

# Change Auditor クイックガイド

# 目次

- [はじめに](#)
- [インストール](#)
- [Change Auditor の必須コンポーネントとインストール要件](#)
- [Change Auditor ソフトウェアのダウンロード](#)
- [Change Auditor のインストール](#)
- [Change Auditor Coordinator のインストール](#)
- [Change Auditor Client のインストール](#)
- [クライアントの開始](#)
- [エージェントのデプロイ](#)
- [Active Directory の監査](#)
- [Active Directory の変更とクエリ](#)
- [Windows File System の監査](#)
- [File Systemのテンプレート設定](#)
- [Windows File System の変更の監査例](#)

# はじめに

このガイドはChange Auditor のインストールおよび基本的な操作手順を説明します。  
また、検証環境での利用を目的としたガイドです。



# インストール

# Change Auditor の必須コンポーネントとインストール要件

- Change Auditorのインストールには次の4つのコンポーネントが必須となります。
  - Change Auditor Client (コンソール)
  - Change Auditor Coordinator (クエリの管理)
  - Change Auditor Agent (監査対象のシステムのログを記録)
  - SQL Server Database
  
- 必要な権限
  - SQL Server Database : dbcreator ロール
  - Change Auditor coordinator : Windows 管理者およびDomain管理者グループのメンバー
  - Change Auditor Clientのインストール: Windows管理者

詳細は下記リリースノート中のSystem Requirements の項目を参照ください。

<https://support.quest.com/ja-jp/technical-documents/change-auditor/7.1.1/release-notes/2#TOPIC-1564232>

# Change Auditor ソフトウェアのダウンロード

ソフトウェアはサポートポータル（ソフトウェアのみ）、もしくは無償評価版（トライアルライセンス）のリンクからダウンロードします。

サポートポータルサイト

<https://support.quest.com/ja-jp/>

← → ↻ support.quest.com/ja-jp/

## Questサポート

サポートが必要な製品名を以下に入力し選択してください

製品名を入力してください（最初の2文字を入力すると候補が選択できます）

すべて見る

サポート契約の更新

最近表示した製品: Recovery Manager for AD Disaster Recovery Edition Change Auditor Metalogix Essentials for Office 365



ナレッジベース  
問題の  
トラブルシューティング



コミュニティフォーラム  
仲間と  
交流する



ソフトウェアのダウンロード  
新しいリリースやホットフィックスのダ  
ウンロード



技術文書  
リリースノート、ガイド、およびマニ  
ュアルを参照する

ホーム > サポート > ソフトウェアのダウンロード > Change Auditor

## Change Auditor - ソフトウェアのダウンロード

お使いのソフトウェア、パッチ、ユーティリティやホットフィックスを見つけるためにフィルターしてください。 [違う製品を選ぶ](#)

7.1.1（製品の最新モデル/バージョン）  
すべての項目

現在有効のサポート保守契約をお持ちのお客様は、以下の関連するインストールをダウンロードすることができます

Change Auditor Maintenance	リリース日	ダウンロード
Change Auditor 7.1.1 Full Maintenance Release (build 7.1.1.20087)	2021/05/10	<a href="#">↓</a>

トライアル

<https://www.quest.com/jp-ja/trials/#%20>

Quest

製品

ソリューション

サポートとサービス

パートナー

会社情報

無料評価版

お見積りのご依頼

ダウンロードトライアルとフリーウェアのソフトウェア  
ビジネスの現状に適応した  
製品の問題のトラブルシューティングにかかる時間を節約し  
評価版のA-Zリスト  
バージョンを早く掌握

A B **C** D E F G H I J K L M N O P Q R S T U V W X Y Z

C

### Change Auditor for Active Directory

あらゆる変更や日々のシステム修正を迅速に追跡し、確認

無料トライアルをダウンロード

今すぐお問い合わせ

### Change Auditor for Active Directory Queries

Windowsファイルサーバのリアルタイムなシステム変更のすべてを追跡、監視し、レポートを受信

無料トライアルをダウンロード

今すぐお問い合わせ

### Change Auditor for EMC

お使いのEMC NASデバイスに関するファイルアクティビティと権限に関連する全イベントを監査

無料トライアルをダウンロード

今すぐお問い合わせ

### Change Auditor for Exchange

Exchangeに対する、重要なグループ、メールボックス、パブリック/プライベートの変更をすべて記録します。

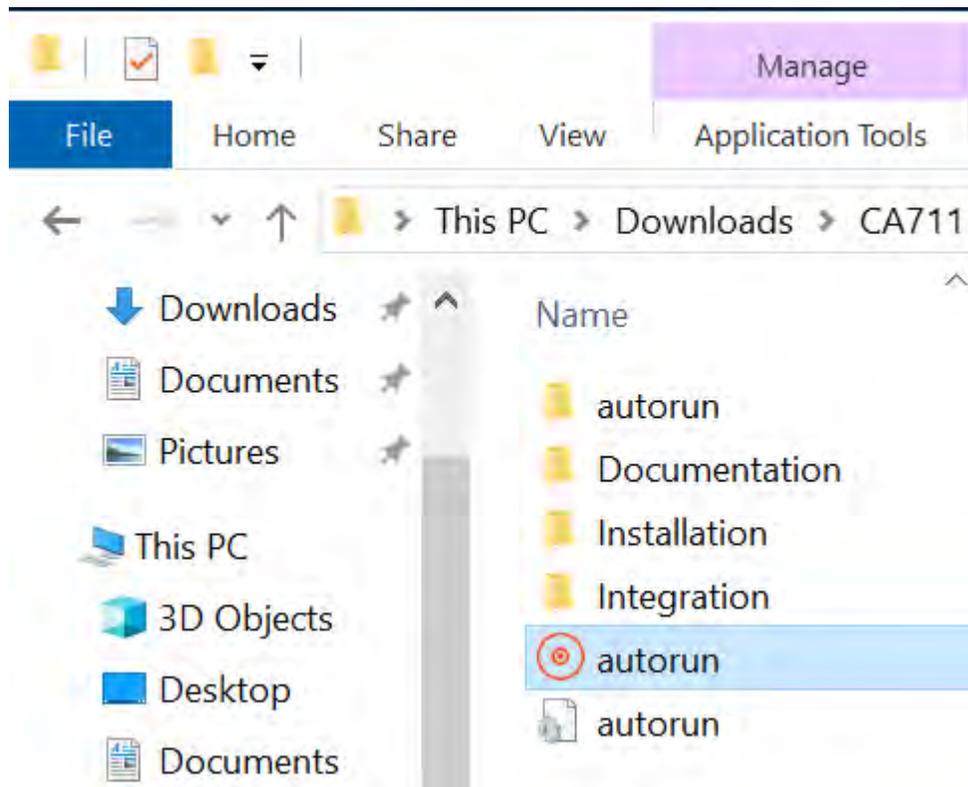
無料トライアルをダウンロード

今すぐお問い合わせ

[目次に戻る](#)

