Change Auditor クイックガイド

Quest

Where Next Meets Now.

目次

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

目次に戻る

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

目次に戻る

Change Auditor ソフトウェアのダウンロード

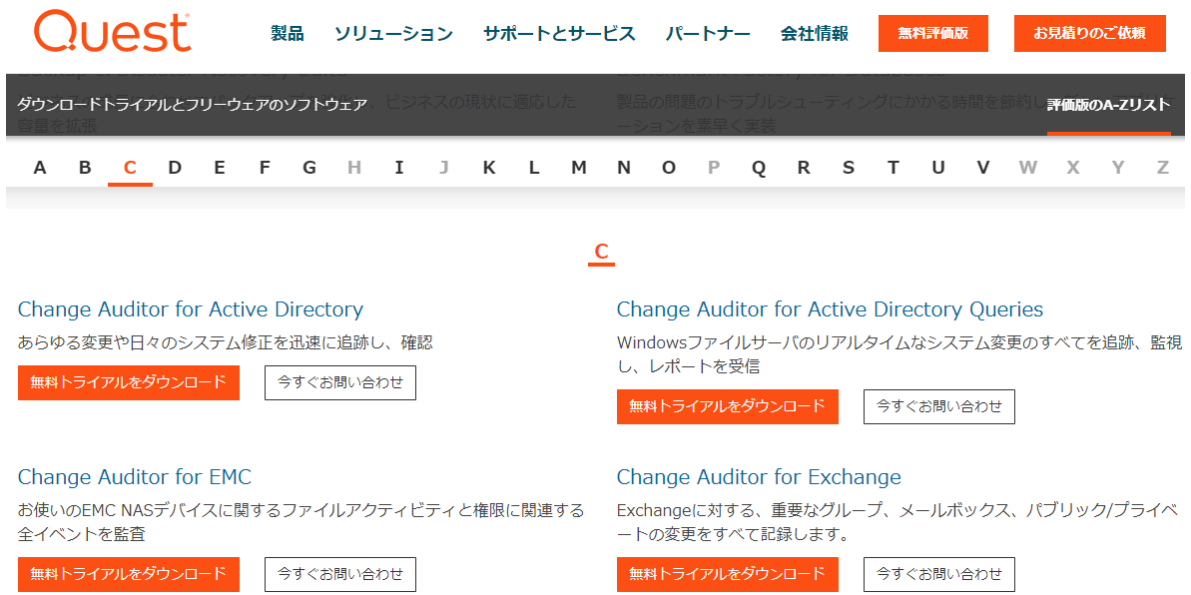
ソフトウェアはサポートポータル（ソフトウェアのみ）、もしくは無償評価版（トライアルライセンス）のリンクからダウンロードします。

サポートポータルサイト

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

トライアル

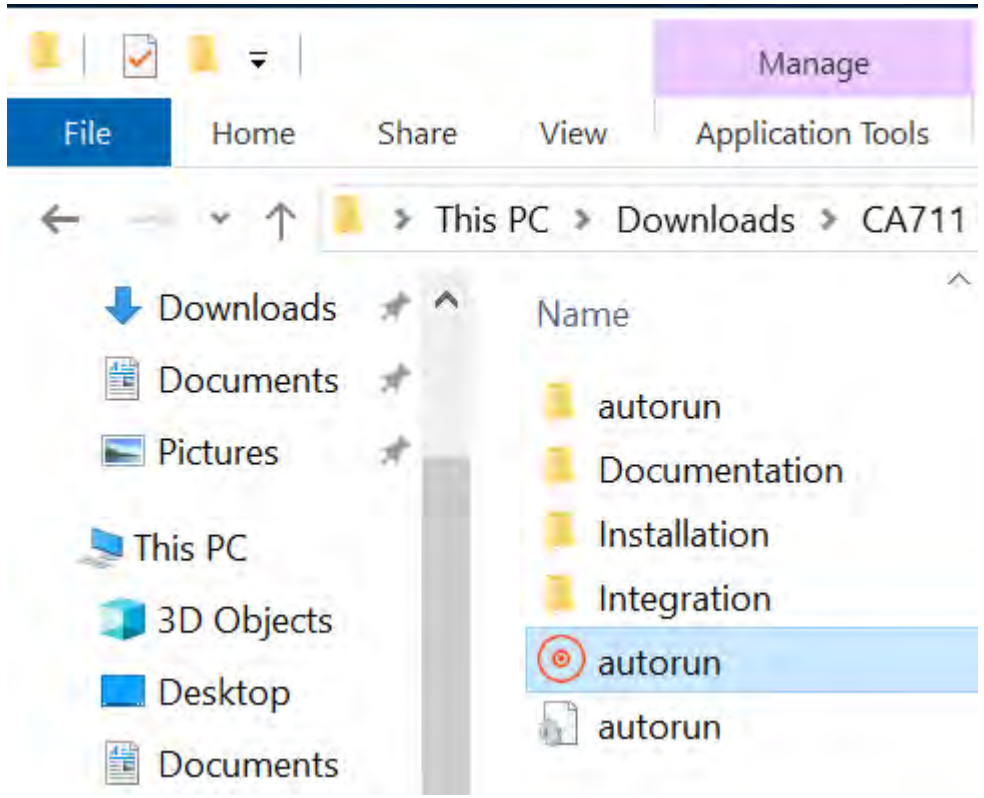
https://www.quest.com/jp-ja/trials/#%20



目次に戻る

Change Auditor のインストール

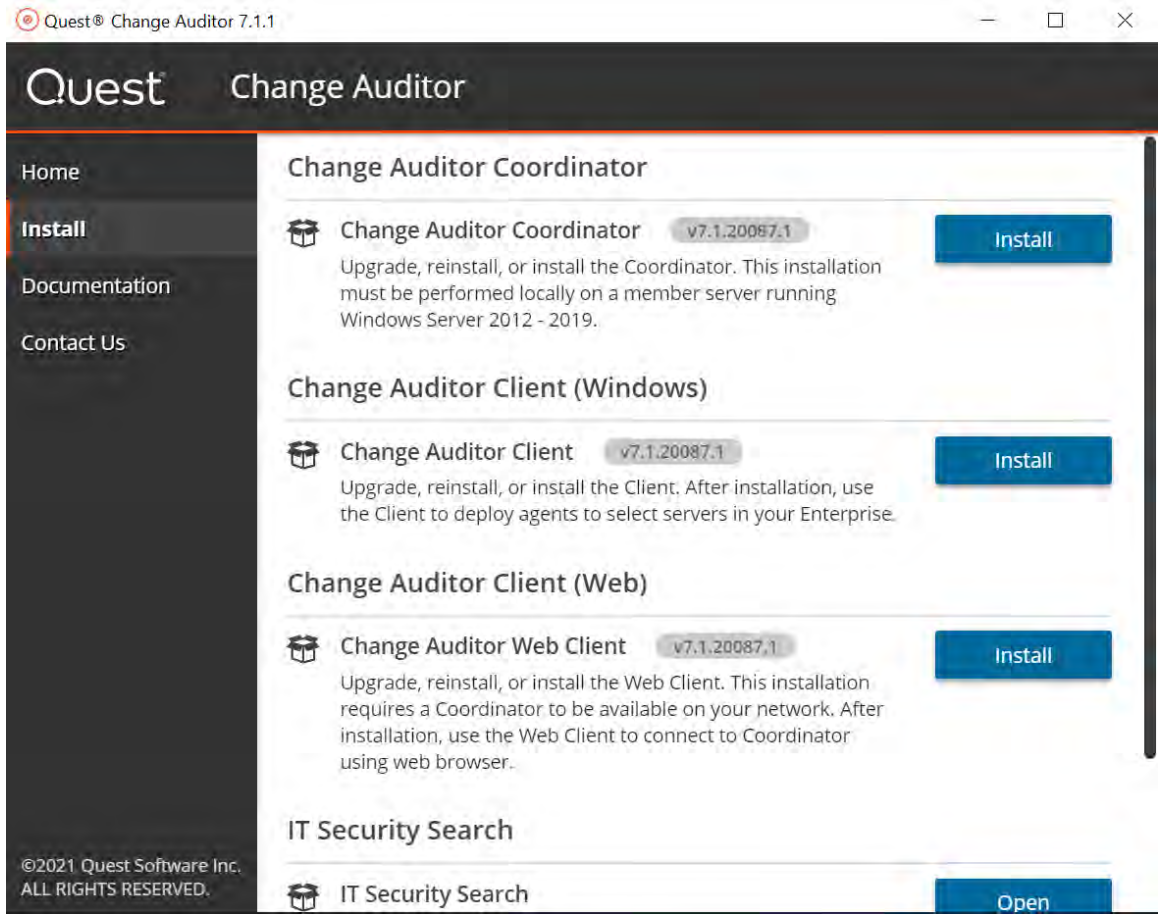
このガイドではCoordinator, Client, およびSQL serverを同じWindows OSにイントールするシナリオを説明します。



