.ps1
- RemoveThreatDetectionConfiguration.ps1

NOTE: By default they are located here: C:\Program Files\Quest\ChangeAuditor\Client\PowerShell Sample Scripts

Connecting to Change Auditor

- Connect-CAClient

Connect-CAClient

Most Change Auditor commands require a connection to a coordinator. You can make multiple connections to different coordinators or deployments in the same script as long as the version of Change Auditor is the same.

This connection can be assigned to a variable and used for any command that requires it. Use this command to search for a suitable coordinator in a Change Auditor installation and create a connection. Suitable coordinators are those which you have access to and can be located by searching through Active Directory service connection points.

NOTE: Connections are closed when the PowerShell session is ended or disconnected.

Table 1. Available parameters

Parameter	Description
-Credential (Optional)	Windows credentials specifying the user to connect to the Change Auditor installation. All operations using this connection will be authorized as this user. When not specified, the current client running PowerShell is used.
-CoordinatorConnectionPoint (Optional)	Specify to use a specific coordinator found from a previous call to Find-CACoordinators.
-SelectLocalCoordinator (Optional)	Create a connection to the local coordinator.
-InstallationName (Optional)	The installation name to connect to. If an installation cannot be found with this name, no connection is made. If more than one Change Auditor installation exists in the current forest, this parameter is mandatory. Omitting it results in a connection failure due to ambiguity.
-DomainName (Optional)	The name of the domain where the Change Auditor installation exists.
-ComputerName (Optional)	The computer to connect to.
-Port (Optional)	The port to connect to.
-WaitForServiceReady (Optional)	The number of seconds to wait for the connected coordinator service to be ready. **NOTE:** If not specified, when the Change Auditor coordinator is not ready for connections due to an in-progress install or upgrade, an error is returned. The maximum is 144,000 seconds, or 10 hours.

Example: Connect to the installation “XYZ” in the specified domain

```
Connect-CAClient –InstallationName ‘XYZ’ -DomainName 'DomainName.com'
```

Managing a Threat Detection configuration

- New-CAThreatDetectionConfiguration
- Get-CAThreatDetectionConfiguration
- Set-CAThreatDetectionConfiguration
- Remove-CAThreatDetectionConfiguration

New-CAThreatDetectionConfiguration

Use this command to create a Threat Detection configuration.

NOTE: When a configuration is created, the Threat Detection server is automatically joined to your coordinator's domain and an associated service account is created. This is required to enable single-sign on to the Threat Detection dashboard.

NOTE: Quest recommends that you use the sample script CreateThreatDetectionConfiguration.ps from Program Files\Quest\ChangeAuditor\Client\PowerShell Sample Scripts.

NOTE: When you create a new configuration, the underlying webhook subscription that is generated is marked as internal. This ensures that the required subscription cannot be removed from an existing configuration.

Table 2. Available parameters

Parameter	Description
-Connection	A connection obtained by using the Connect-CAClient command. See Connecting to Change Auditor.
-TDServer	The Threat Detection server fully qualified domain name.
-TDPassword	The password used to access the Threat Detection server. Use the integration password that was specified during the Threat Detection server deployment.
-DomainAdminCredential	The credentials required to join the Threat Detection server to your coordinator's domain to enable access to the dashboard using windows integrated authentication. **NOTE:** The user must be a domain administrator or have been delegated the following tasks using the Active Directory Delegation Control wizard: ▪ Create, delete, and manage user account. ▪ Join a computer to the domain.
-HistoricalDays (Optional)	The number of days of historical events to send to the Threat Detection server. For details, see Historical events and your baseline calculations.
-AllowedCoordinators (Optional)	The DNS or NetBIOS name of the coordinators permitted to send events. If none are specified, all coordinators installed at the time of configuration are permitted to send events. **NOTE:** The list order does not determine which coordinator is selected to send events.