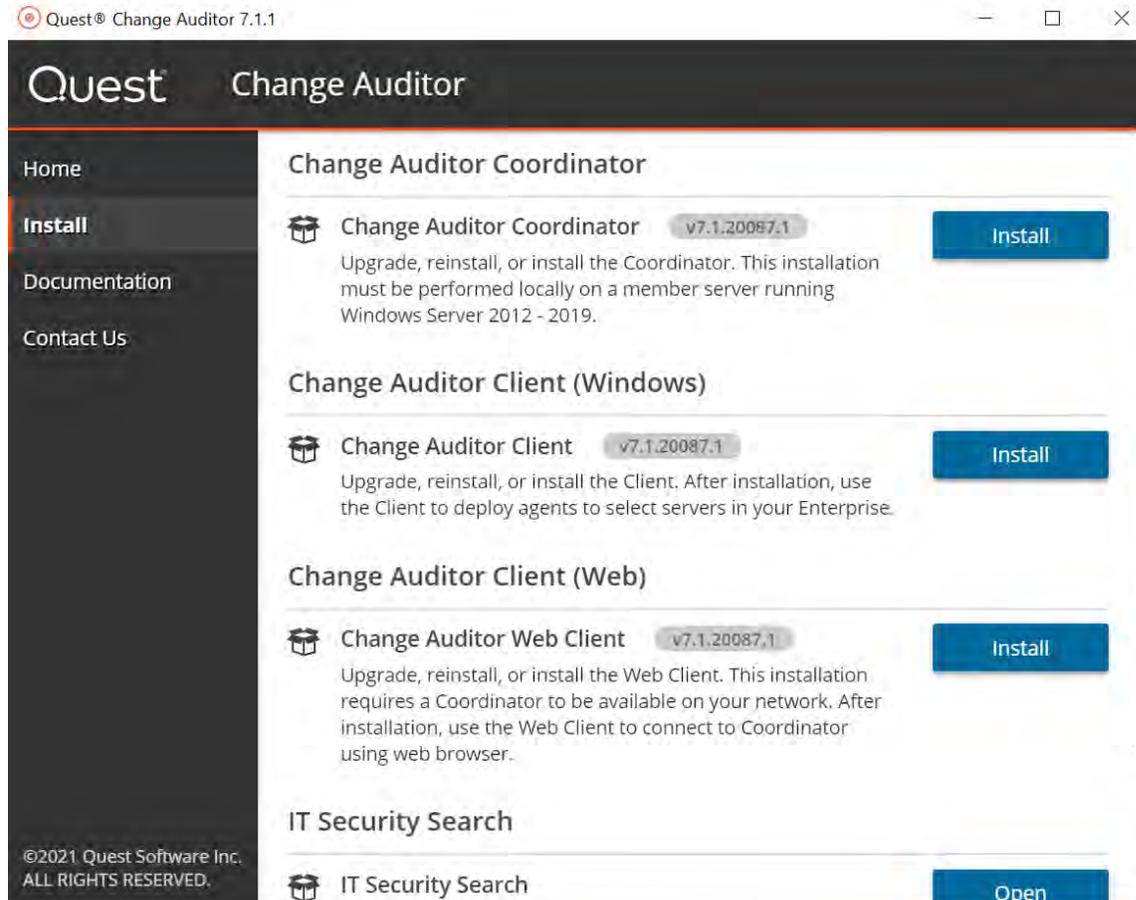
# Change Auditor のインストール

このガイドではCoordinator, Client, およびSQL serverを同じWindows OSにインストールするシナリオを説明します。



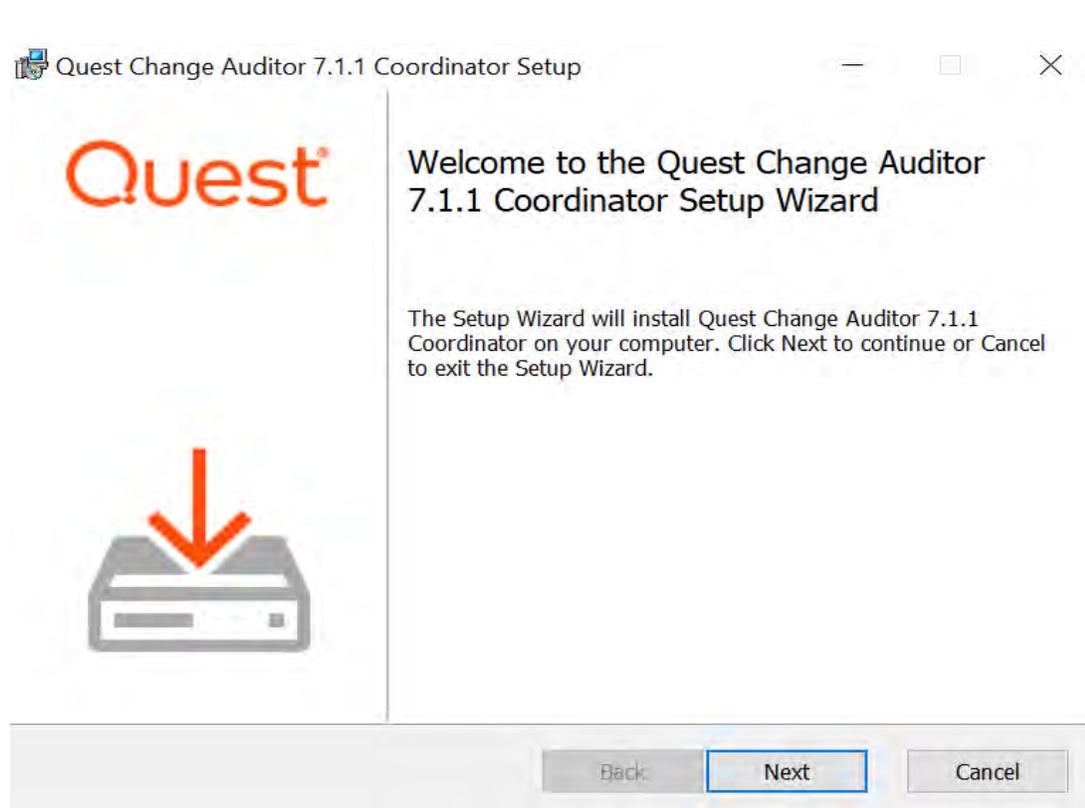
autorunをクリックしてウィザードを起動します。

# Change Auditor Coordinator のインストール

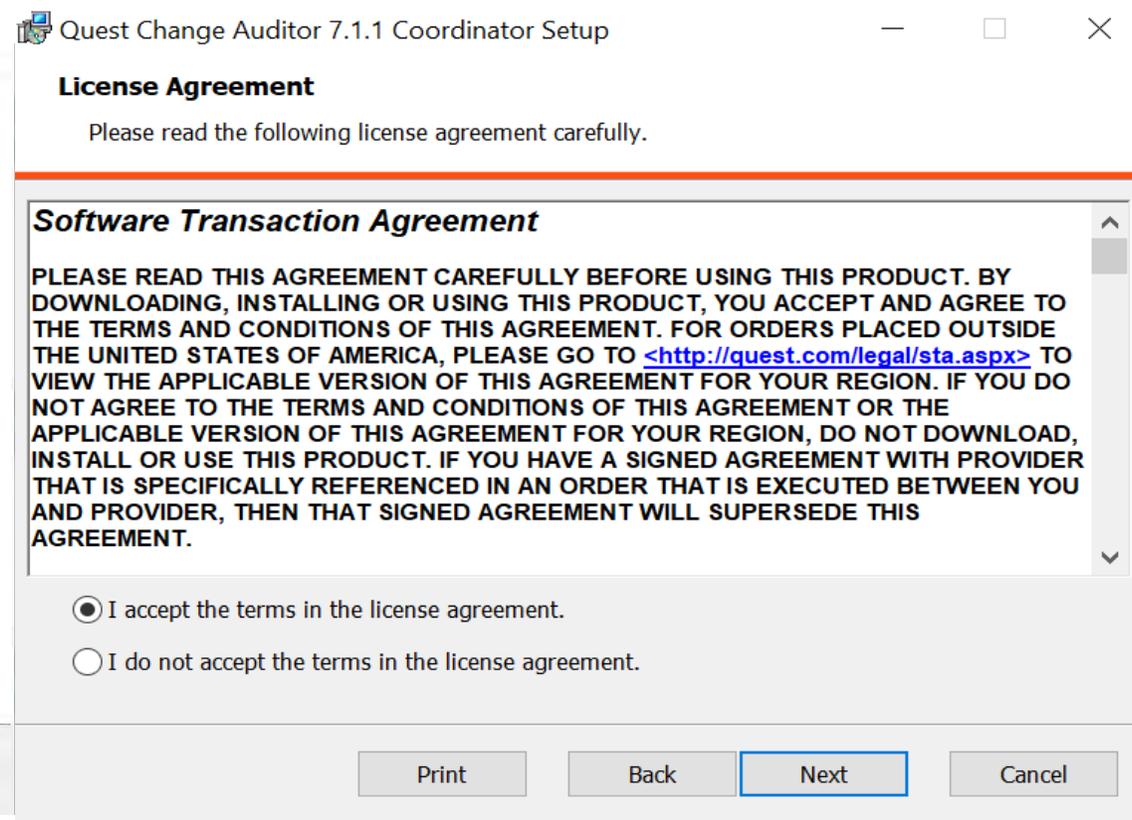


Change Auditor Coordinator のInstallボタンを選択します。

# Change Auditor Coordinator のインストール

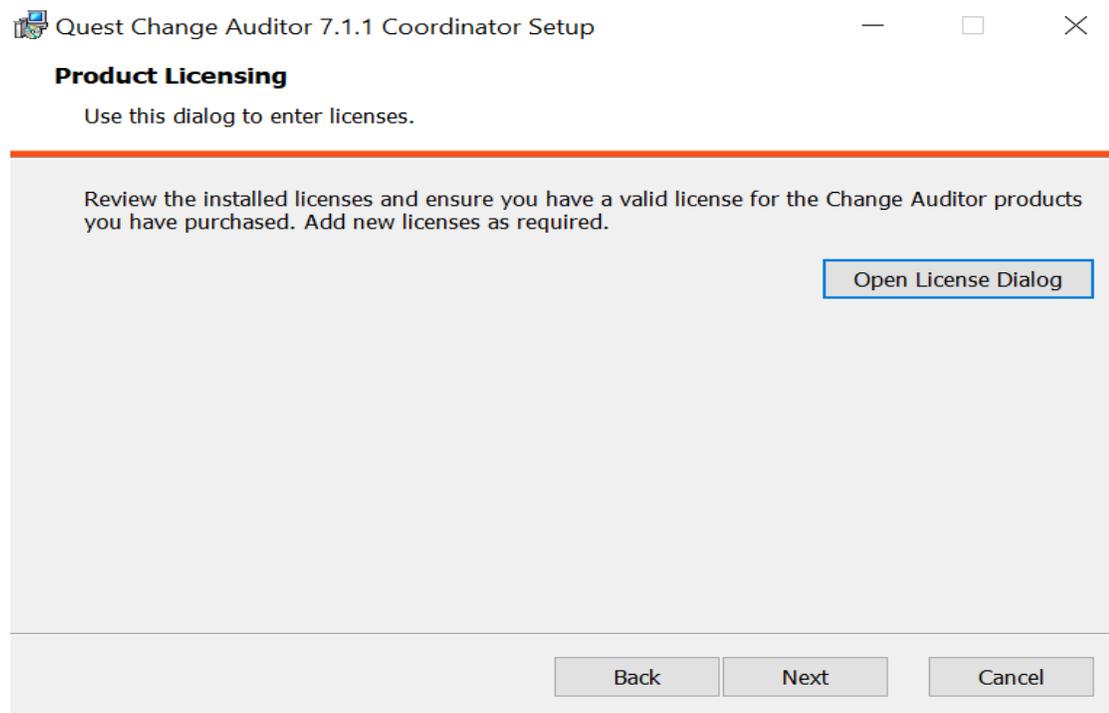


Nextをクリックして次に進みます。

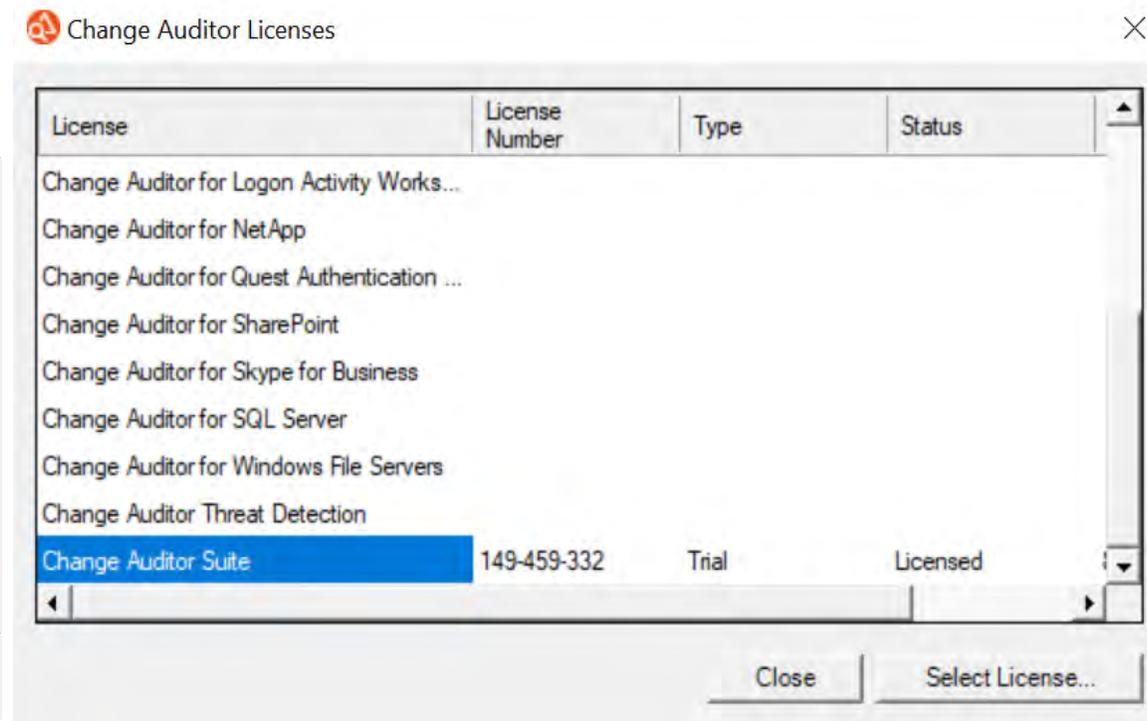


License Agreement でI accept... を選択して次に進みます。

# Change Auditor Coordinator のインストール

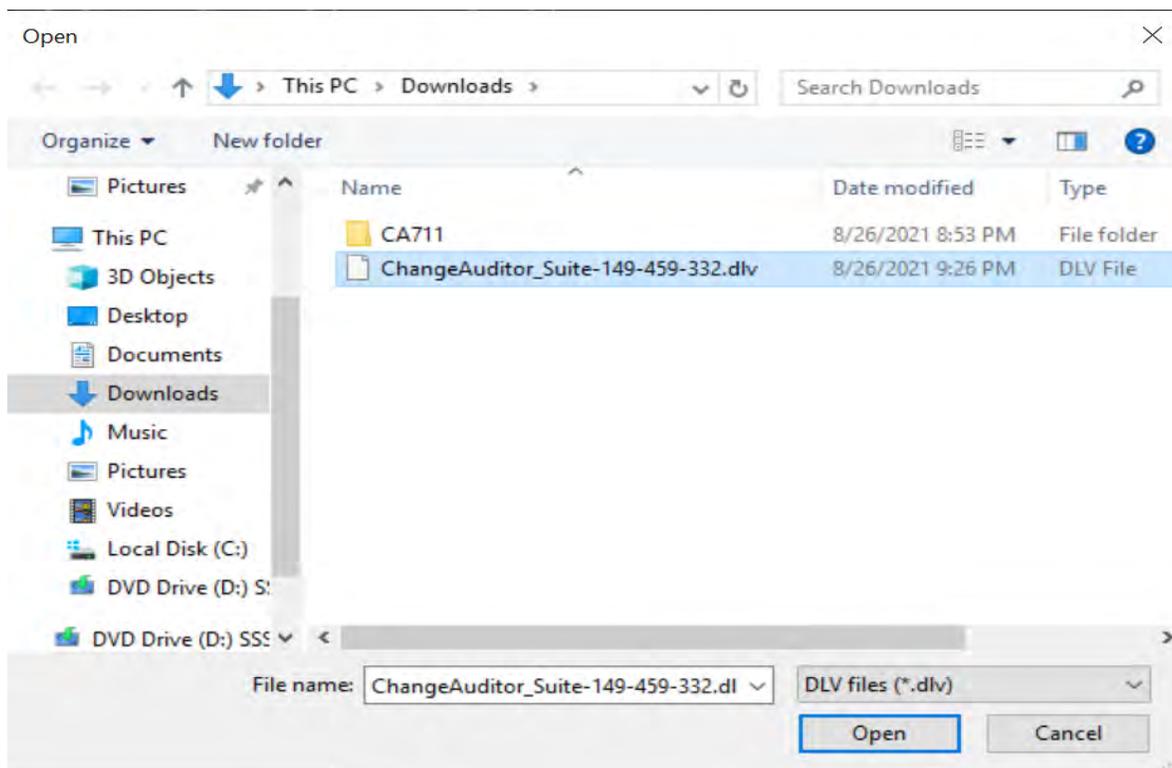


追加したいライセンスを選択し、Select License ボタンをクリックします。

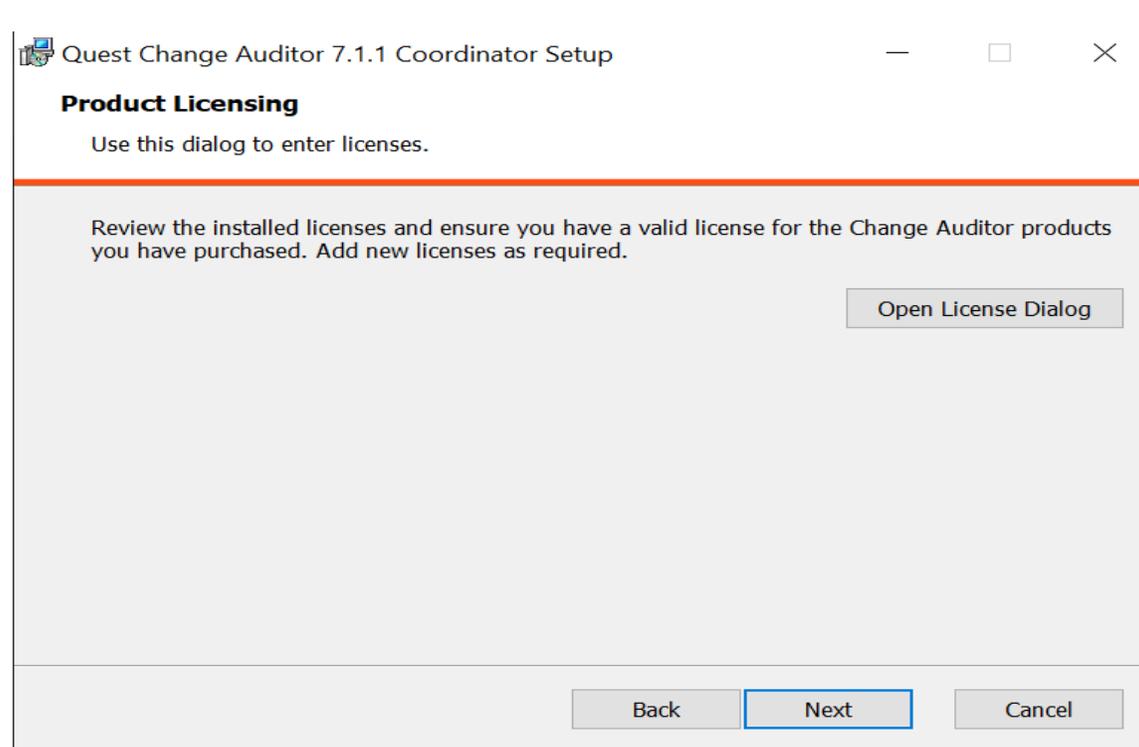


Open License Dialogボタンをクリックします。

# Change Auditor Coordinator のインストール



ライセンスファイル (.dlv) を選択します。



Nextをクリックして次に進みます。

# Change Auditor Coordinator のインストール

Quest Change Auditor 7.1.1 Coordinator Setup

### Installation Name

Specify the unique name to identify this installation.

You must provide a Change Auditor Installation Name which uniquely identifies this installation within your Active Directory environment. Use the Browse button to find existing Change Auditor installations.

By selecting an existing Change Auditor installation, you are joining this component to the installation. Use the default if you plan to have only one installation in your Active Directory forest.

Change Auditor Installation Name:

Back Next Cancel