autorunをクリックしてウィザードを起動します。

目次に戻る

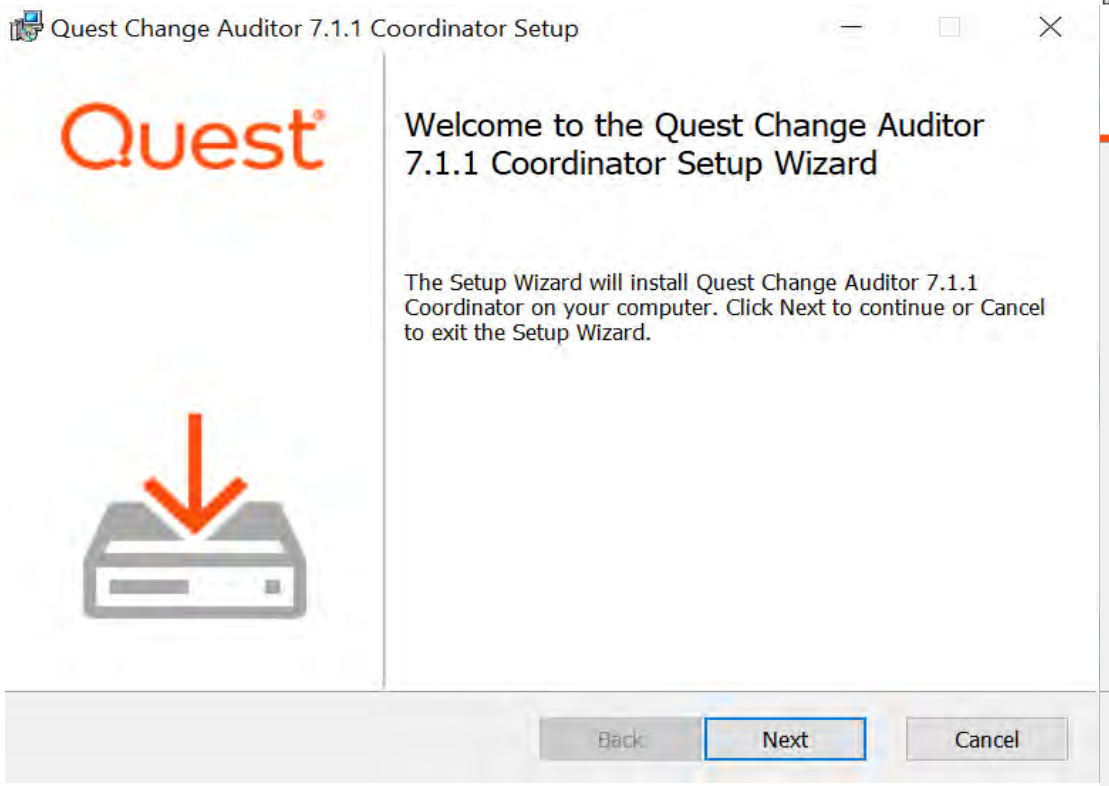
Change Auditor Coordinator のインストール



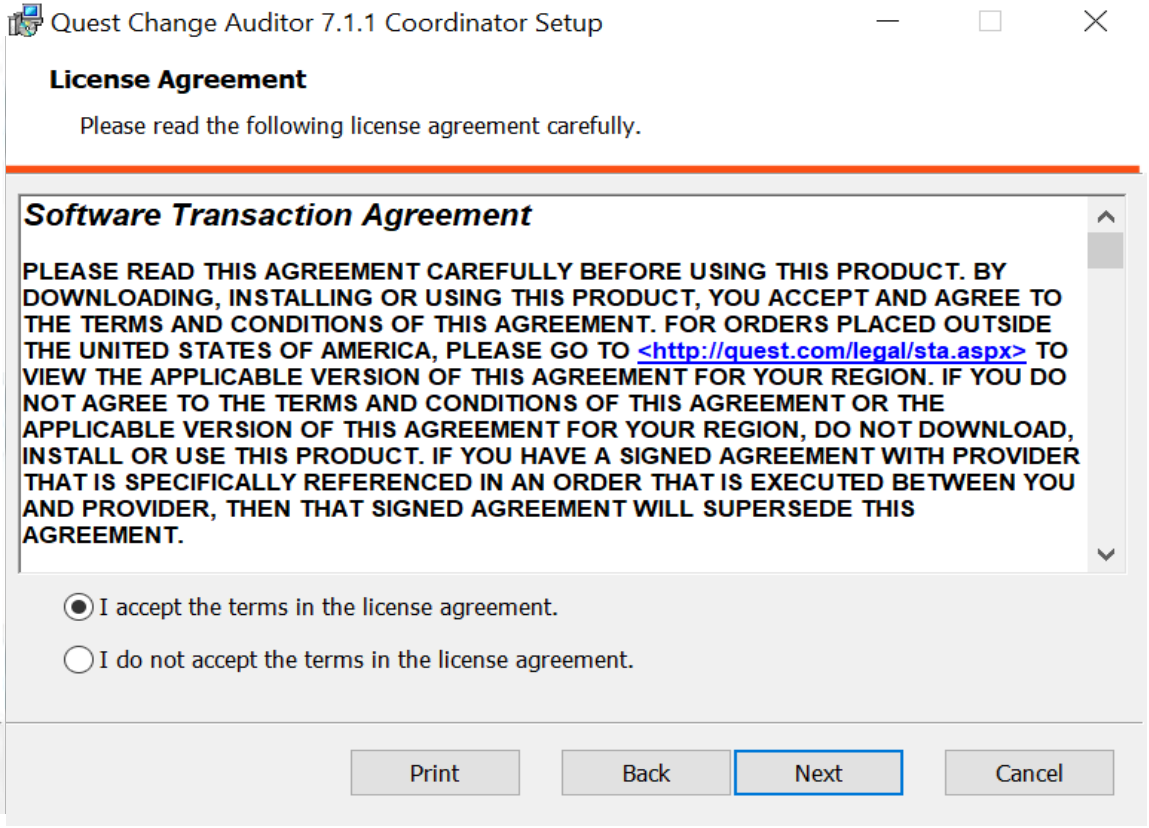
Change Auditor Coordinator のInstallボタンを選択します。

目次に戻る

Change Auditor Coordinator のインストール



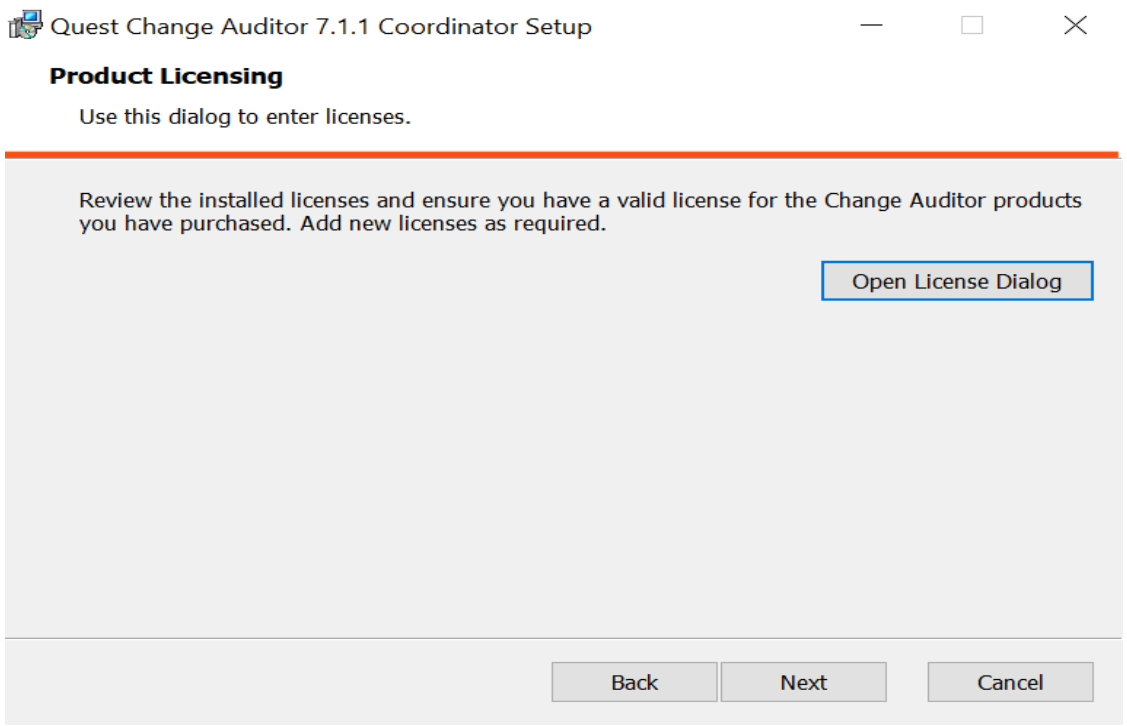
Nextをクリックして次に進みます。



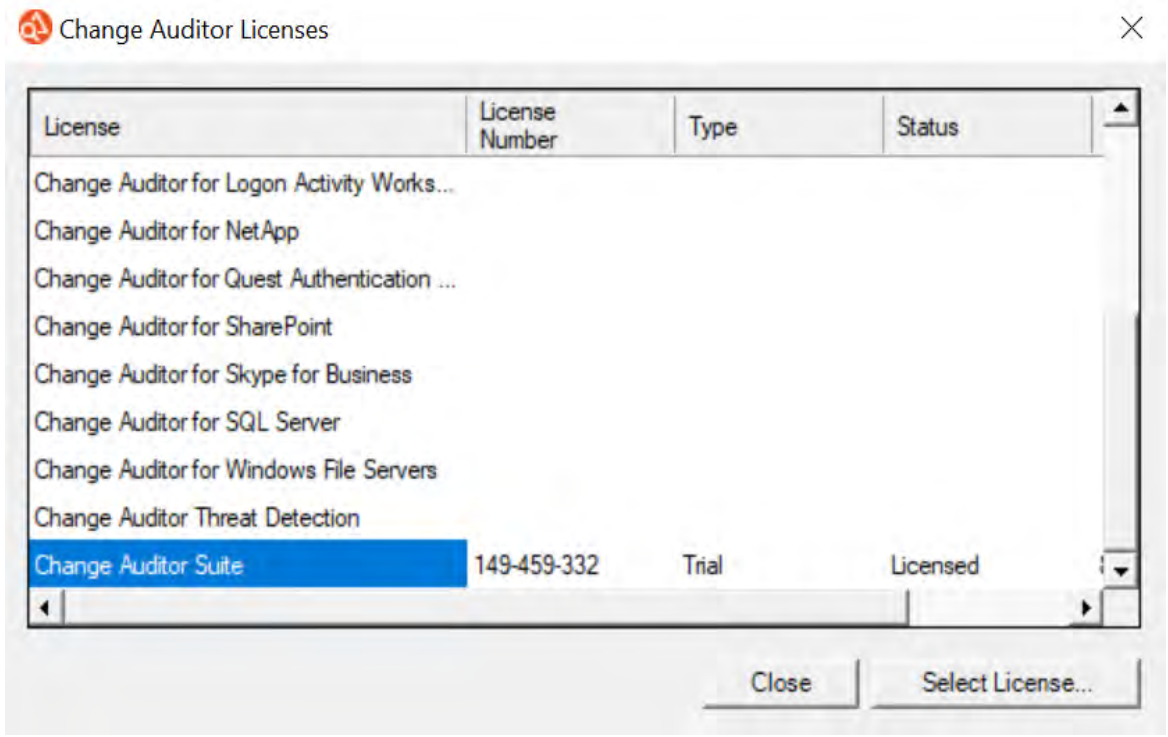
License Agreement でI accept… を選択して次に進みます。

目次に戻る

Change Auditor Coordinator のインストール



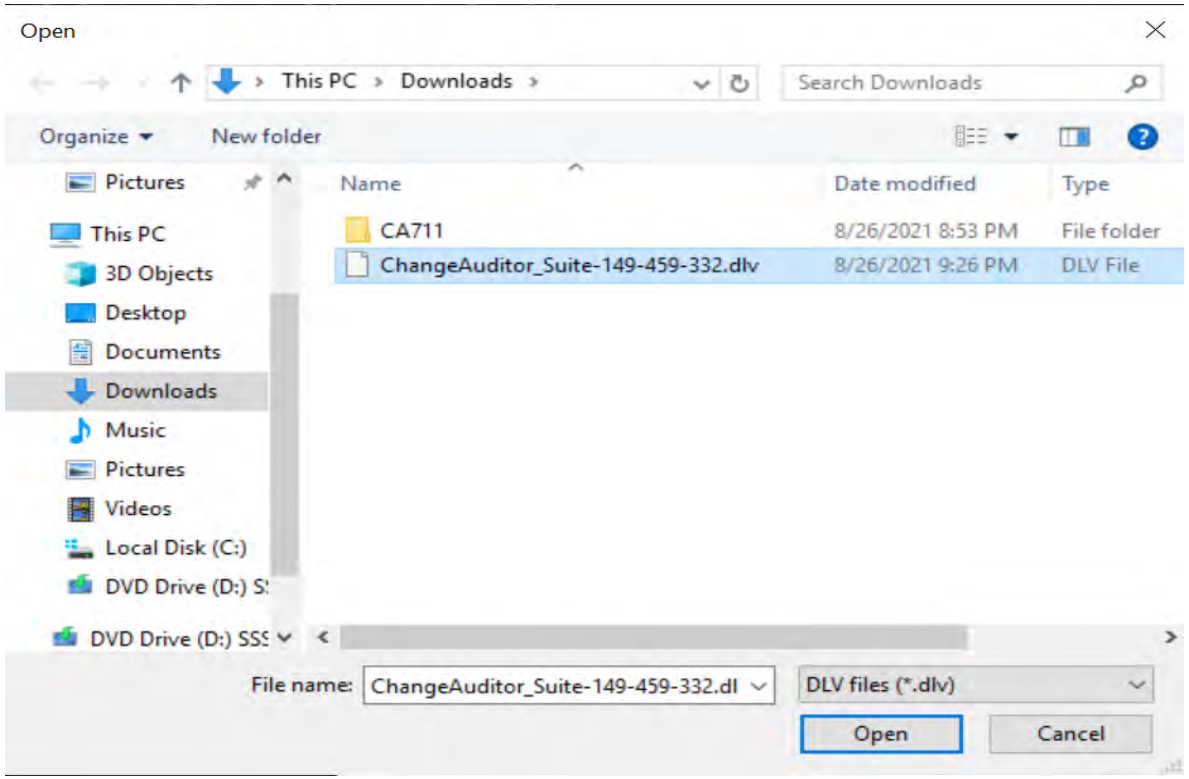
追加したいライセンスを選択し、Select License ボタンをクリックします。