Example: Creating a configuration

```
New-ThreatDetectionConfiguration -Connection $connection -TDServer
'ServerName.Domain.Com' -TDPassword $TDPassword -DomainAdminCredential
$DomainAdminCredential -HistoricalDays 30
-AllowedCoordinators @('machine1.domain.com','machine2.domain.com')
```

Get-CAThreatDetectionConfiguration

Use this command to view the Threat Detection configuration information and information about the associated subscription.

Table 3. Available parameters

Parameter	Description
-Connection	A connection obtained by using the Connect-CAClient command. See Connecting to Change Auditor.

Example: Review Threat Detection configuration details

```
Get-ThreatDetectionConfiguration -Connection $connection
```

Command output

The command returns the following information. For more information about some of these settings see the Change Auditor SIEM Integration Guide.

Table 4. Available configuration information

Setting	Description
TDServer	The Threat Detection server fully qualified domain name.
ConfigurationState	State of the configuration: • Configured: Threat Detection has been configured • Unconfigured: Threat Detection has not been configured • A valid Change Auditor Threat Detection license is required
HistoricalDays	How many days of historical events have been sent to Threat Detection server.
TDServerStatus	Status of the Threat Detection server: • Online • Offline
DataProcessingStatus	Status of the data processing. For example, building baseline.
TDServerVersion	Threat Detection server version.
TDSubscriptionId	Threat Detection subscription ID.
StartTime	Starting point in time for events to send.
Subsystems	Subsystems that have been selected for event sending.
TDSubscriptionEnabled	Whether the Threat Detection subscription is enabled.
NotificationInterval	How often how often (in milliseconds) events are sent.
HeartbeatInterval	Interval (in milliseconds) that a heartbeat check is made for the configuration.
BatchSize	Batch size. The maximum number of events to include in a single notification message.
NotificationUrl	Url for notifications.
HeartbeatUrl	Url for heartbeat notifications.
LastEventTime	When the last event was sent.
LastEventResponse	Last event response (For example OK, HTTP 429 - Too many events being sent, and HTTP 401 - Unauthorized access.)
LastHeartbeatTime	When the last heartbeat was sent.
LastHeartbeatResponse	The last heartbeat response. (For example OK, HTTP 429 - Too many events being sent, and HTTP 401 - Unauthorized access.)
EventsSent	Number of events sent.
BatchesSent	Number of batches sent.
HeartbeatsSent	Number of heartbeats sent.
BookmarkTime	Time the last event was sent.

Table 4. Available configuration information

Setting	Description
AllowedCoordinators	List of coordinators permitted to send events.
LastCoordinator	The coordinator that is sending events. If the subscription is disabled, this is the last coordinator that sent events.

Set-CAThreatDetectionConfiguration

Use this command to modify the list of allowed coordinators for the Threat Detection configuration.

Table 5. Available parameters

Parameter	Description
-Connection	A connection obtained by using the Connect-CAClient command. See Connecting to Change Auditor.
-AllowedCoordinators (Optional)	The DNS or NetBIOS name of the coordinators permitted to send events. If none are specified, all coordinators installed at the time of configuration are permitted to send events. **NOTE:** The list order does not determine which coordinator is selected to send events.

Example: Modifying a configuration

```
Set-CAThreatDetectionConfiguration -Connection $connection -AllowedCoordinators
@('machine1.domain.com','machine2.domain.com')
```

Example: To clear a previous list of allowed coordinators

```
Set-CAThreatDetectionConfiguration -Connection $connection -AllowedCoordinators @()
```

Remove-CAThreatDetectionConfiguration

Use this command to remove a Threat Detection configuration.

NOTE:

Deleting the configuration only removes configuration information from Change Auditor. It does not remove data or configuration on the Threat Detection server.

- If you are removing the configuration as a part of a clean up process, you can delete the Threat Detection server after removing configuration.
- If you are removing the configuration and plan to start over, you can either revert to a snapshot from a previously deployed (but not configured) Threat Detection server or deploy a new Threat Detection server.
- When you join the server to the domain during configuration, Change Auditor creates a computer and service account in the domain required for Integrated Windows Authentication. The computer and service account must be removed from the domain when a configuration is removed.