Change Auditor Coordinator前を入力し、次に進みます。

Quest Change Auditor 7.1.1 Coordinator Setup

### Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Quest Change Auditor 7.1.1 Coordinator to:

Back Next Cancel

インストールの場所を指定して次に進みます。

[目次に戻る](#)

# Change Auditor Coordinator のインストール

Quest Change Auditor 7.1.1 Coordinator Setup

### SQL Server Information

Specify SQL server and logon information.

SQL Server and instance:

Name of database catalog:

Connect using:

- Azure Active Directory authentication
- Windows authentication
- SQL authentication

Login ID:   Encrypt connection

Password:

Domain:

使用するSQL serverのインスタンスと認証情報を入力し次に進みます。

Quest Change Auditor 7.1.1 Coordinator Setup

### Change Auditor Administrators

Security group settings

Add the current user to the "ChangeAuditor Administrators - FIRST" security group.

Add the current user...を選択し次に進みます。

# Change Auditor Coordinator のインストール

Quest Change Auditor 7.1.1 Coordinator Setup

## Specify Port Information

Assign a static port or default to a dynamic port.

Client Port:	<input type="text" value="0"/>
Public SDK Port:	<input type="text" value="0"/>
Agent Port (Legacy):	<input type="text" value="0"/>
Agent Port:	<input type="text" value="0"/>

Back Next Cancel

ポートを指定します。ここでは、デフォルトの設定を使用します。  
注：ゼロ（0）はダイナミックポートを示しています。

Quest Change Auditor 7.1.1 Coordinator Setup

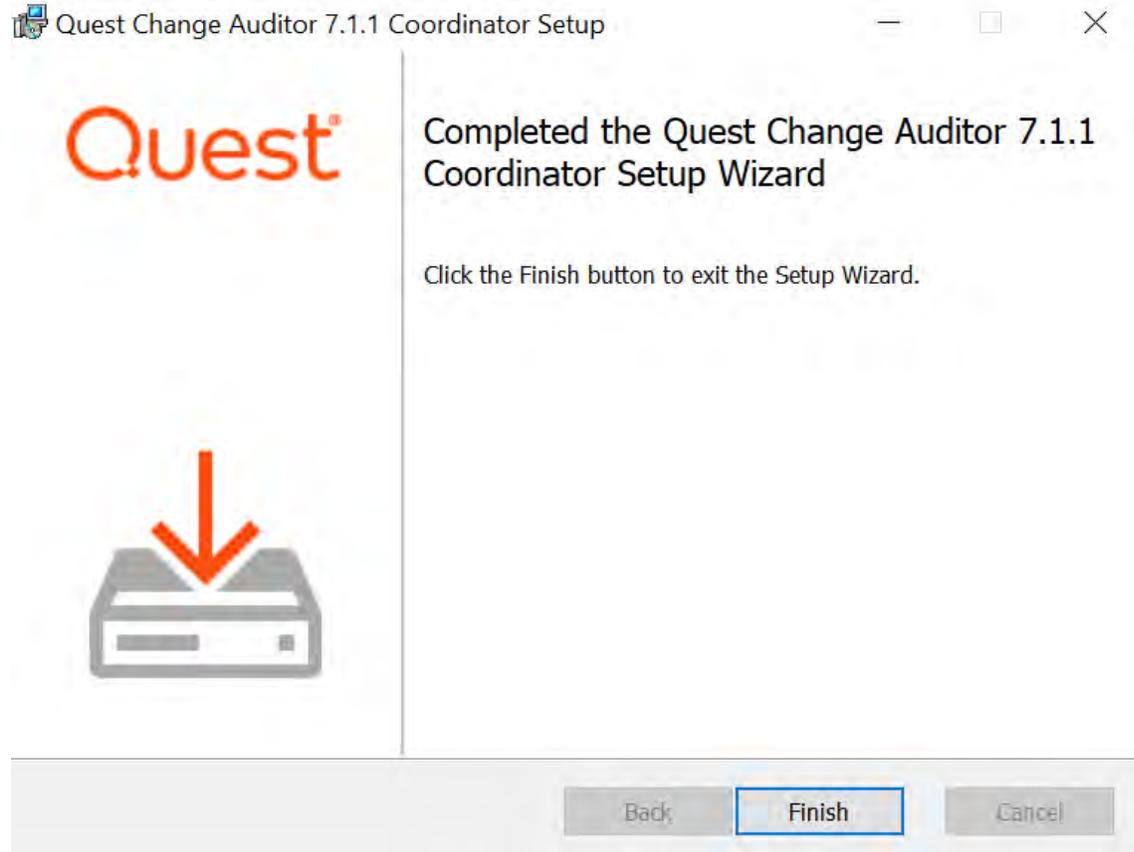
## Ready to install Quest Change Auditor 7.1.1 Coordinator