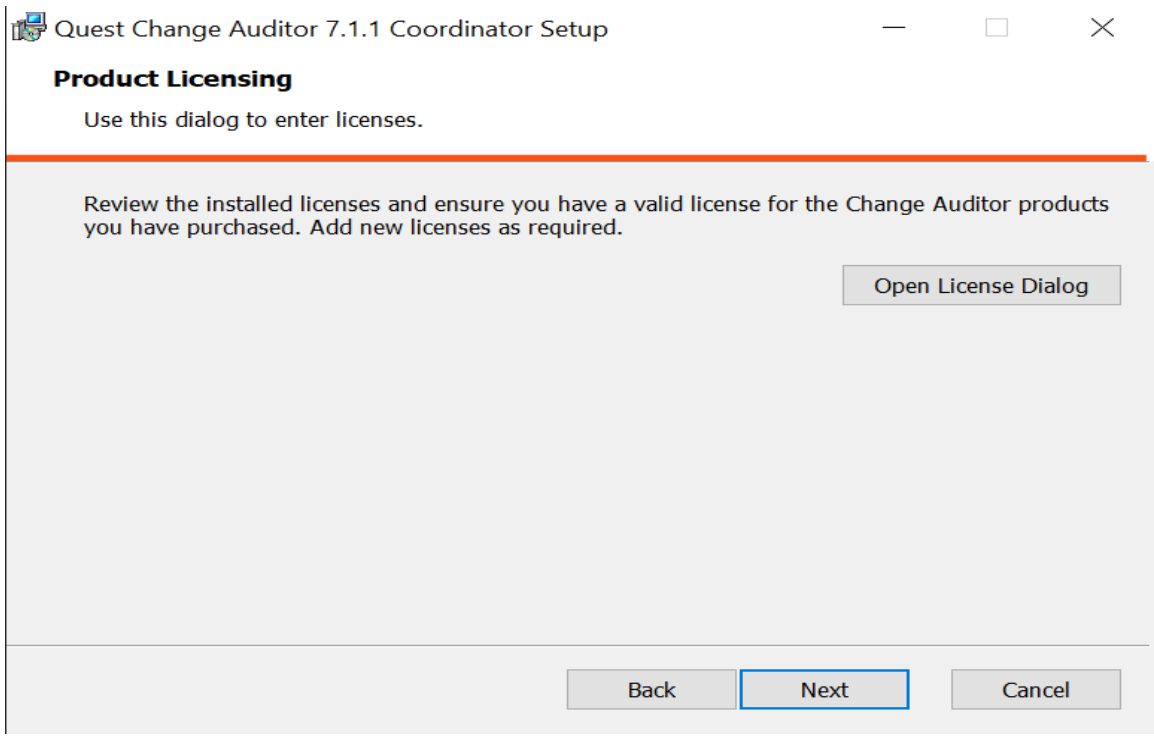
Open License Dialogボタンをクリックします。

目次に戻る

Change Auditor Coordinator のインストール



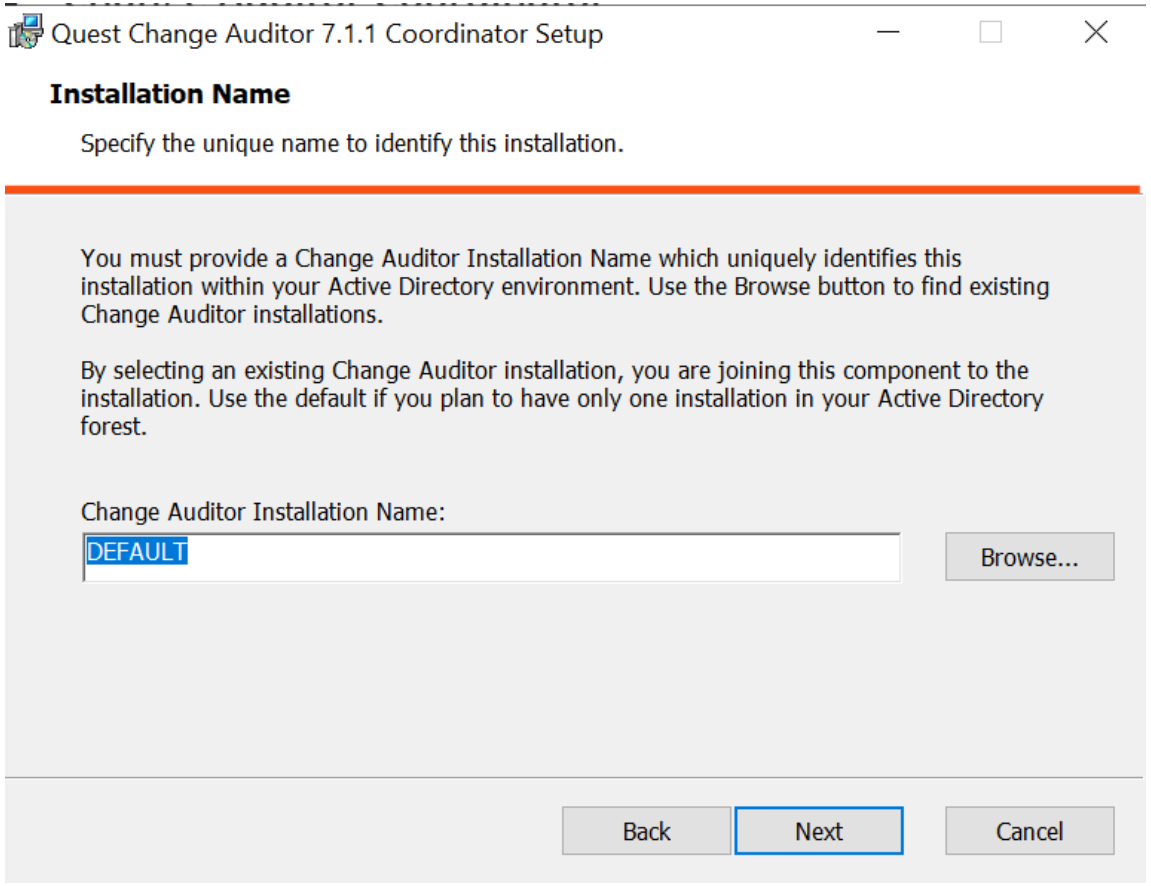
ライセンスファイル（.dlv）を選択します。



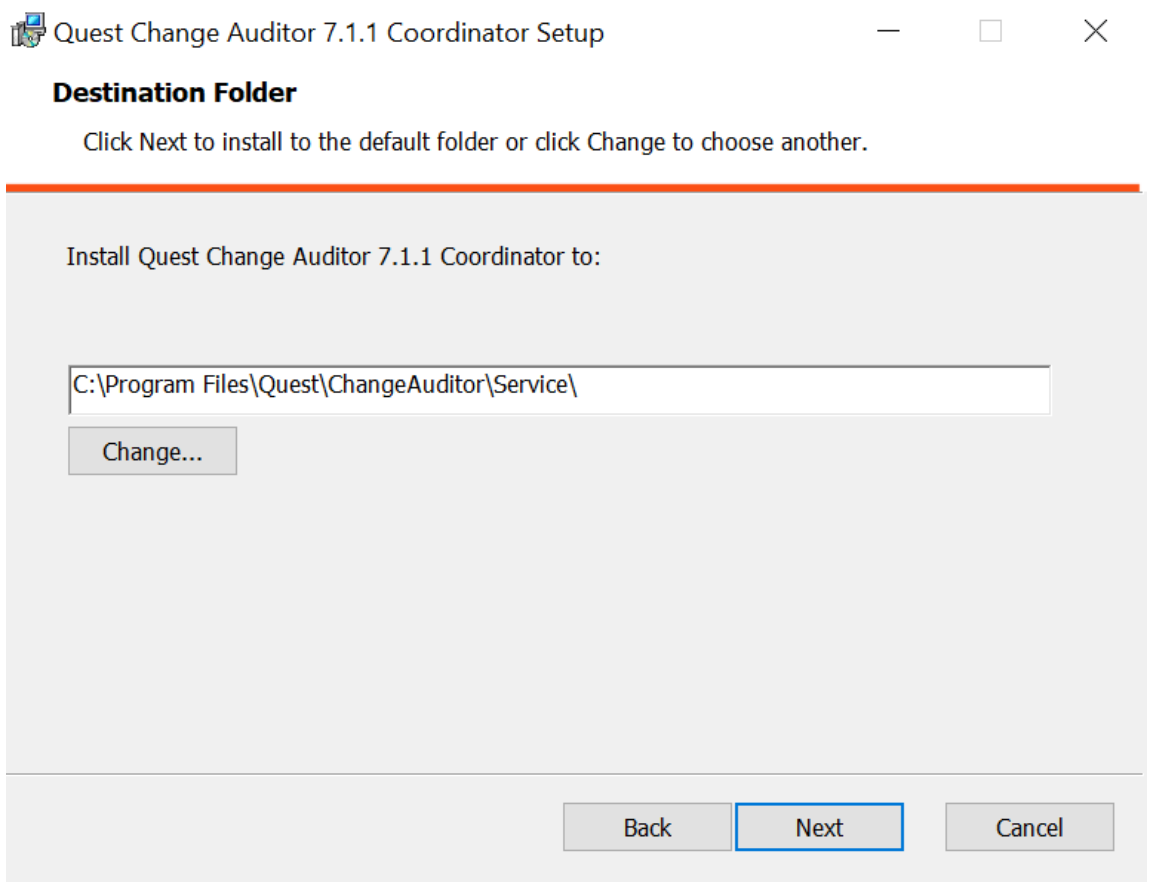
Nextをクリックして次に進みます。

目次に戻る

Change Auditor Coordinator のインストール



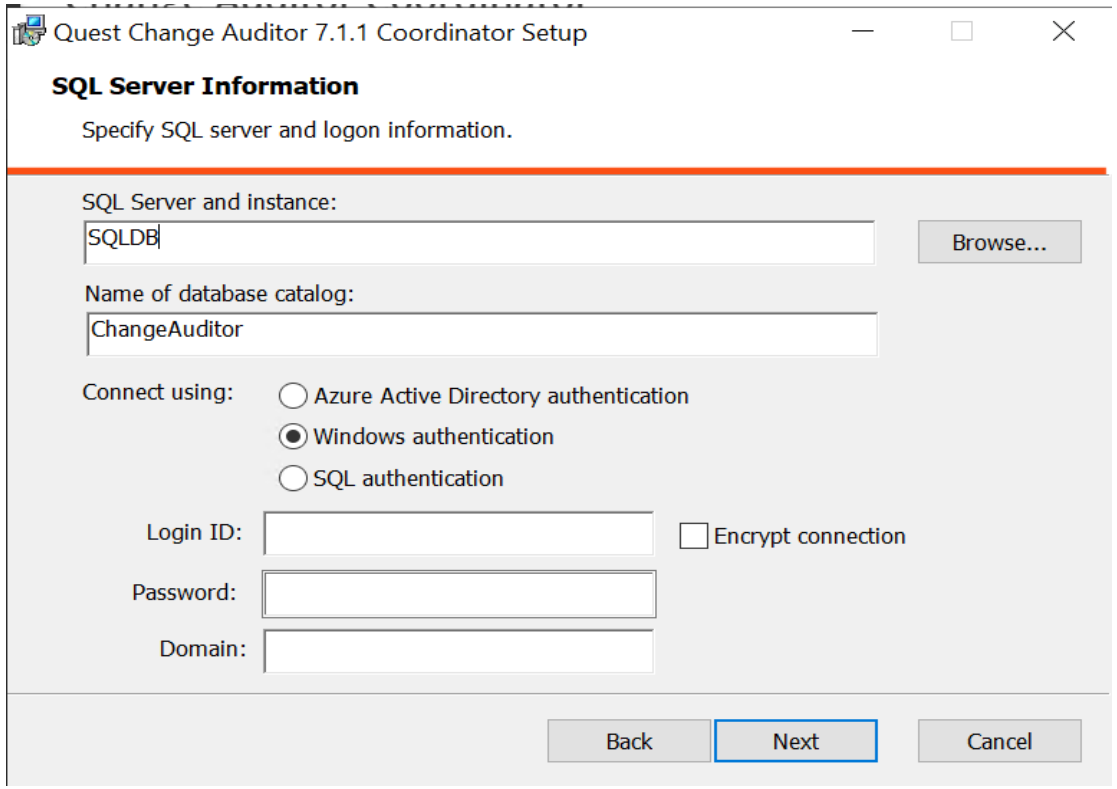
Change Auditor Coordinator前を入力し、次に進みます。