Table 6. Available parameters

Parameter	Description
-Connection	A connection obtained by using the Connect-CAClient command. See Connecting to Change Auditor.

Example: Remove the Threat Detection configuration

```
Remove-ThreatDetectionConfiguration -Connection $connection
```

3

Appendix: System Architecture

- Threat Detection system overview

Threat Detection system overview

The integration process to analyze events includes the following:

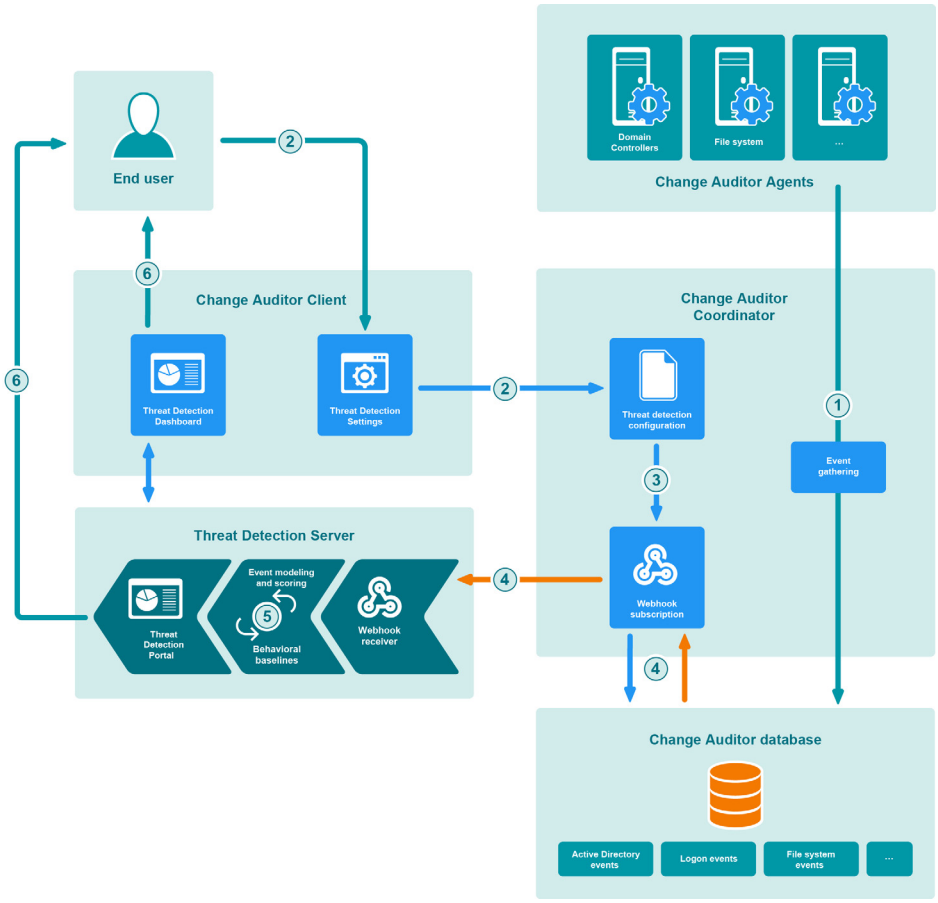

Figure 1. Event processing for Threat Detection

1. Change Auditor agents collect events from various systems and the coordinator writes the events into the database.
2. Users create a Threat Detection configuration using the Change Auditor client.
3. As part of the configuration, the coordinator creates the webhook subscription to send events to the Threat Detection server. The subscription contains information such as where to send events (the URL of the webhook receiver in the Threat Detection server), which events to include, and the coordinator responsible for event forwarding.
4. The designated coordinator continually queries events from the Change Auditor database and sends them to the webhook receiver in the Threat Detection server.
5. Threat Detection server performs event modeling and scoring.
6. Threat indicators, alerts, and risky users are displayed in the Threat Detection dashboard.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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.