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Back Install Cancel

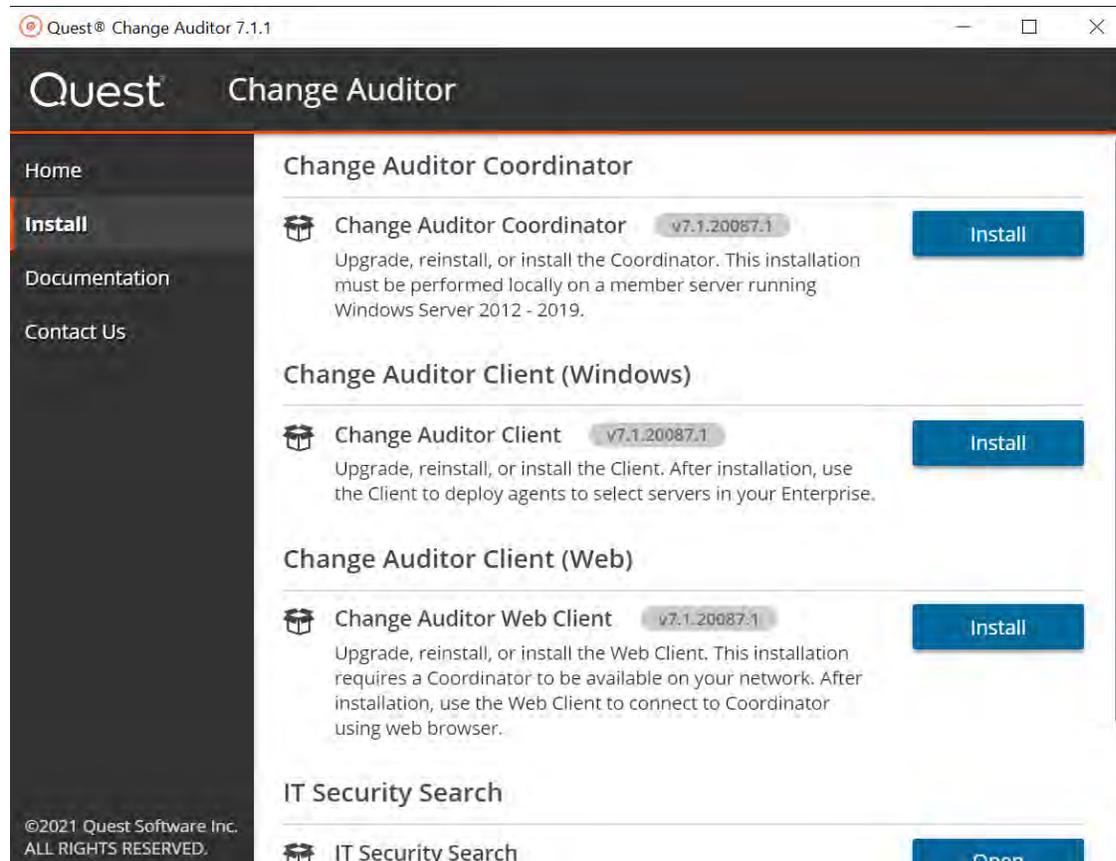
Installボタンをクリックしてインストールを開始します。

# Change Auditor Coordinator のインストール



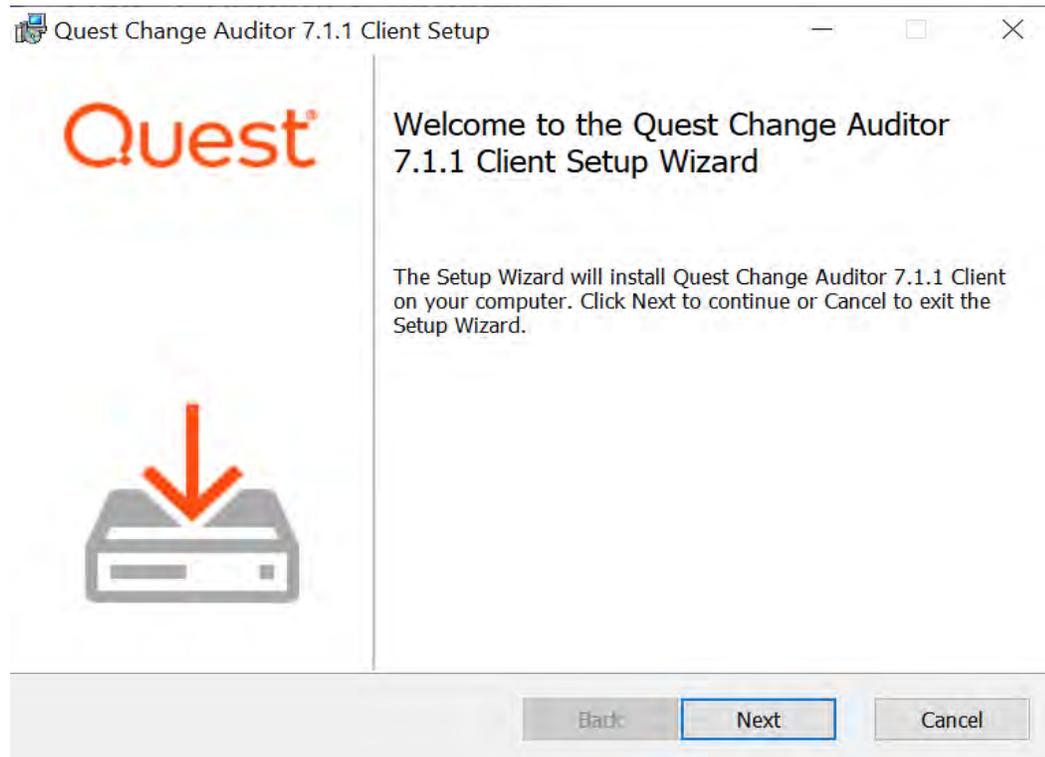
完了後、Finishボタンをクリックしてウィザードを終了します。

# Change Auditor Client のインストール

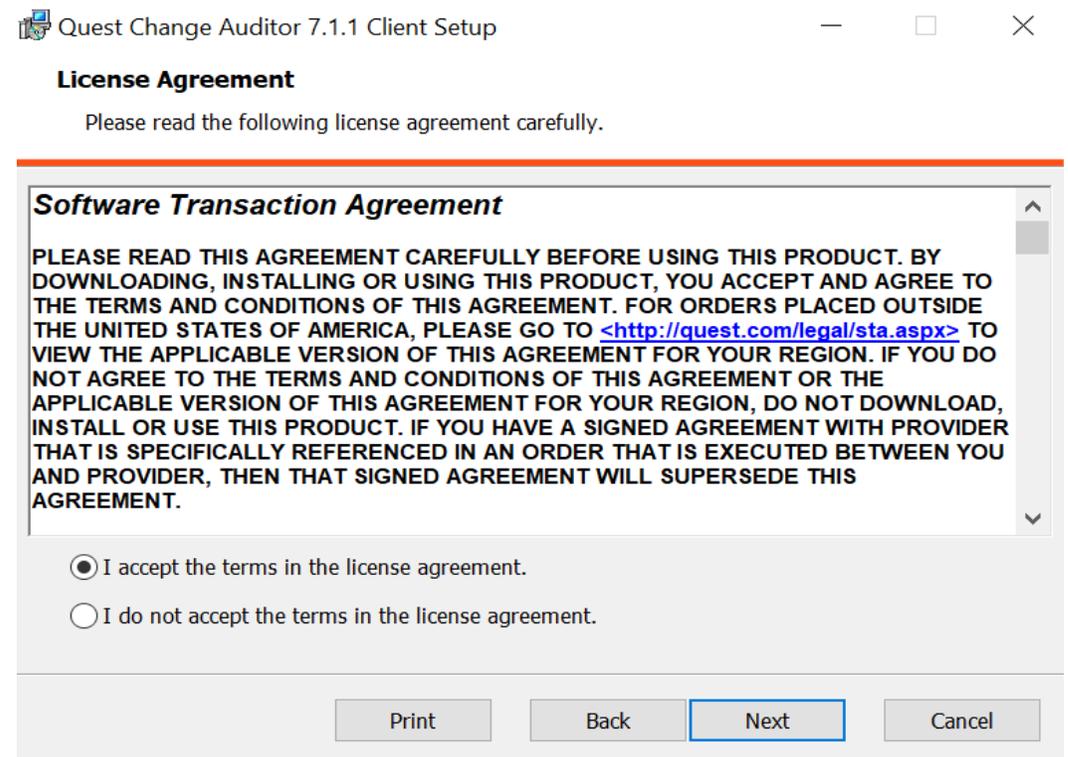


Change Auditor Client (Windows)のInstallボタンをクリックしてウィザードを開始します。

# Change Auditor Client のインストール

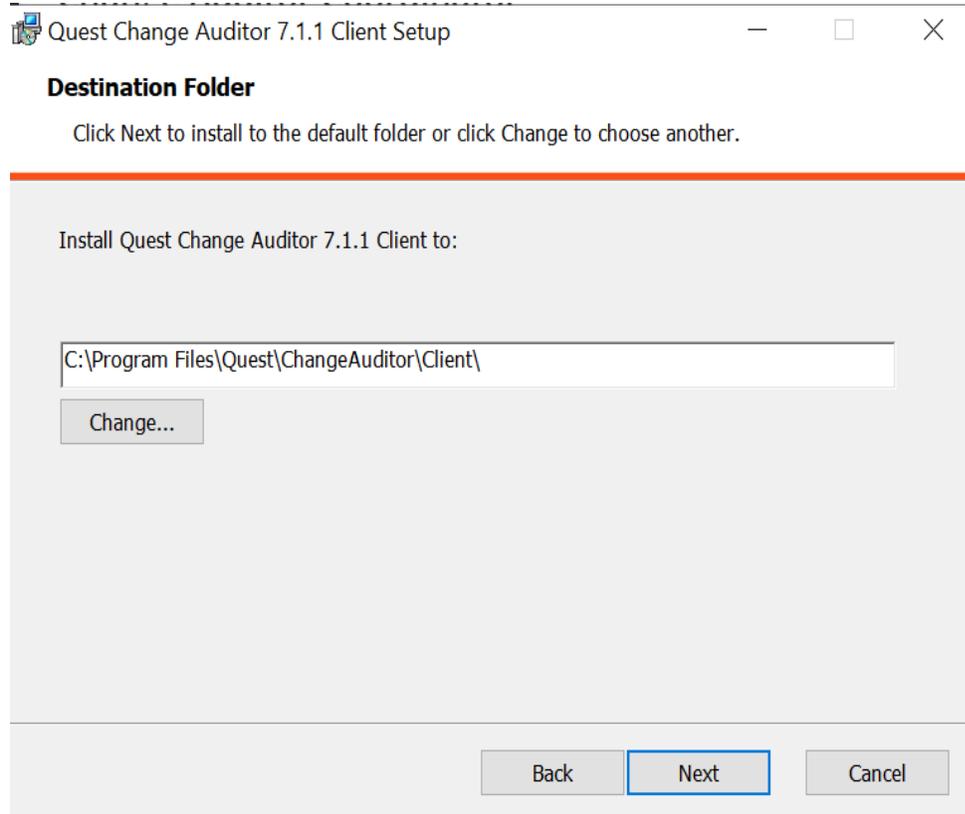


Nextをクリックして次に進みます。

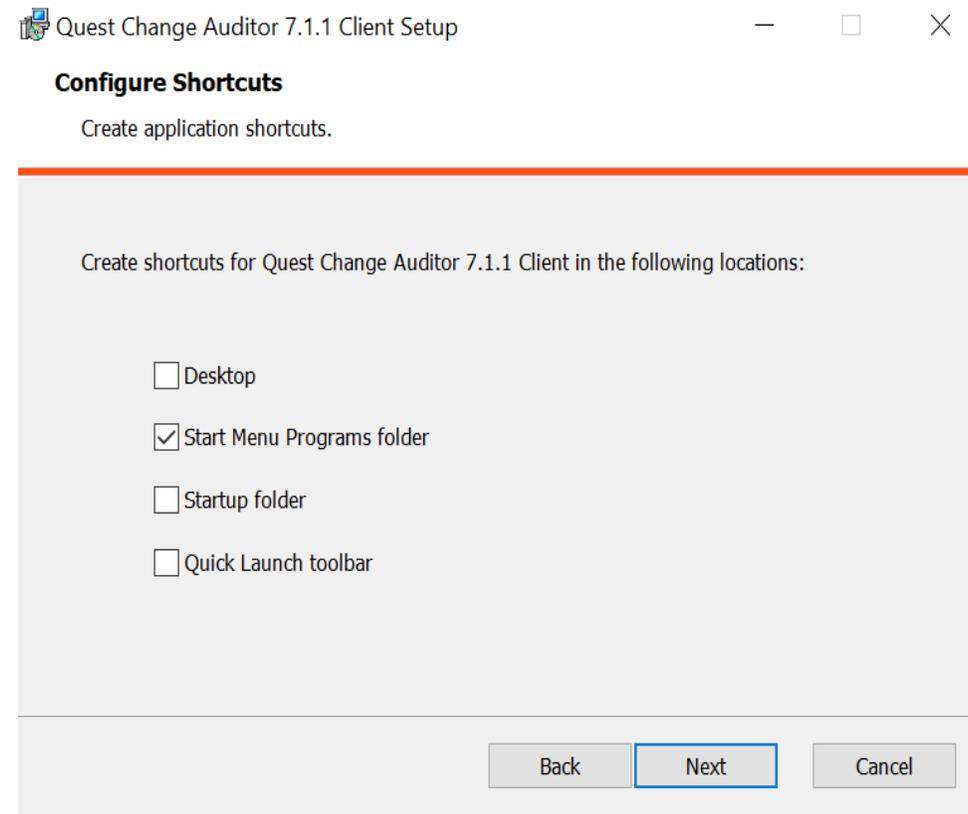


I accept…を選択し次に進みます。

# Change Auditor Client のインストール

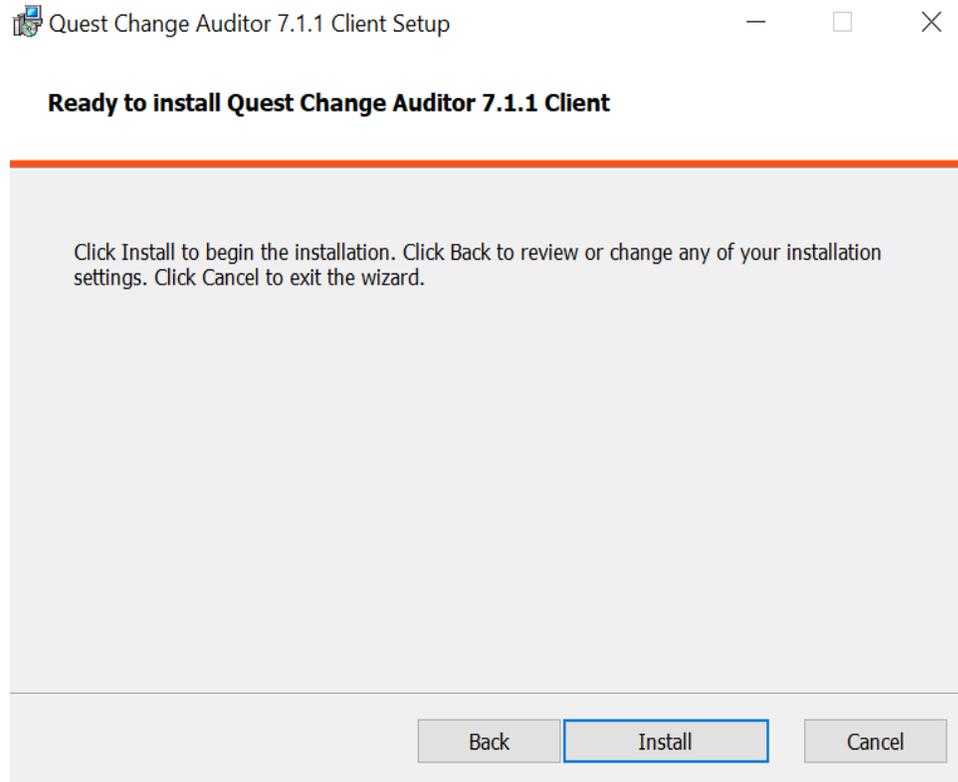