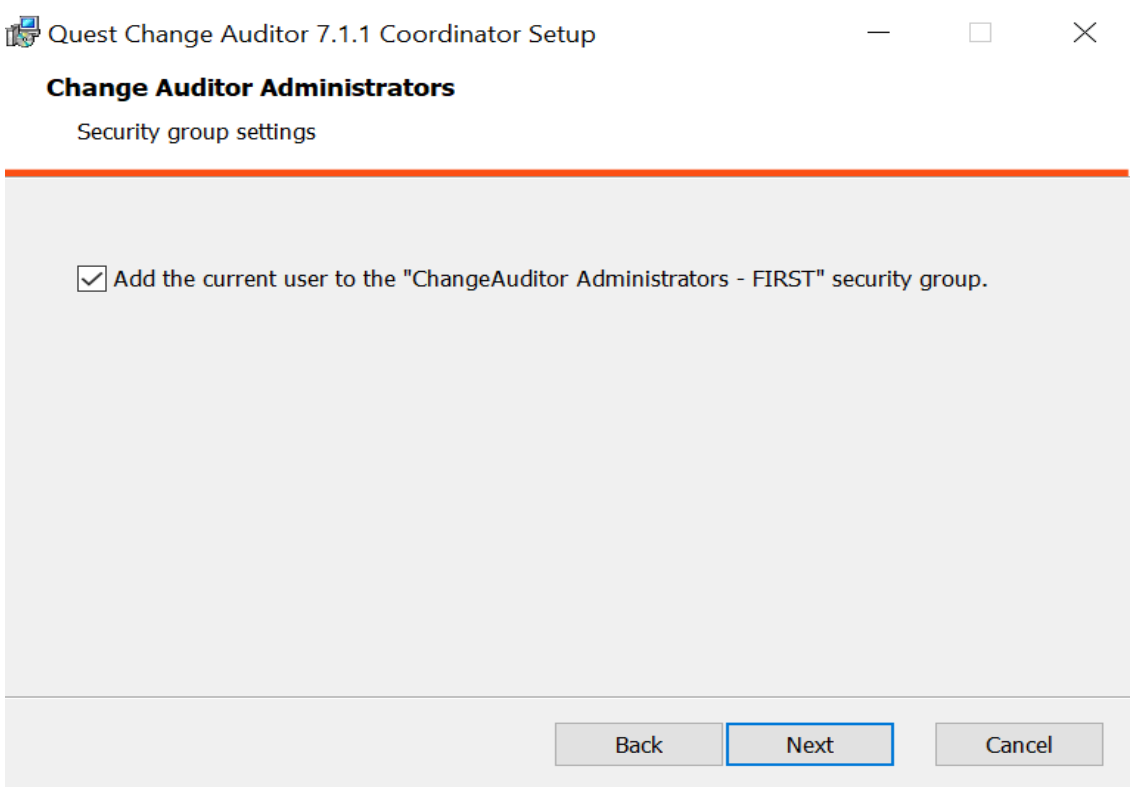
インストールの場所を指定して次に進みます。

目次に戻る

Change Auditor Coordinator のインストール



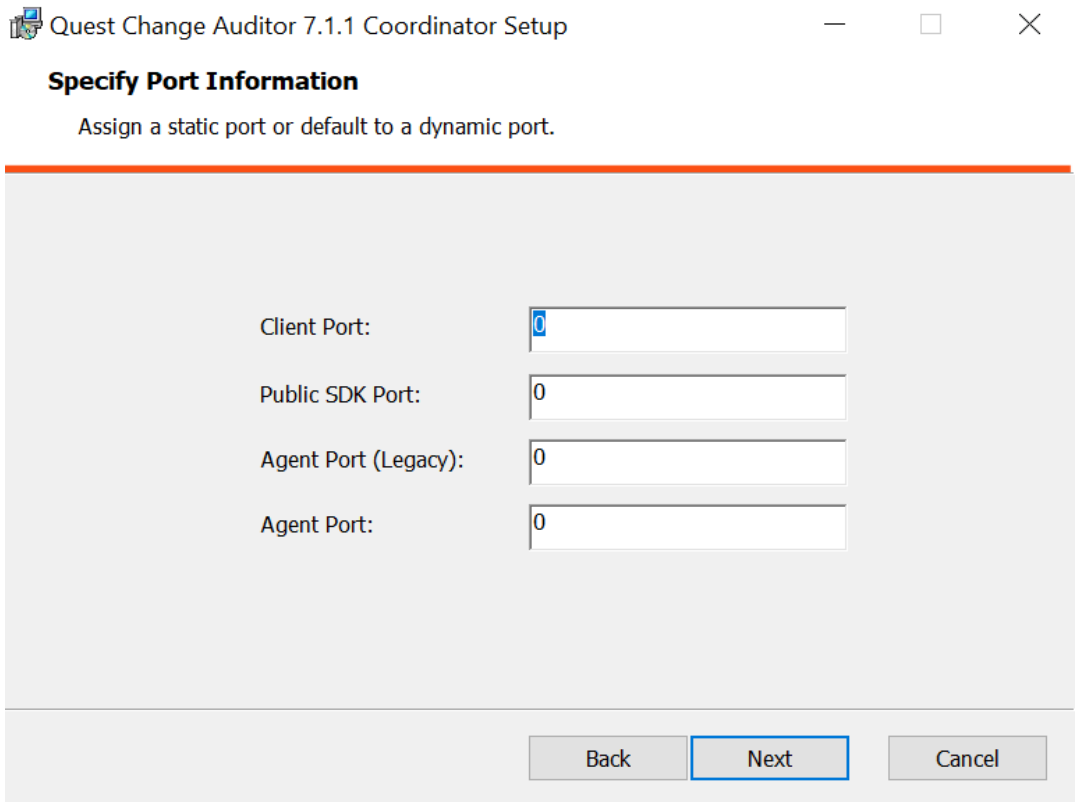
使用するSQL serverのインスタンスと認証情報を入力し次に進みます。



Add the current user…を選択し次に進みます。

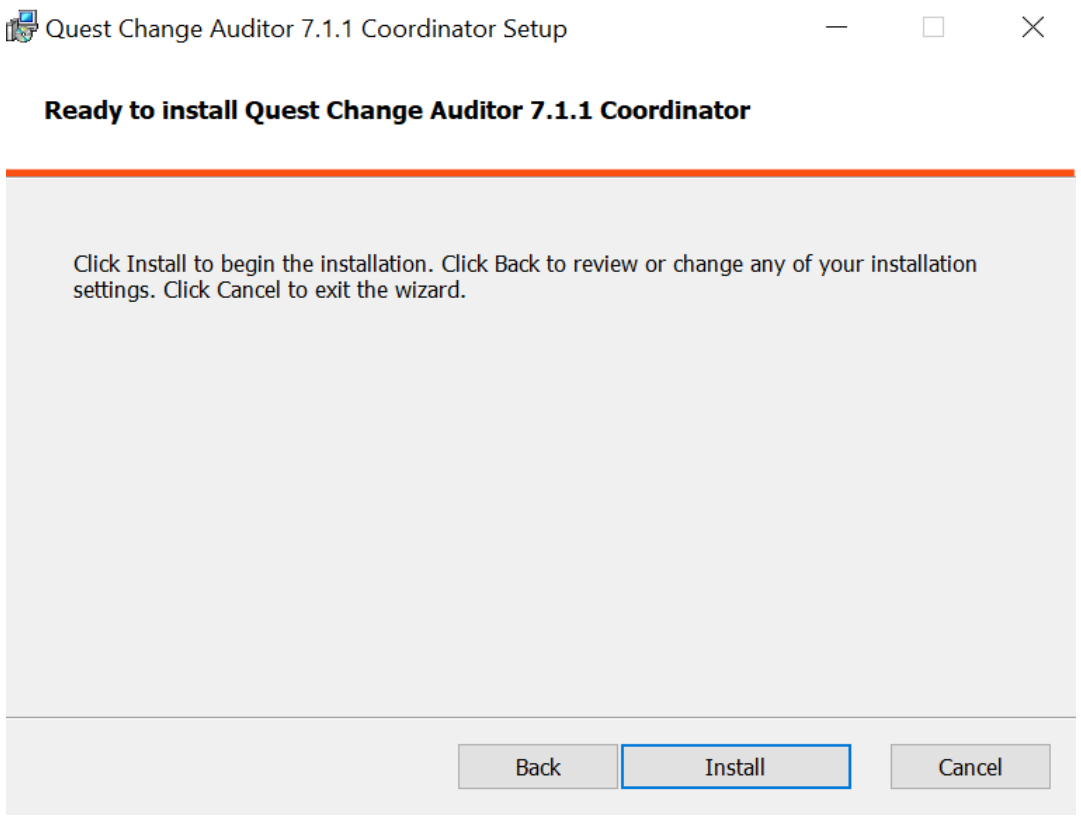
目次に戻る

Change Auditor Coordinator のインストール



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。

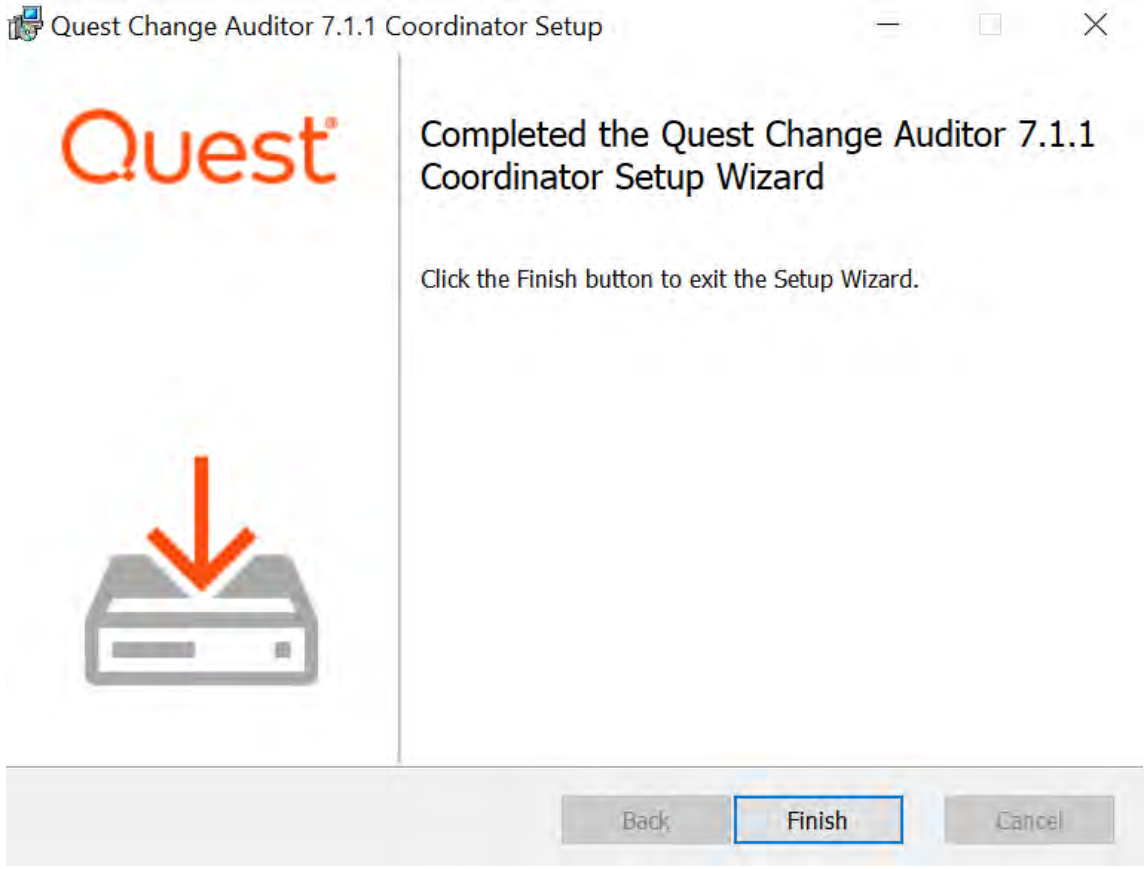
注：セロ（０）はダイナミックポートを示しています。



Installボタンをクリックしてインストールを開始します。

目次に戻る

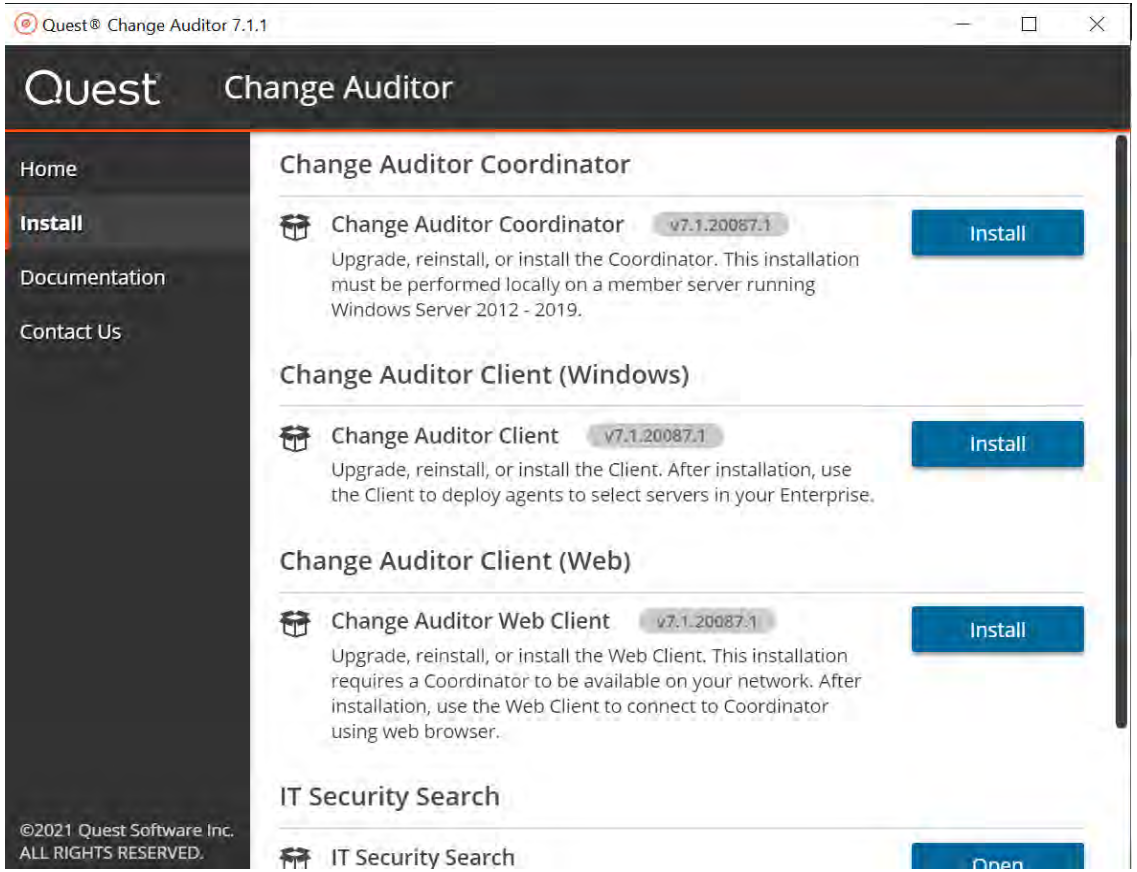
Change Auditor Coordinator のインストール



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。

目次に戻る

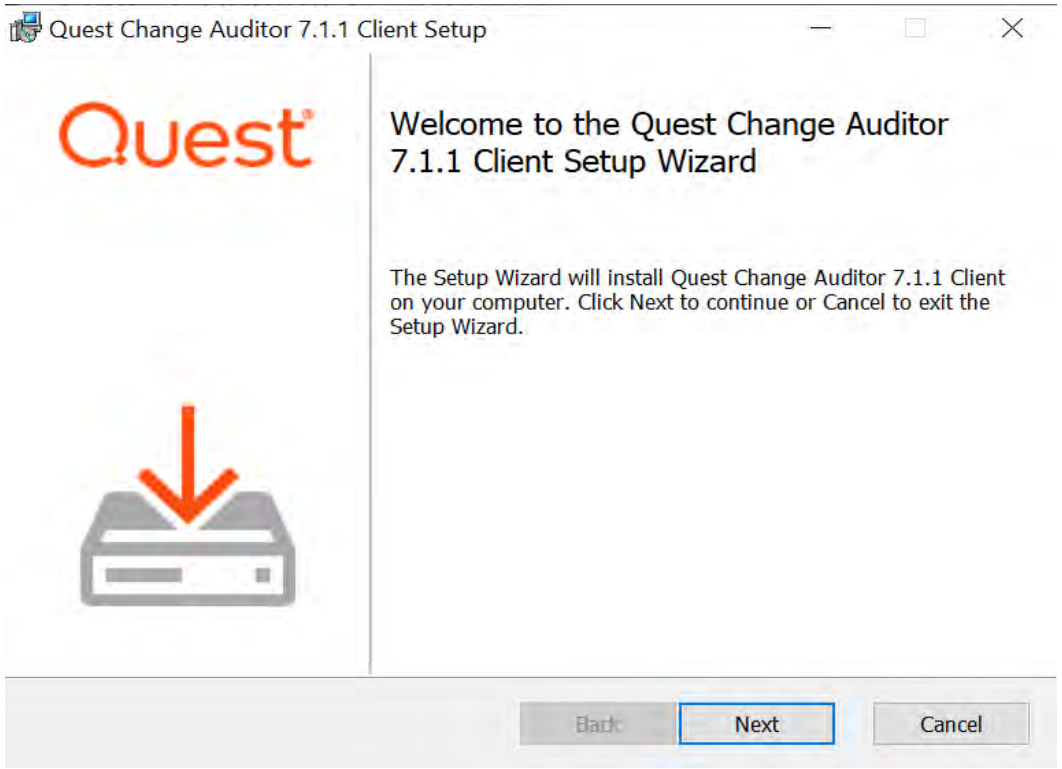
Change Auditor Client のインストール



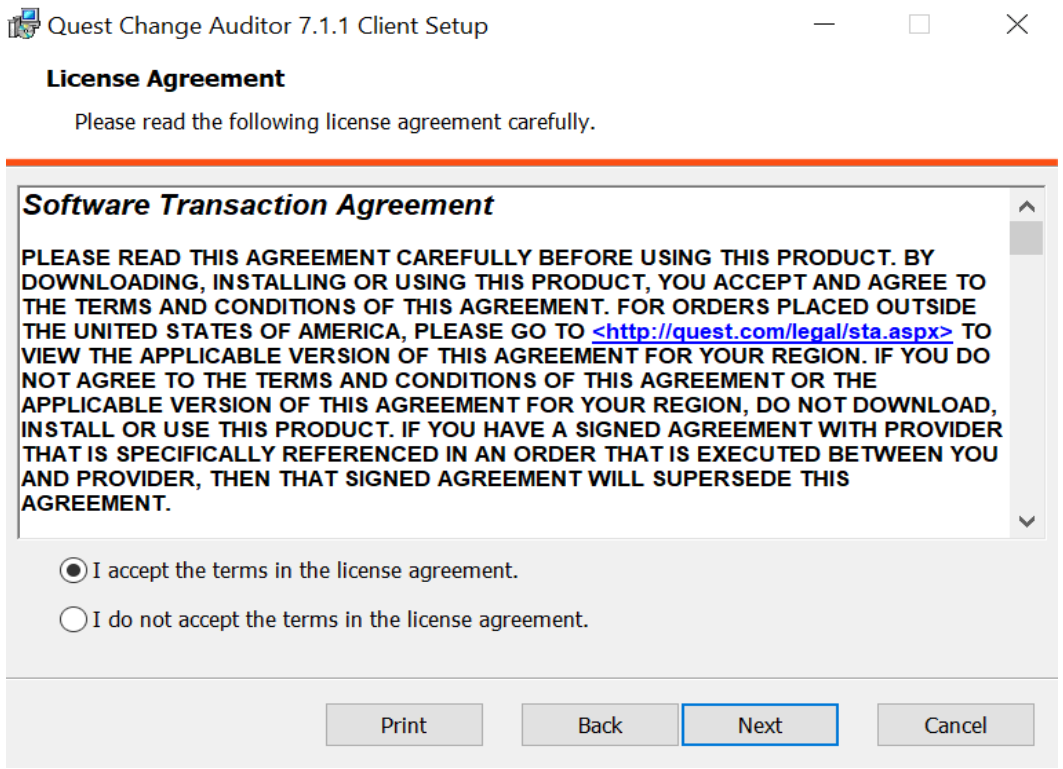
Change Auditor Client (Windows)のInstallボタンをクリックしてウィザードを開始します。