インストールの場所を指定して次に進みます。

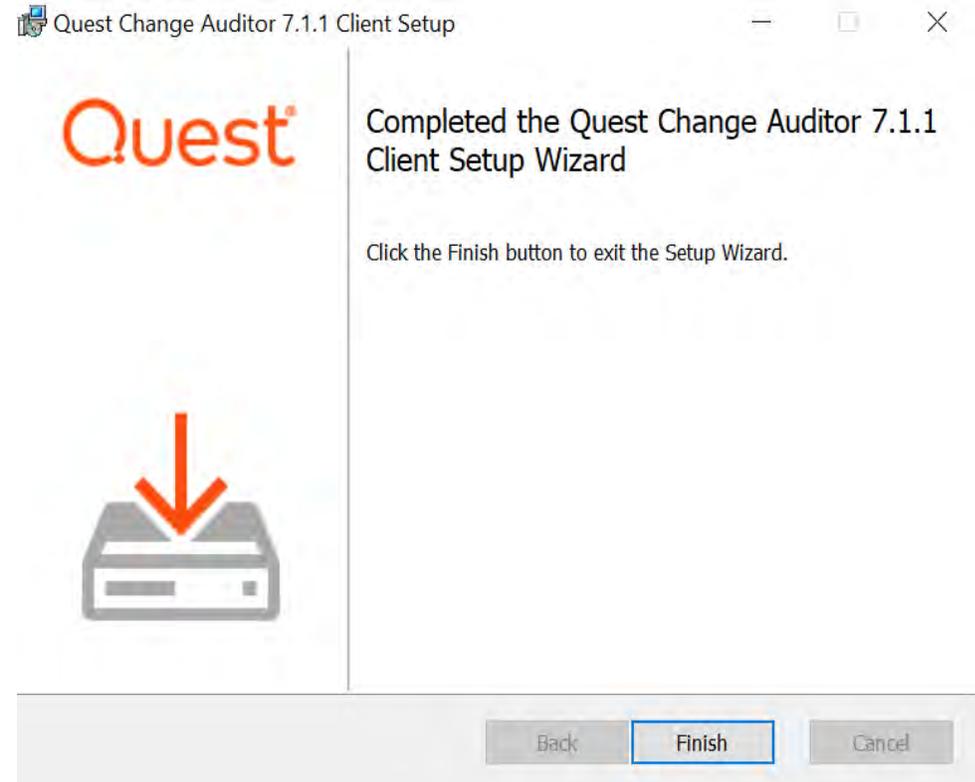


ショートカットを選択し次に進みます。

# Change Auditor Client のインストール



Installボタンをクリックしてインストールを開始します。



完了後Finishボタンをクリックしてウィザードを終了します。



# Client の開始および エージェントのデプロイ

# クライアントの開始

Windowsの スタートメニューから Change Auditor Clientを選択し起動します。

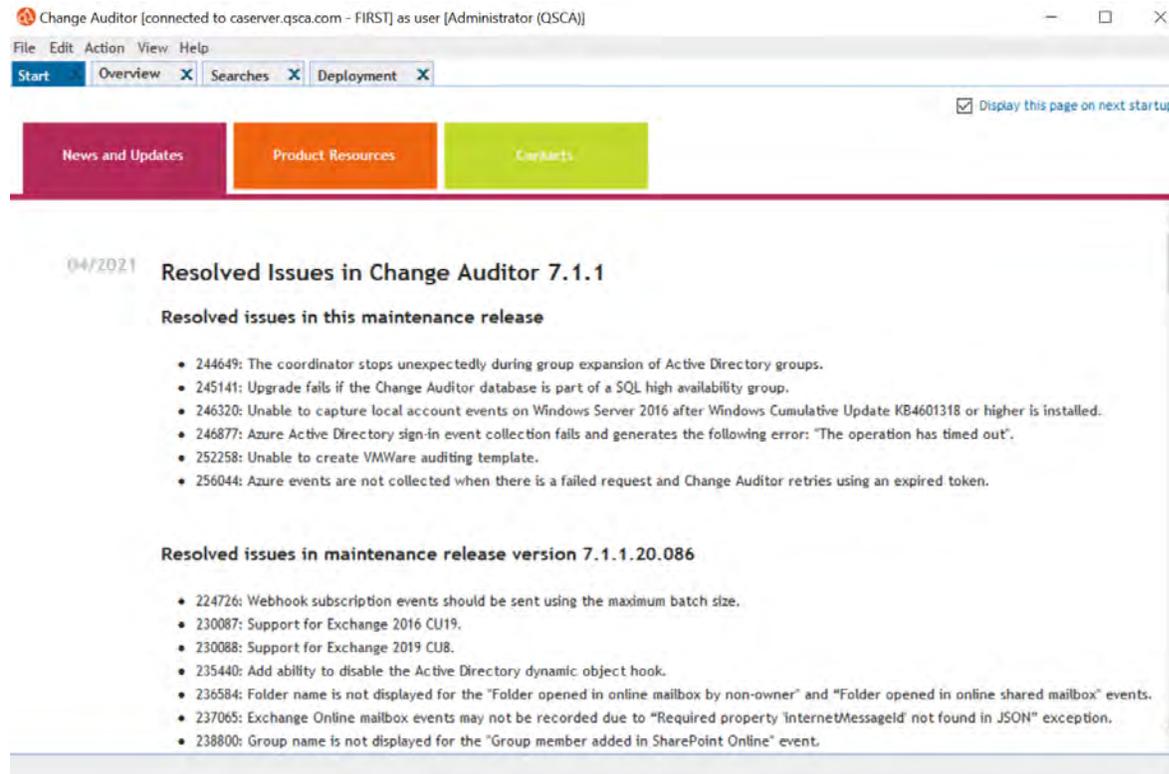


接続するChange Auditor Coordinatorを選択してConnectをクリックしています。

注：接続に失敗する場合はQuest Change Auditor Coordinator serviceが実行されている事、および、アカウントがChange Auditor Administrators もしくはChange Auditor Operators security groupのメンバーであることを確認ください。

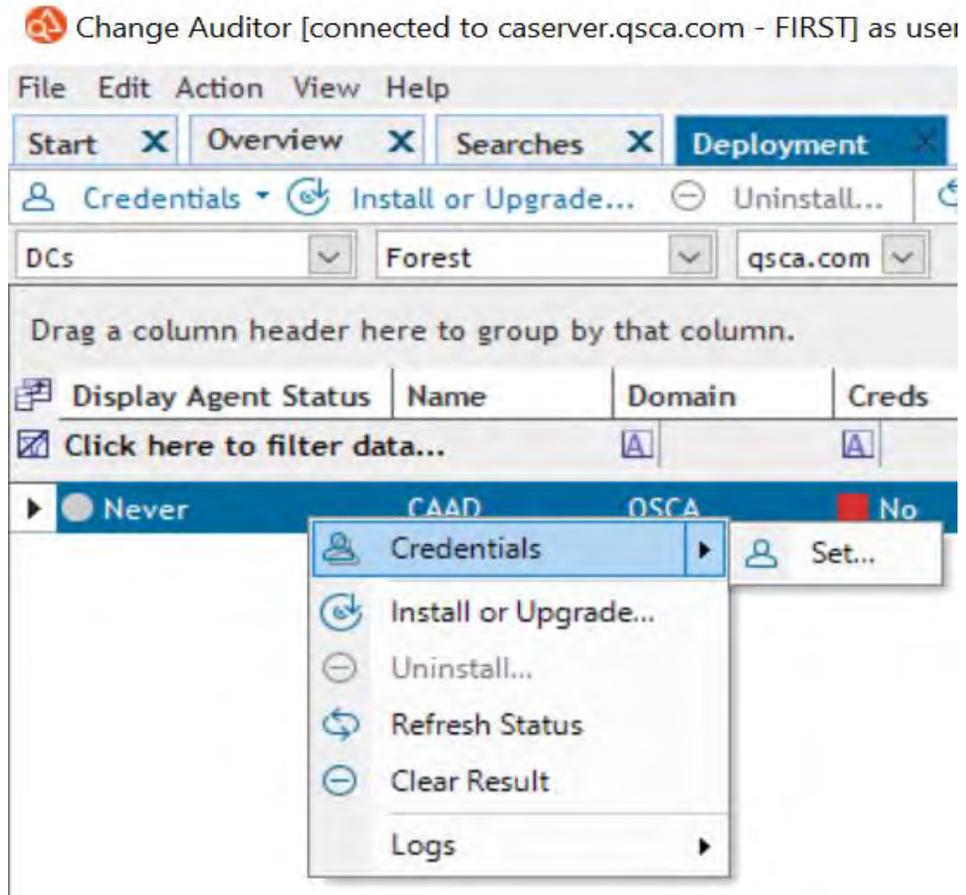
接続が成功すると、スタートページが表示されます。Deploymentタブをクリックしてエージェントをデプロイします。