目次に戻る

Change Auditor Client のインストール



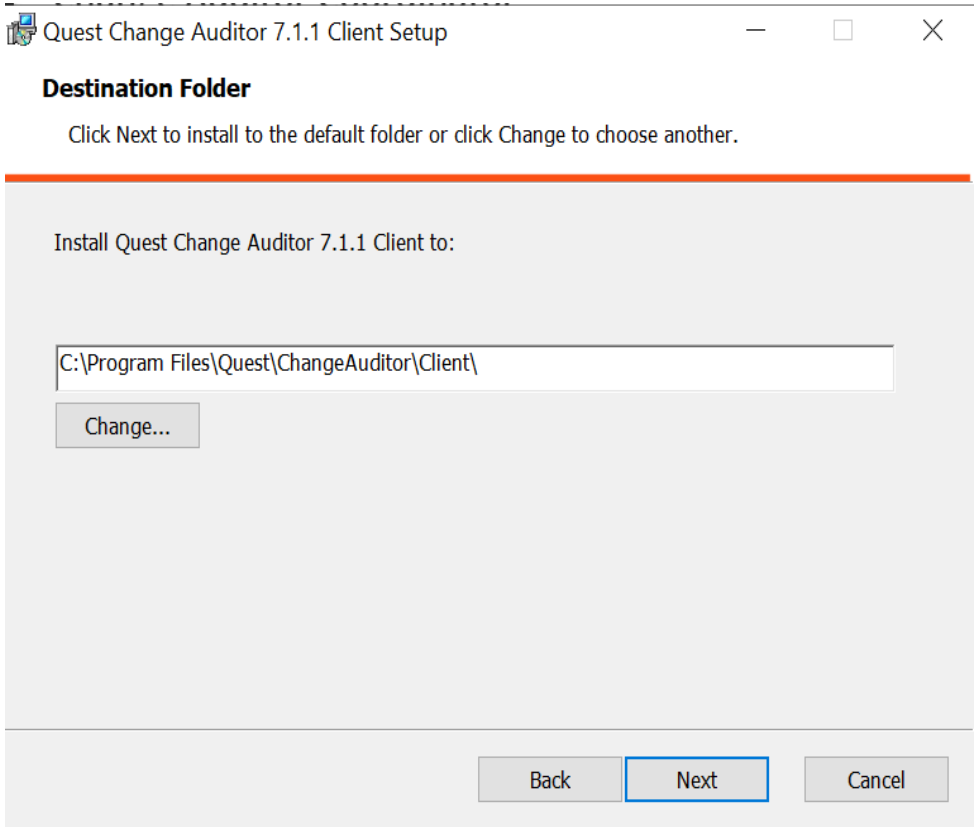
Nextをクリックして次に進みます。



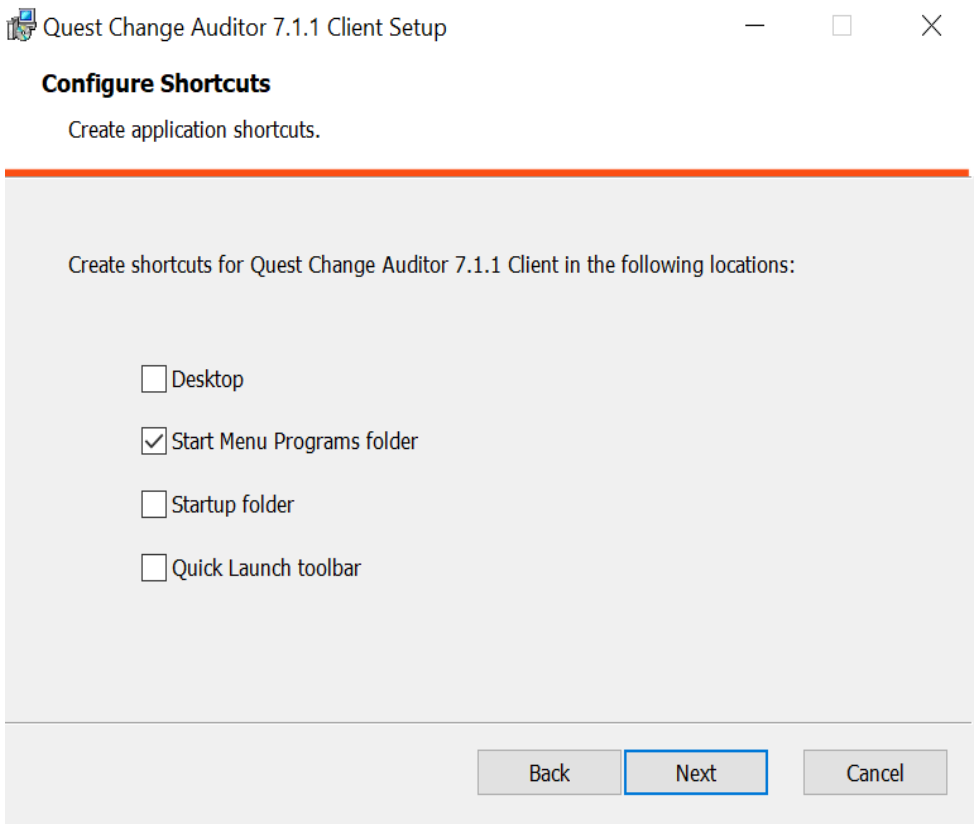
I accept…を選択し次に進みます。

目次に戻る

Change Auditor Client のインストール



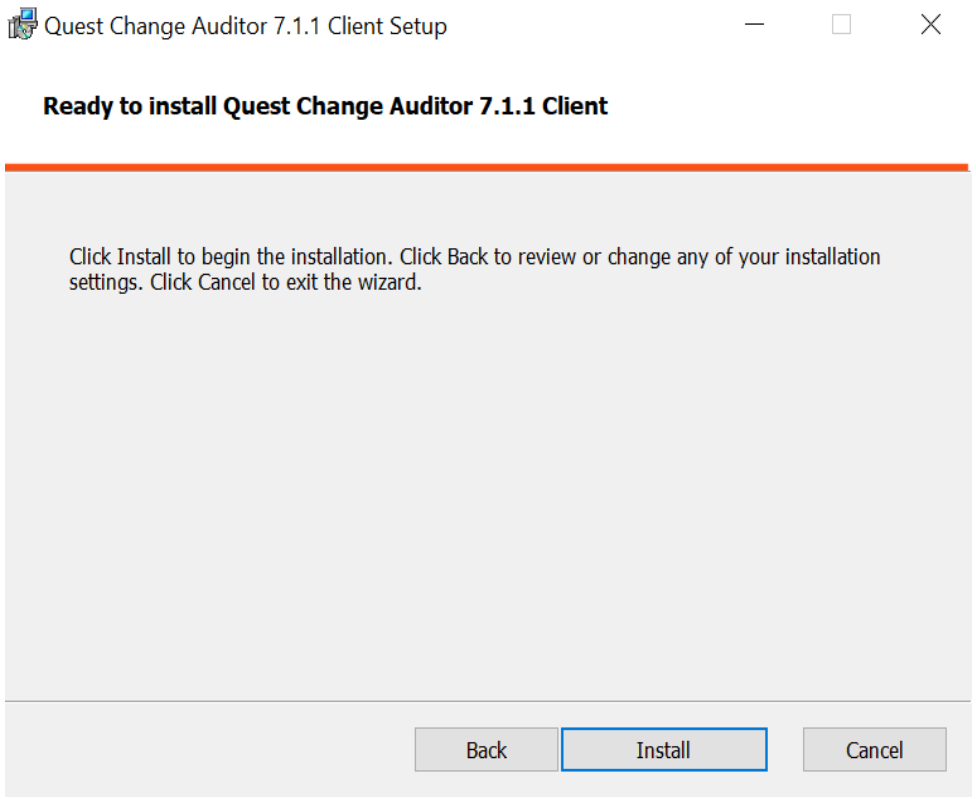
インストールの場所を指定して次に進みます。



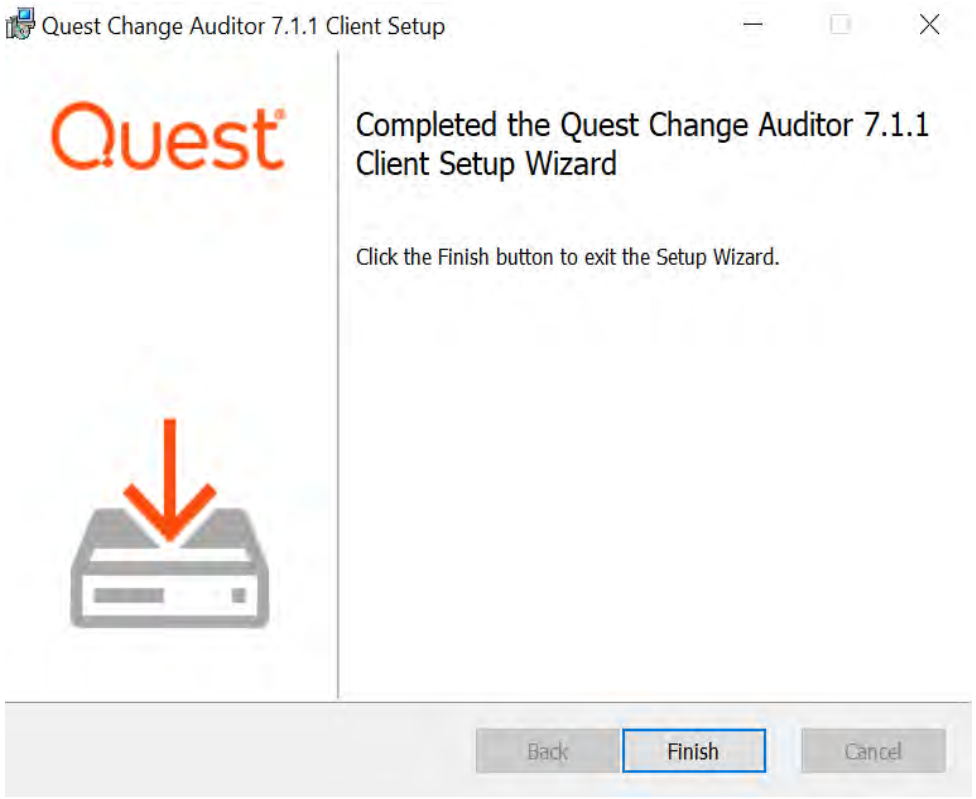
ショートカットを選択し次に進みます。

目次に戻る

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。

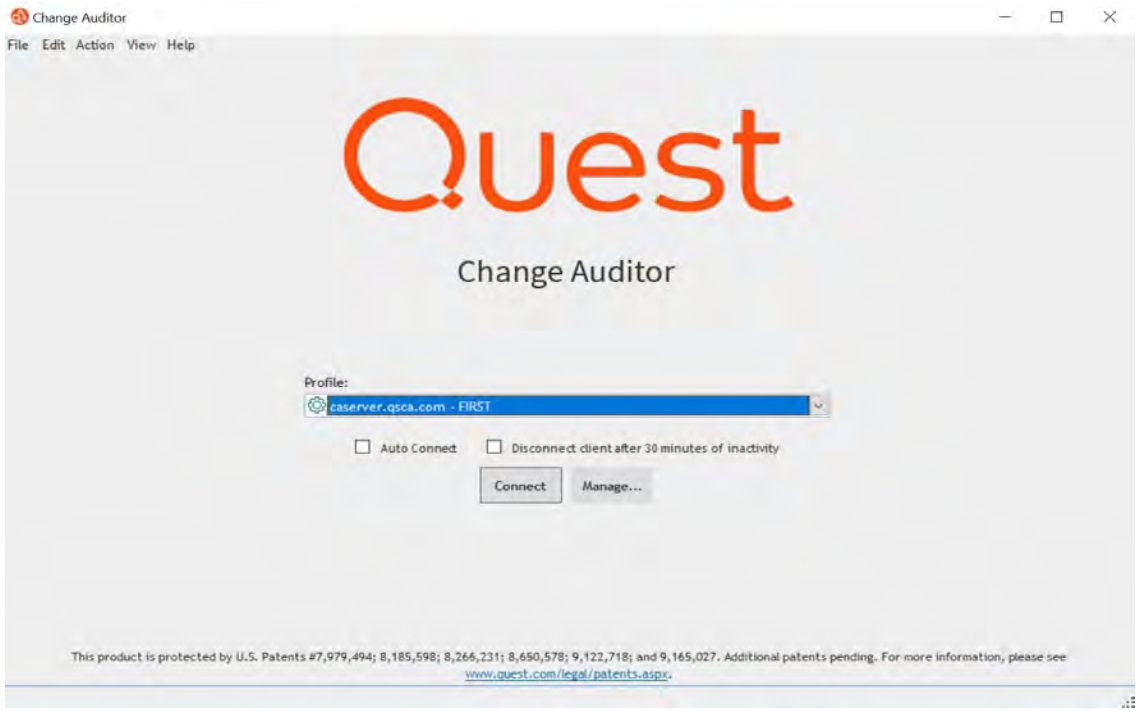
目次に戻る

Client の開始および エージェントのデプロイ

目次に戻る

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。



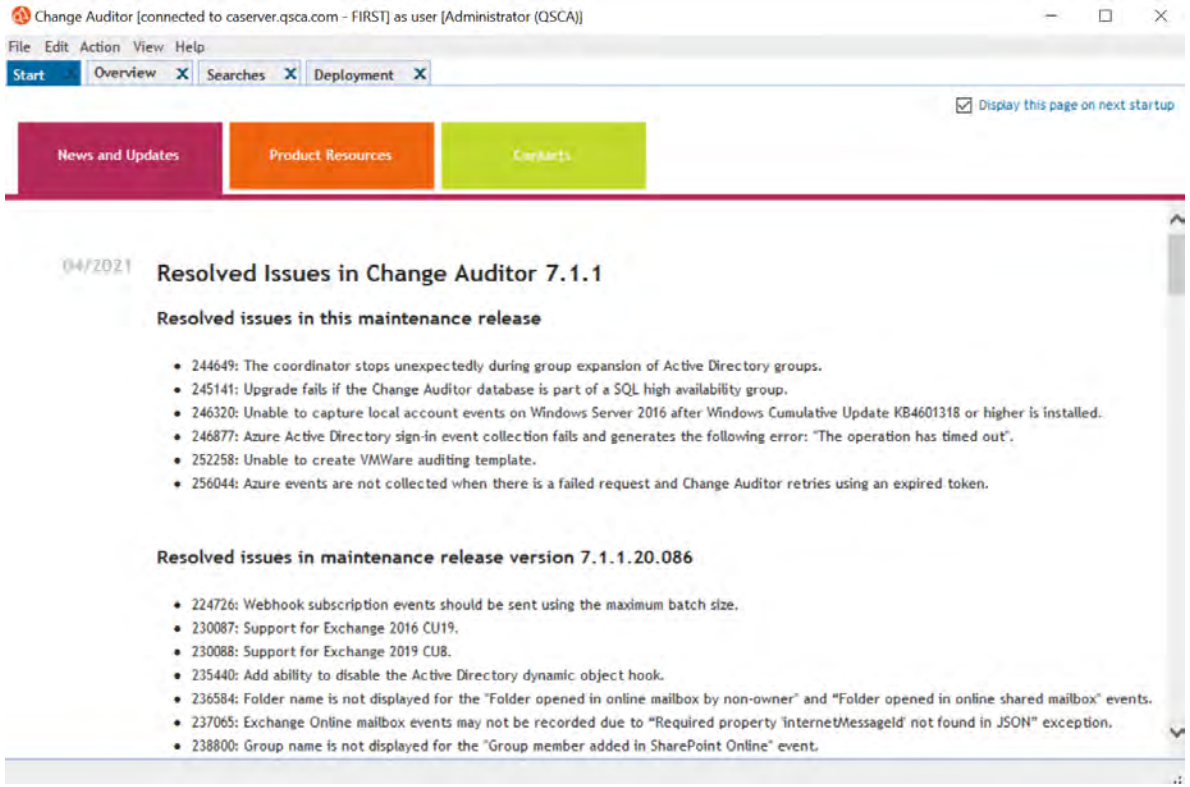
接続するChange Auditor Coordinatorを選択して
Connectをクリックしてます。

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
ChangeAuditor Administrators もしくはChangeAuditor 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でデプロイします。