# クライアントの開始

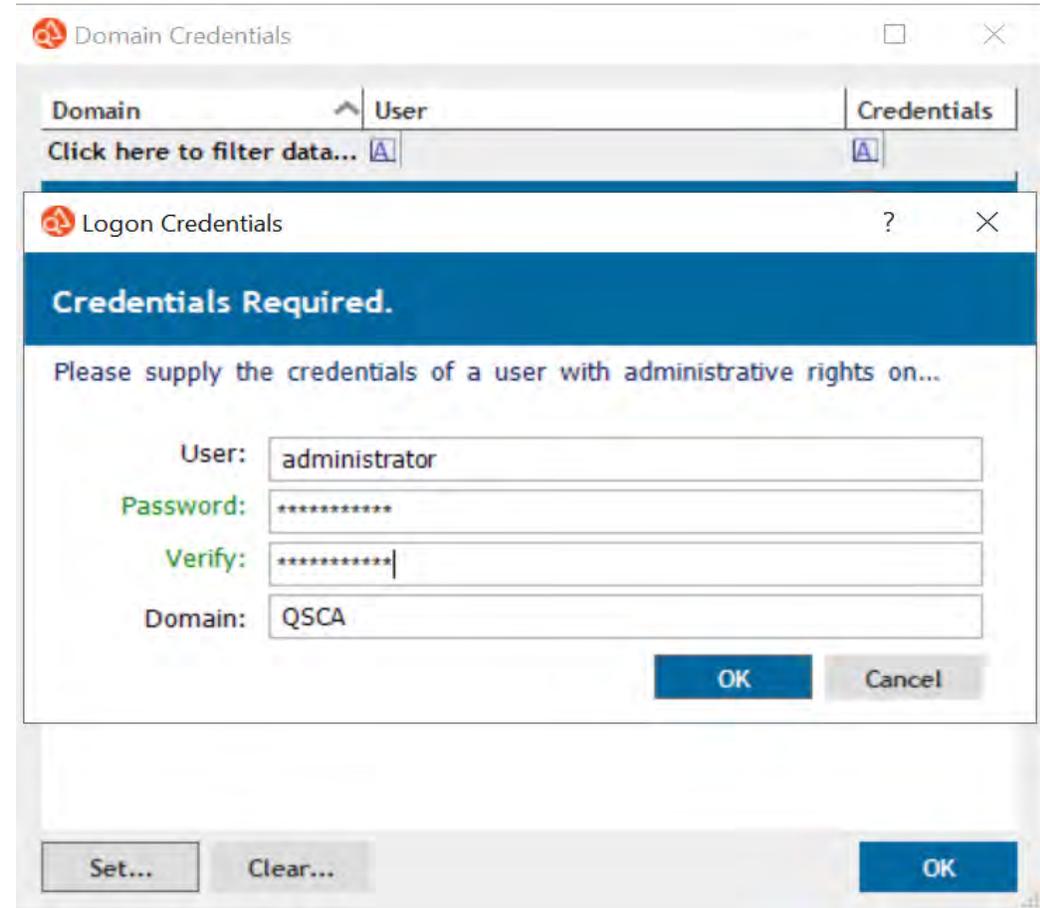


接続が成功すると、スタートページが表示されます。  
Deploymentタブをクリックしてエージェントをでデプロイします。

# エージェントのデプロイ

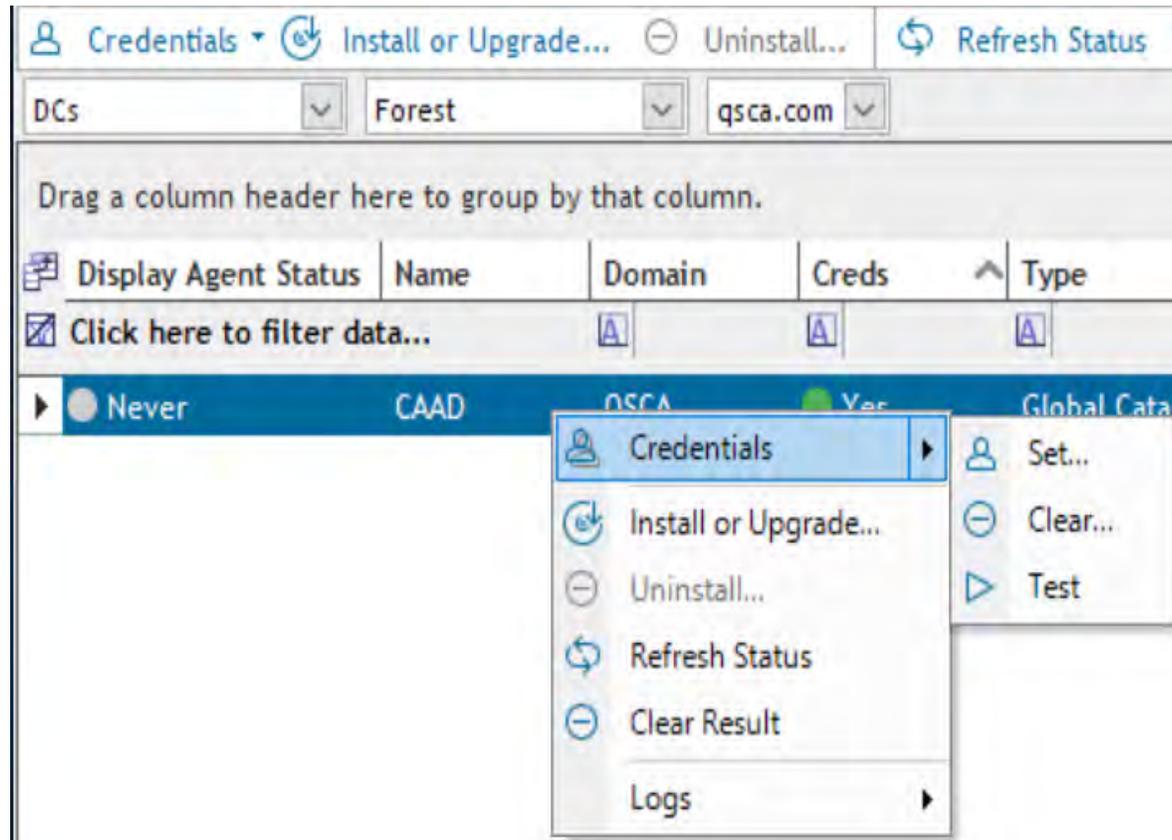


Deploymentタブでエージェントをインストールするシステムを選択して、右クリック→Credentials →Setを選択します。

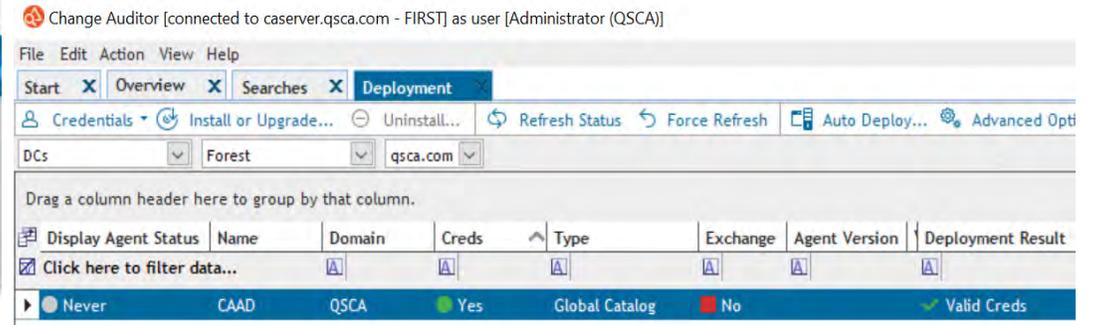


SetボタンをクリックしてLogon Credentials を開きます。ユーザ名、パスワードを入力してOKをクリックします。

# エージェントのデプロイ

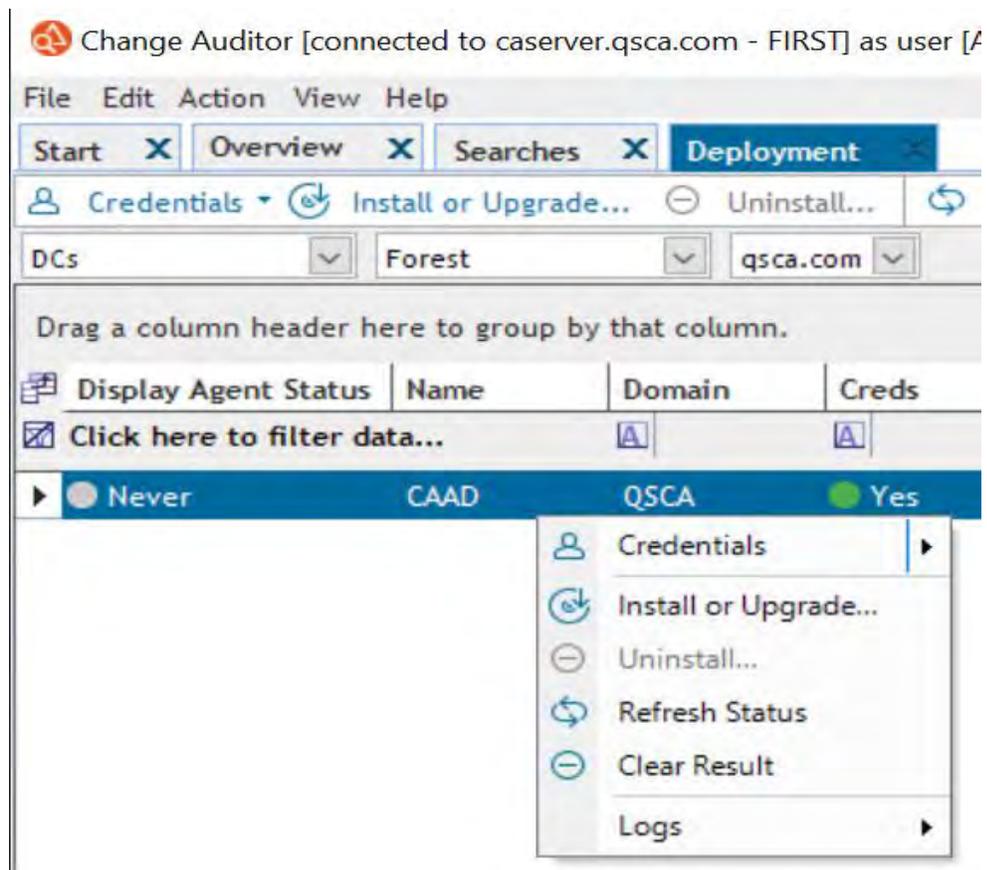


認証の設定後、対象のシステムを右クリック→Credentials  
→Testを選択します。

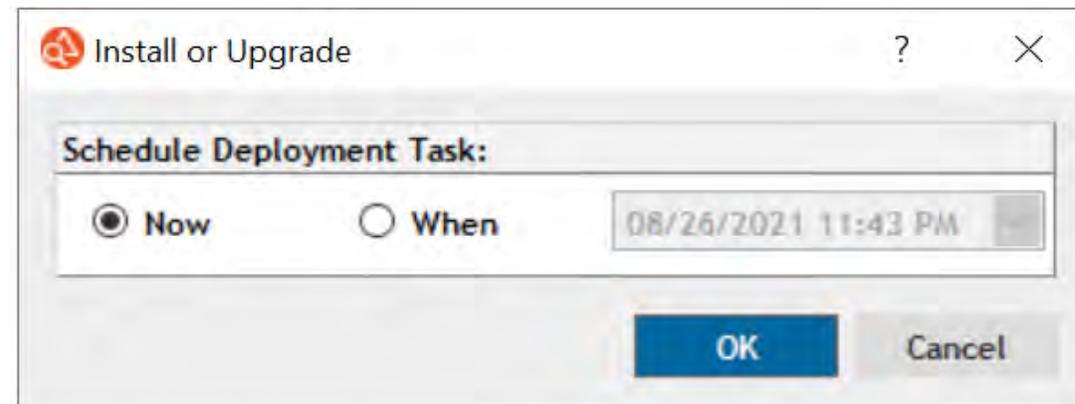


Deployment ResultにValid Credsが表示されたことを確認後、インストールを実行します。

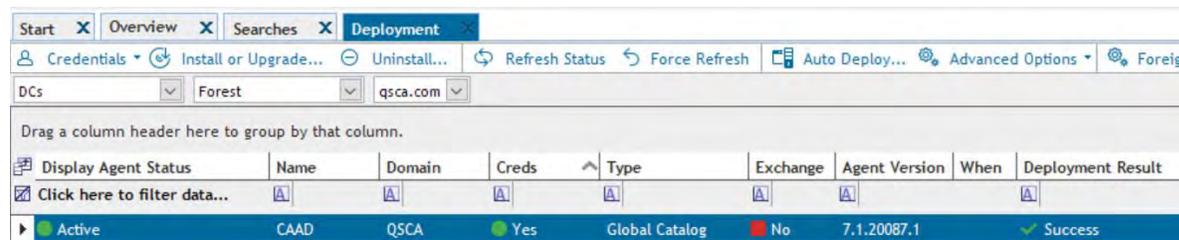
# エージェントのデプロイ



- 1 対象のシステムを右クリック→Install or Upgradeを選択します。



- 2 インストールをスケジュールする場合は、Whenを選び時間を指定します。ここではデフォルトの即実行Nowを選択しOKをクリックします。



- 3 インストールが成功すると、Deployment ResultにSuccess、Deployment Agent StatusにActiveが表示されます。

注 : Deployment Agent StatusがActiveでない場合は、エージェントをインストールした対象のシステム上でQuest Change Auditor agent サービスが正常に実行されている事を確認してください。



# Active Directory の監査

# Active Directory の変更とクエリ

このセクションでは、Active Directory に変更を加えて後のイベント生成および表示の手順を説明します。

注：対象のADにはエージェントがインストールされサービスが正常に実行されている事を確認ください。

- Active Directoryに以下の変更を加えます。
  - Active Directory Users and Computersを開き'Quest Test'というOUを作成します。このOUはどのレベルでも構いません。
  - 'Sample GPO'というGPOを作成し、'Quest Test'にリンクさせます。
  - Domain Adminsセキュリティグループに新規ユーザを追加します。
  - Active Directory Sites and Servicesを開きInter-Site Transport→IPでDEFAULTSITE LINKをダブルクリックし、replicationの値を変更します。
- スタートメニューからChange Auditor Clientを起動します。
- Searchesタブを選択します。
- Shared | Built-inを展開しAll Eventsをクリックします。右のペインでAll Active Directory Eventsをダブルクリックします。イベントが生成され表示されます。
- 上記の変更のイベントを確認します。各イベントをダブルクリックすると詳細が表示されます。

(図：Active Directory イベント)

Change Auditor [connected to caserver.qsca.com - FIRST] as user [Administrator (QSCA)]

File Edit Action View Help

Start X Overview X Searches X Administration Tasks X Agent Statistics X CAFS01 Events Total\* X CAAD Events Total X All Active Directory Events X

Search Properties Event Details Print

Run on: 8/29/2021 12:47 PM Run Time: 00:00:00 Refresh

Records: 51

Severity	Time Detected	Subsystem	User	Event	Computer	Action	Facility	Site	Domain
High	8/29/2021 11:49 AM	Active Directory	QSCA\Administrator	Interval changed	CAAD	Modify Attribute	Site Link...	Default...	QSCA
High	8/29/2021 11:28 AM	Active Directory	QSCA\Administrator	Member added to critical ent...	CAAD	Add Attribute	Forest C...	Default...	QSCA
Medium	8/29/2021 11:28 AM	Active Directory	QSCA\Administrator	Member added to group	CAAD	Add Attribute	Custom...	Default...	QSCA
Medium	8/29/2021 11:28 AM	Active Directory	QSCA\Administrator	Nested member added to gro...	CAAD	Add Attribute	Custom...	Default...	QSCA
Medium	8/29/2021 11:28 AM	Active Directory	QSCA\Administrator	User member-of added	CAAD	Add Attribute	Custom...	Default...	QSCA
High	8/29/2021 10:58 AM	Active Directory	QSCA\Administrator	Group policy link added to OU	CAAD	Add Attribute	Group Po...	Default...	QSCA
High	8/29/2021 10:53 AM	Active Directory	QSCA\Administrator	Group policy object renamed	CAAD	Modify Attribute	Group Po...	Default...	QSCA
High	8/29/2021 10:53 AM	Active Directory	QSCA\Administrator	Group policy object added	CAAD	Add Object	Group Po...	Default...	QSCA
High	8/29/2021 10:37 AM	Active Directory	QSCA\Administrator	DACL changed on domain obj...	CAAD	Modify Attribute	Domain...	Default...	QSCA
High	8/29/2021 10:37 AM	Active Directory	QSCA\Administrator	DACL changed on OU object	CAAD	Modify Attribute	OU	Default...	QSCA

Copy Email... Print Knowledge Base... Comments... Disable Related Search Add to Search Protect

**High Severity**

Who: QSCA\Administrator

Where: CAAD

What: The interval of the site link DEFAULTIPSITELINK changed.