目次に戻る

クライアントの開始

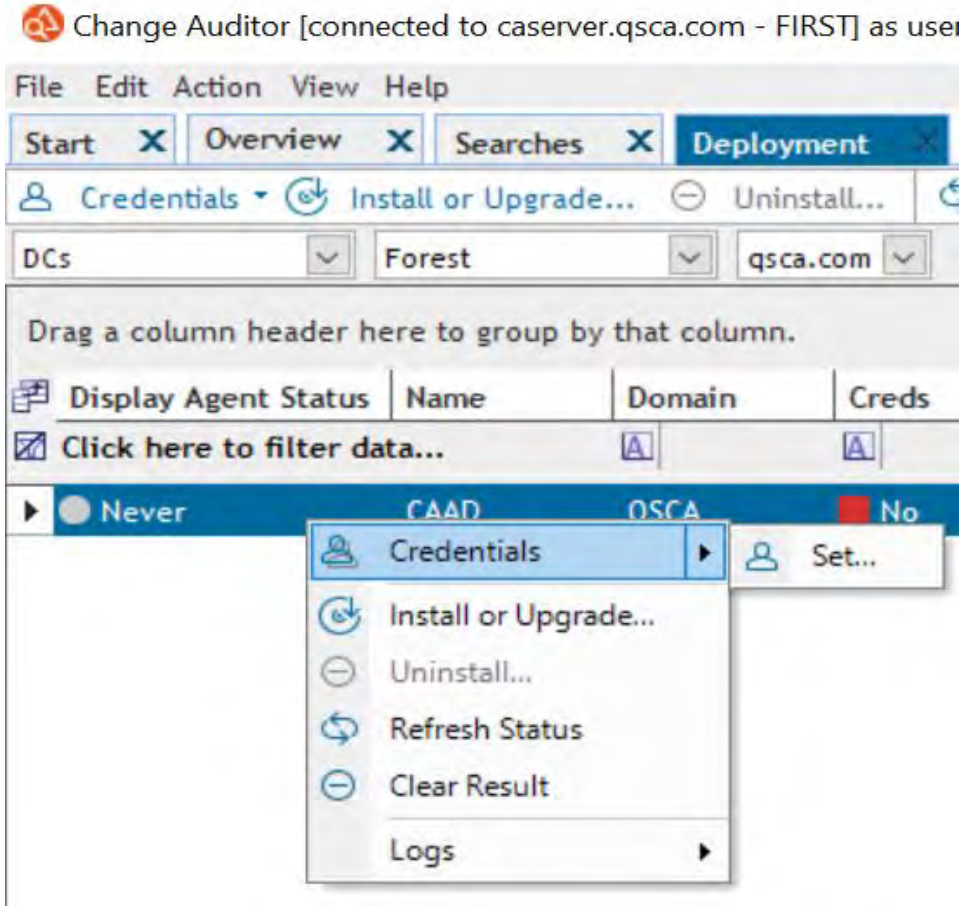


接続が成功すると、スタートページが表示されます。

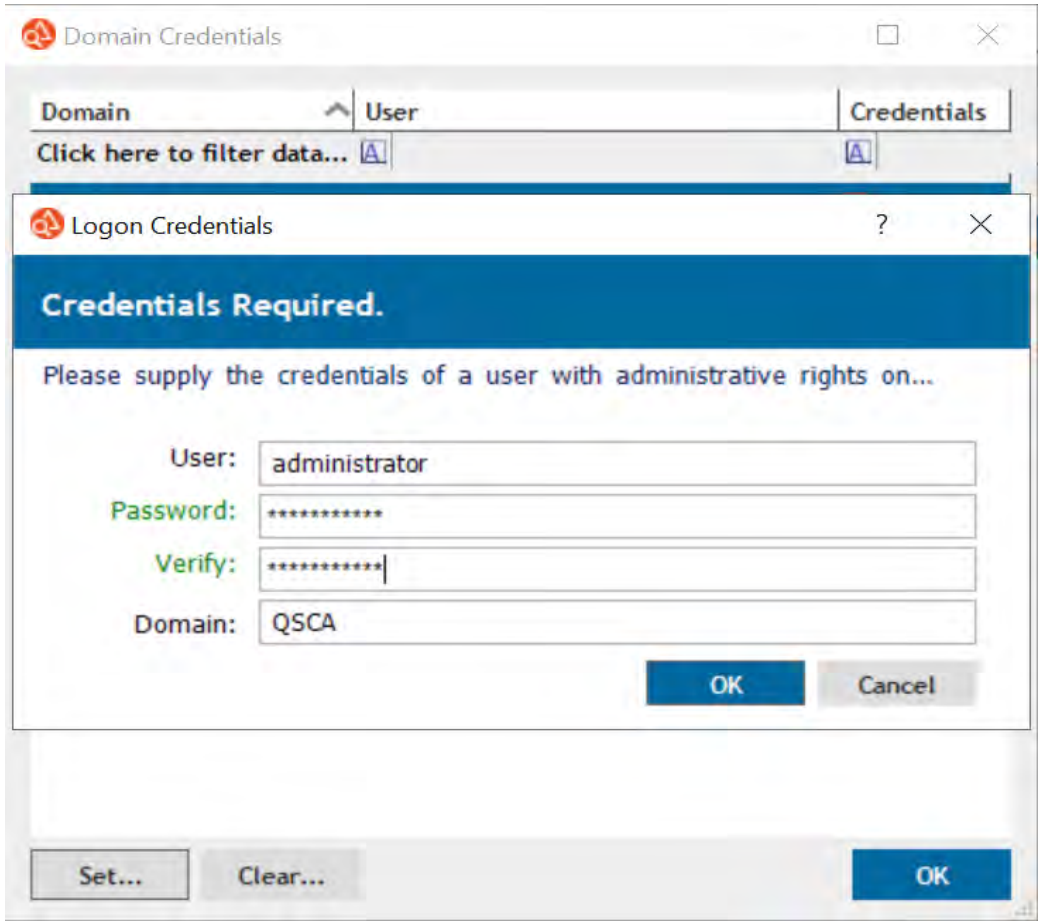
Deploymentタブをクリックしてエージェントをでデプロイします。

目次に戻る

エージェントのデプロイ



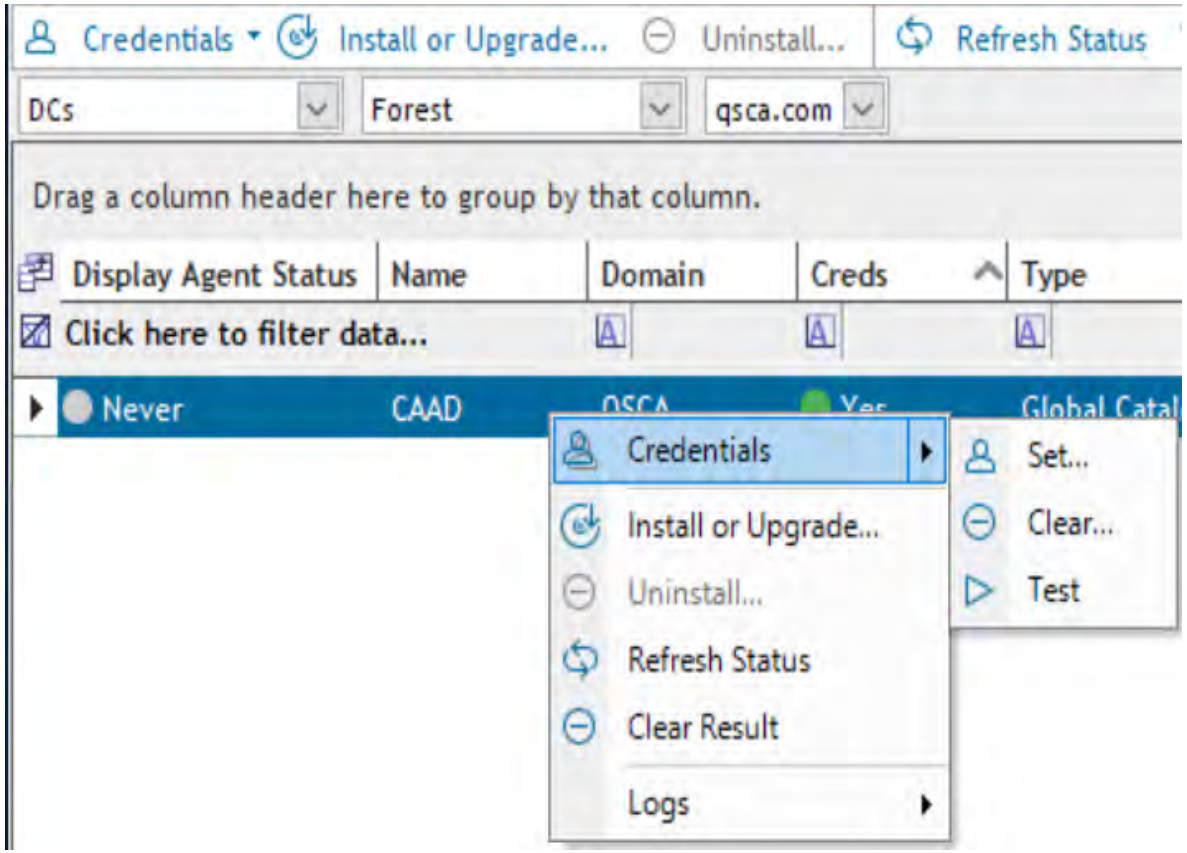
Deploymentタブでエージェントをインストールするシステムを選択して、右クリック→Credentials →Setを選択します。



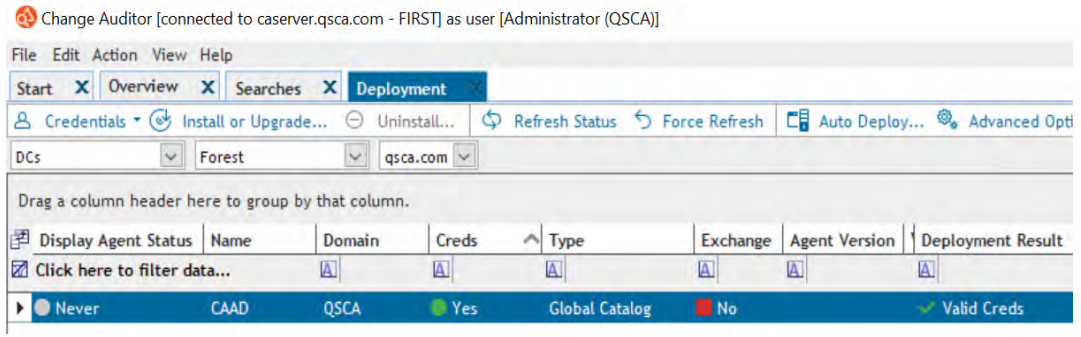
SetボタンをクリックしてLogon Credentials を開きます。
ユーザ名、パスワードを入力してOKをクリックします。