Active Directory

Class: siteLink

Object: qsca.com/Configuration/Sites/Inter-Site Transports/IP/DEFAULTIPSITELINK

From: 180

To: 240

Source: Change Auditor

Action: Modify Attribute

Attr: replInterval

When: 8/29/2021 11:49:01 AM

Origin: caad.qsca.com (10.31.17.213)

Result: Success

Facility: Site Link Configuration

Authentication: Kerberos

Port: 389

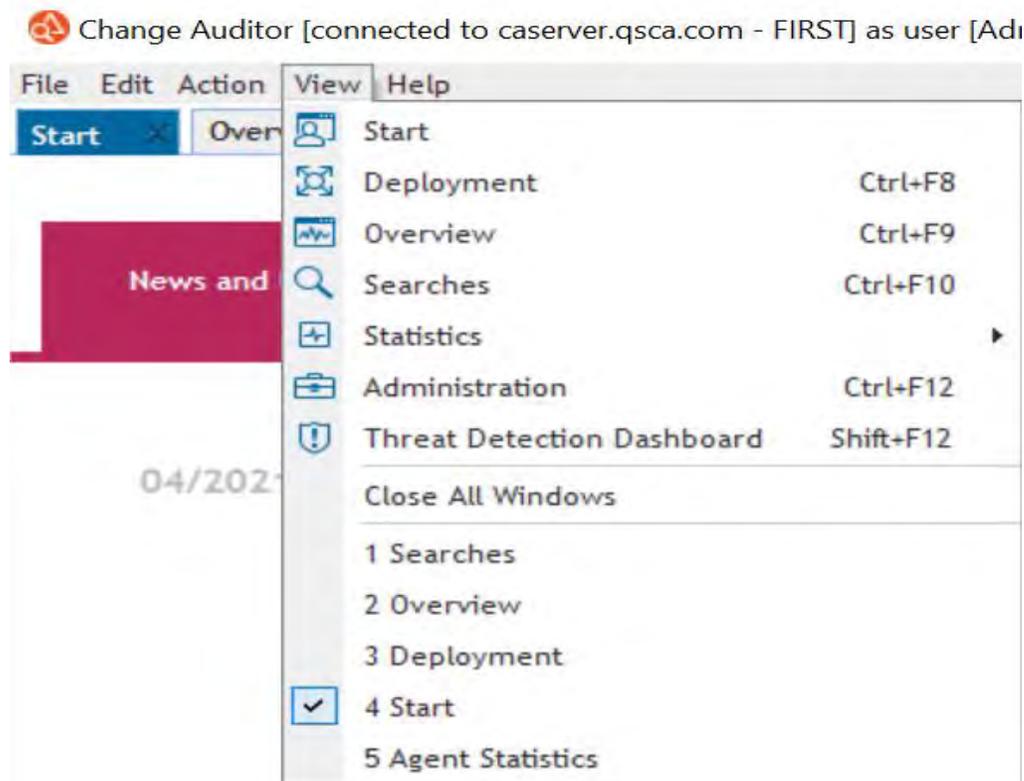
図 : Active Directory イベント



# Windows File System の監査

# File Systemのテンプレート設定

このセクションではFile Systemの監査に必要なテンプレートを作成する手順を説明します。



View →Administrationを選択します。

# File Systemのテンプレート設定

Start X Overview X Searches X Deployment X Agent Statistics X Administration Tasks X

Attributes 3

- Azure Active Directory (0)

Applications

- Exchange Mailbox (0)
- Office 365 (0)
- VMware (0)
- SharePoint (0)
- Skype for Business (0)

SQL

- SQL Server (1)
- SQL Data Level (0)

Server

- File System (0) 2
- Registry (0)
- Services (0)

NAS

- EMC (0)
- NetApp (0)
- FluidFS (0)

Configuration

**Auditing** 1

Protection

Administration Tasks

Add... Edit... Assign... Delete Print

Template Name	Group Enabled	Path Filter	Process
Click here to filter data...			

1. Administration Tasksタブの左ペインからAuditingをクリックします。
2. 左ペインからServer→File Systemをクリックします。
3. Add...をクリックしてFile System Auditing Wizard を開きます。

File System Auditing Wizard

Use this wizard to create or modify a File System Auditing Template.

Template Name: 3

Audit Path:  File  Folder  All Drives Paths must be local. Auditing shares or mapped drives is not supported.

Path	Type	Scope	Include Mask	Exclude
------	------	-------	--------------	---------

Events Inclusions Exclusions

Select the file and/or folder events to audit.

<input checked="" type="checkbox"/> File Events	<input checked="" type="checkbox"/> Folder Events
---	---

Discard file open events from browsing  Discard Windows Explorer tooltip events from folder browsing

Help Back Next Finish Cancel

# File Systemのテンプレート設定

File System Auditing Wizard

Use this wizard to create or modify a File System Auditing Template.

Template Name:  
FS template

Audit Path:  File  Folder  All Drives Paths must be local. Auditing shares or mapped drives is not supported.

c:\FSTest

Path	Type	Scope	Include Mask	Exclude
------	------	-------	--------------	---------

Events | Inclusions | Exclusions

Select the file and/or folder events to audit.

File Events  Folder Events

Discard file open events from browsing  Discard Windows Explorer tooltip events from folder browsing

Help Back Next Finish Cancel

1. **Template**名を入力します。
2. **Audit Path**で**Folder**を選択し、パスを指定します。**Add**をクリックしてパスを追加します。

注：ファイルサーバー上のローカルのパスを指定します。共有もしくはマップしたドライブは未対応です。

# File Systemのテンプレート設定

File System Auditing Wizard

Use this wizard to create or modify a File System Auditing Template.

Template Name: FS template

Audit Path:  File  Folder  All Drives ⚠ Paths must be local. Auditing shares or mapped drives is not supported.

Path	Type	Scope	Include Mask	Exclude
c:\FSTest	Folder	This object and all chil...		0 File; 0 Folder

Events  Inclusions  Exclusions

Select the file and/or folder events to audit.

<input checked="" type="checkbox"/> File Events	<input checked="" type="checkbox"/> Folder Events
<input checked="" type="checkbox"/> Failed file access (Change Auditor Protection)	<input checked="" type="checkbox"/> Failed folder access (Change Auditor Protection)
<input checked="" type="checkbox"/> Failed file access (NTFS permissions)	<input checked="" type="checkbox"/> Failed folder access (NTFS permissions)
<input checked="" type="checkbox"/> File access rights changed	<input checked="" type="checkbox"/> Failed share access (Change Auditor Protection)
<input checked="" type="checkbox"/> File attribute changed	<input checked="" type="checkbox"/> Failed share access (NTFS permissions)

Discard file open events from browsing  Discard Windows Explorer tooltip events from folder browsing

Help Back Next Finish Cancel

EventタブでFile EventsとFolder Eventsを選択します。

File System Auditing Wizard

Use this wizard to create or modify a File System Auditing Template.

Template Name: FS template

Audit Path:  File  Folder  All Drives ⚠ Paths must be local. Auditing shares or mapped drives is not supported.

Path	Type	Scope	Include Mask	Exclude
c:\FSTest	Folder	This object and all chil...	*	0 File; 0 Folder

Events  Inclusions  Exclusions

Add the file masks to audit. [Click here for examples.](#)

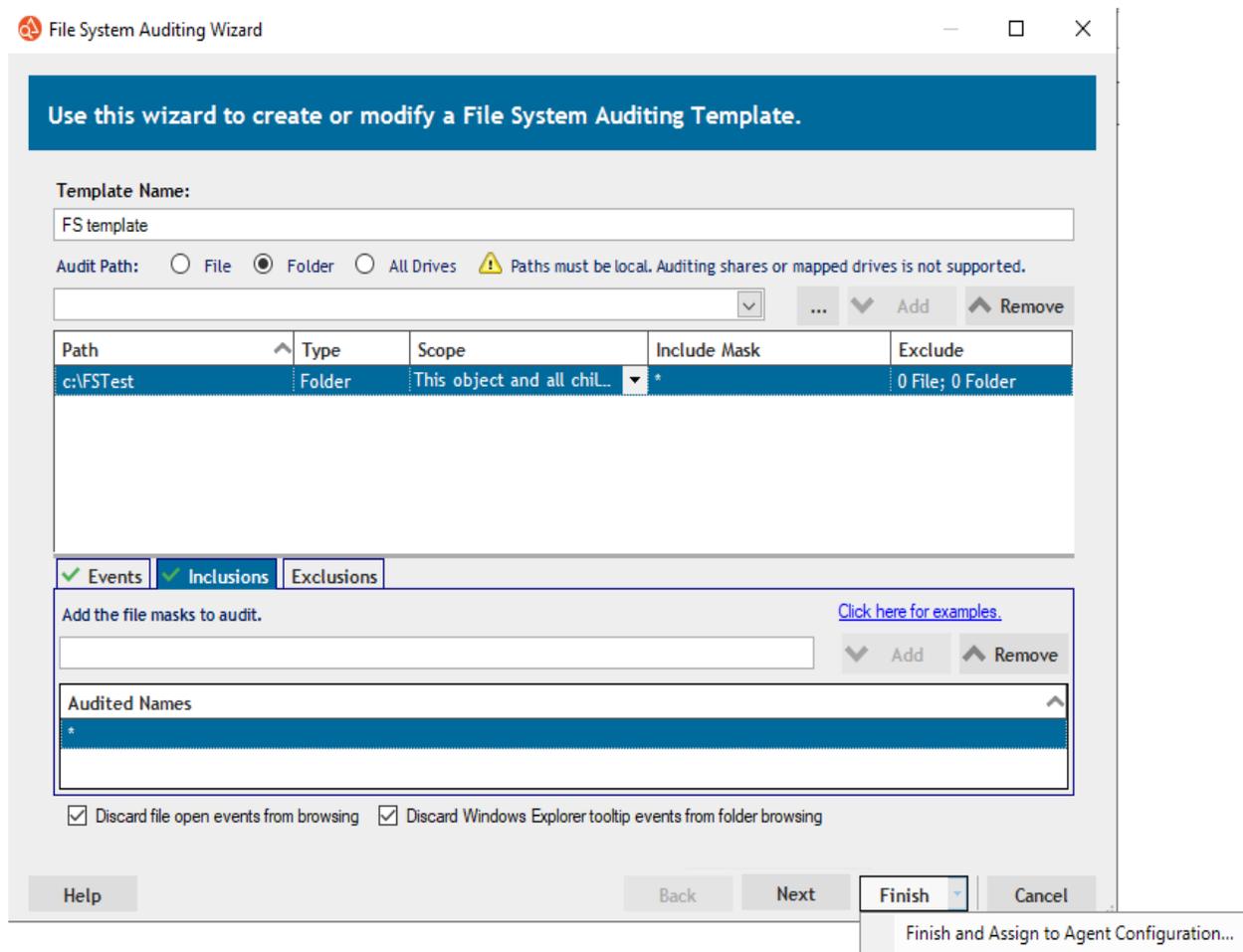
Audited Names

Discard file open events from browsing  Discard Windows Explorer tooltip events from folder browsing

Help Back Next Finish Cancel

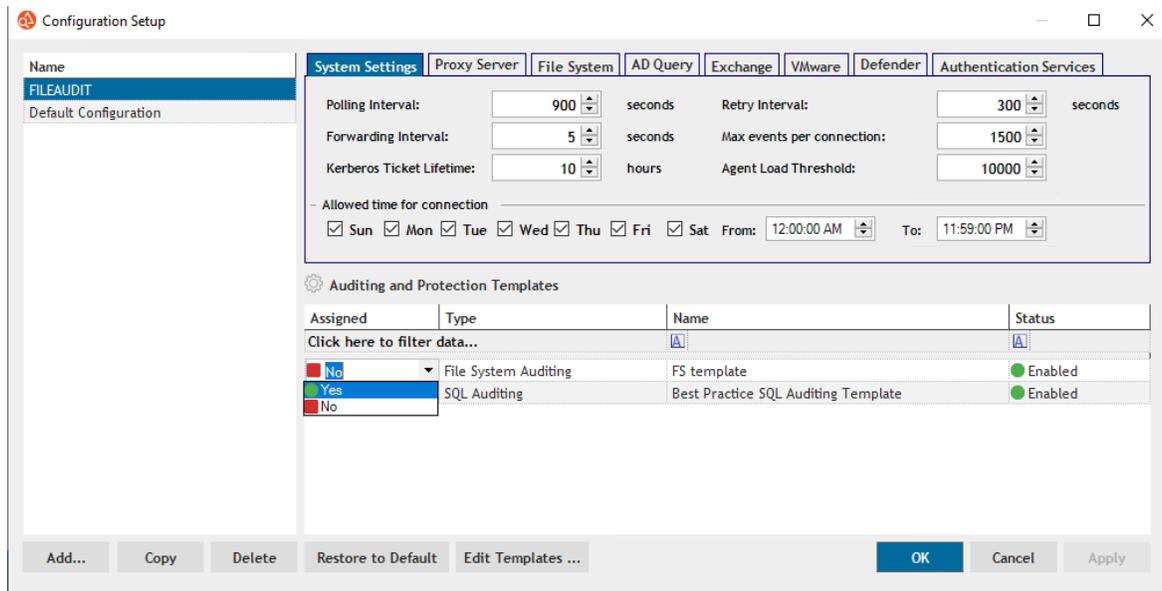
InclusionsタブでAdd the file masks to auditに\* (アスタリスク) を追加します。

# File Systemのテンプレート設定

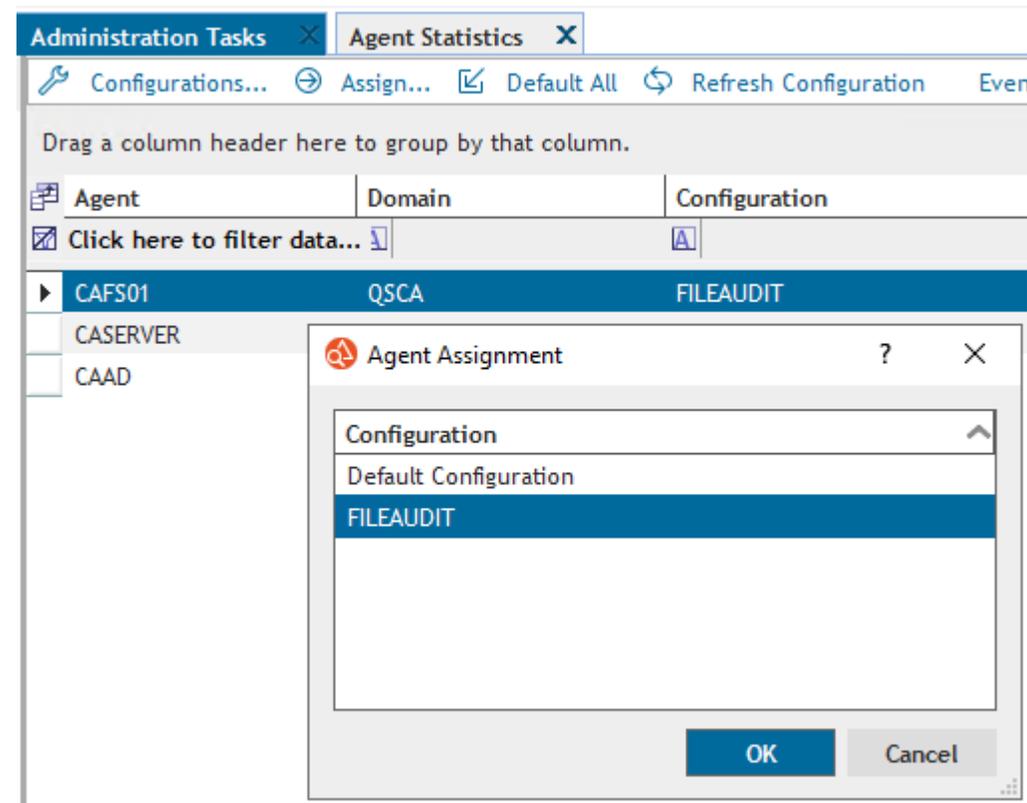


**Finish**ボタンから**Finish and Assign to Agent Configuration...**を選択します。

# File Systemのテンプレート設定



**Configuration Setup** ページの左ペインから使用する構成を選択します。作成したテンプレートを選び**Assigned**の項目で**Yes**を選択します。OKをクリックしてウィンドウを閉じます。



エージェントを選択し、**Assign...**をクリックして**Agent Assignment**を開きます。

テンプレートに適用した構成を選びOKをクリックします。

# File Systemのテンプレート設定

Configurations... Assign... Default All Refresh Configuration Event Logging... Logs Print

Drag a column header here to group by that column.

Agent	Domain	Configuration	Office 365	Azure Activ...	File System
<input checked="" type="checkbox"/> Click here to filter data...					
CAFS01	QSCA	FILEAUDIT	None	None	Auditing
CASERVER	QSCA	Default Configuration	None	None	None
CAAD	QSCA	Default Configuration	None	None	None

テンプレートが適用されるとFile System の項目が**Auditing**と表示されます。

# Windows File System の変更の監査例

ここでは、File Systemの簡単なテスト手順を説明します。

1. 前述に設定したFile systemのフォルダーに変更を加えます。

例：

- ファイルを追加
- 既存のファイルの権限を変更（ファイルを右クリック→セキュリティタブ→ユーザ追加）
- 既存ファイルの削除
- サブフォルダを追加

2. Change Auditor Client でイベントを次のいずれかの方法で確認します。

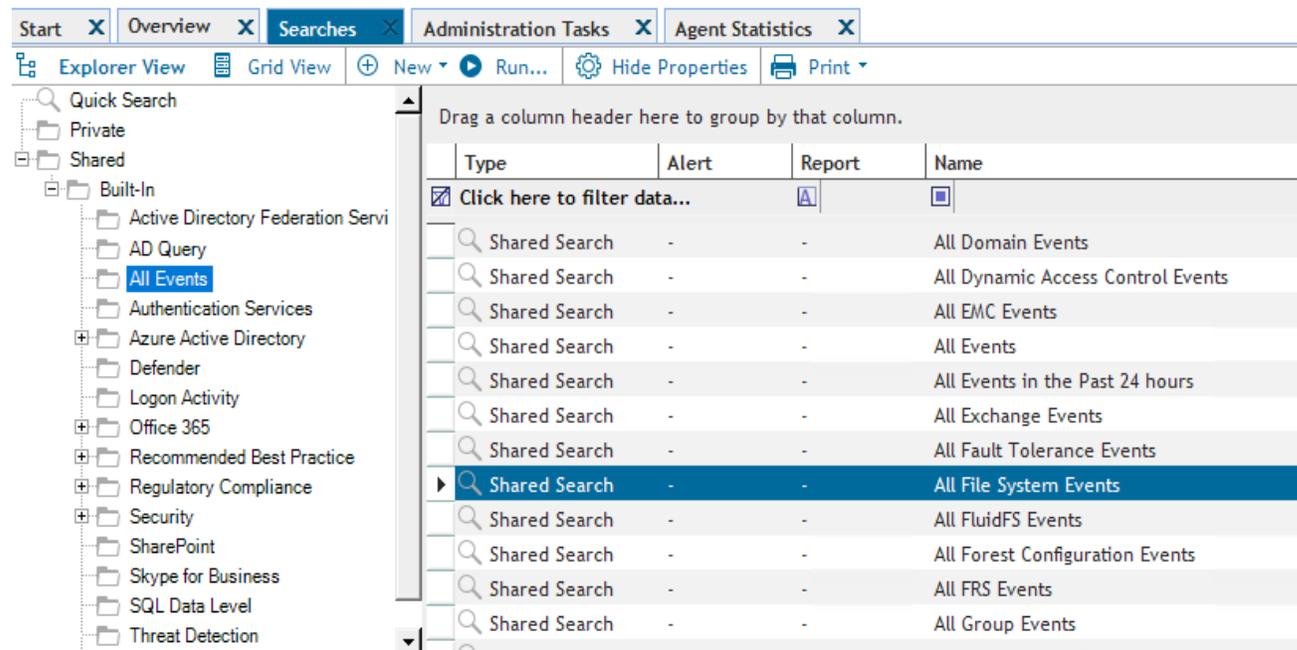
1) Agent Statisticsタブで対象のエージェントのEvents Today項目の件数のリンクをクリックします。

Status	Agent	Domain	Load	Uptime	Last Update	Events Today	Events Total	DB Size
Active	CAFS01	QSCA	Normal	0d 13h 38m	8/28/2021 1:36 PM	<a href="#">163</a>	176	3.39 MB

# Windows File System の変更の監査例

2) Searches タブでAll Events →All File System Events をダブルクリックします。

注：エージェントがインストールされているすべてのFile Systemが対象になります。



# Windows File System の変更の監査例

File System (ファイルサーバー) の イベントが表示されます。

項目等のフィルタリング、その他の詳細はユーザーガイドを参照ください。

The screenshot displays the Change Auditor interface. The main window shows a list of events under the 'CAF501 Events Total\*' tab. The table below summarizes the visible events:

Severity	Time Detected	Subsystem	User	Event	Computer	Action	Domain	Result
Medium	8/28/2021 2:11 PM	File System	CAF501\cafsuser01	File moved	CAF501	Move Object	QSCA	Success
Medium	8/28/2021 2:11 PM	File System	CAF501\cafsuser01	File deleted	CAF501	Delete Object	QSCA	Success
Medium	8/28/2021 2:10 PM	File System	CAF501\cafsuser01	Folder created	CAF501	Add Object	QSCA	Success
Medium	8/28/2021 2:10 PM	File System	CAF501\cafsuser01	File moved	CAF501	Move Object	QSCA	Success
Medium	8/28/2021 2:05 PM	File System	CAF501\cafsuser01	File access rights changed	CAF501	Modify Attribute	QSCA	Success
Medium	8/28/2021 2:04 PM	File System	CAF501\cafsuser01	File renamed	CAF501	Rename Object	QSCA	Success
Medium	8/28/2021 12:18 AM	File System	CAF501\Administrator	File created	CAF501	Add Object	QSCA	Success
Medium	8/28/2021 12:18 AM	File System	CAF501\Administrator	File created	CAF501	Add Object	QSCA	Success

The detailed view for the 'File deleted' event shows the following information:

- Severity:** Medium
- Who:** CAF501\cafsuser01
- Where:** CAF501
- What:** File C:\FSTest\subfolder\ビットマップ rename.bmp deleted on QSCA\CAF501.
- File System**
- Path:** C:\FSTest\subfolder\ビットマップ rename.bmp
- Attribute:**
- When:** 8/28/2021 2:11:53 PM
- Origin:** cafs01.qsca.com (10.31.17.215)
- Result:** Success
- Facility:** Custom File System Monitoring
- Action:** Delete Object
- Process:** C:\Windows\System32\dlhhost.exe
- Source:** Change Auditor

Quest

[目次に戻る](#)

Where Next Meets Now.