目次に戻る

エージェントのデプロイ



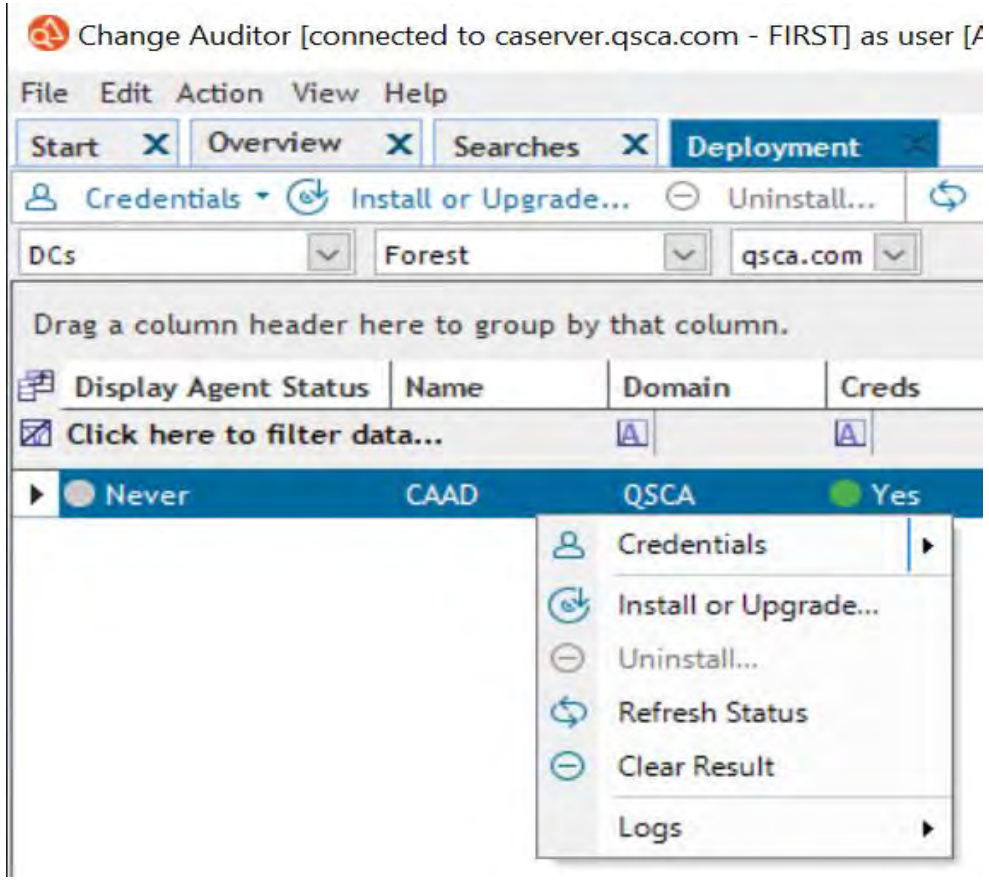
認証の設定後、対象のシステムを右クリック→Credentials→Testを選択します。



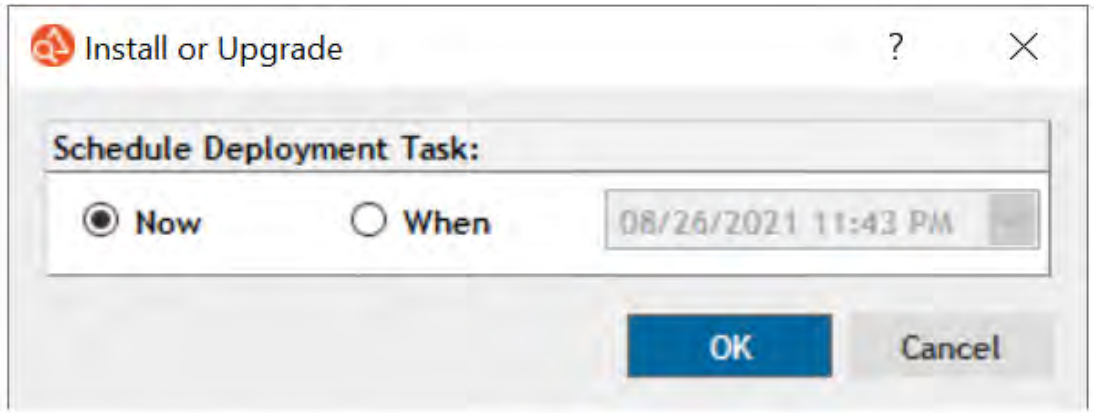
Deployment ResultにValid Credsが表示されたことを確認後、インストールを実行します。

目次に戻る

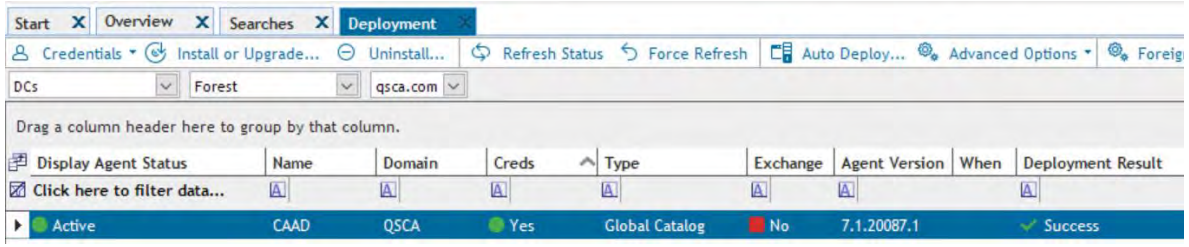
エージェントのデプロイ



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。

目次に戻る

Active Directory の監査

目次に戻る

Active Directory の変更とクエリ

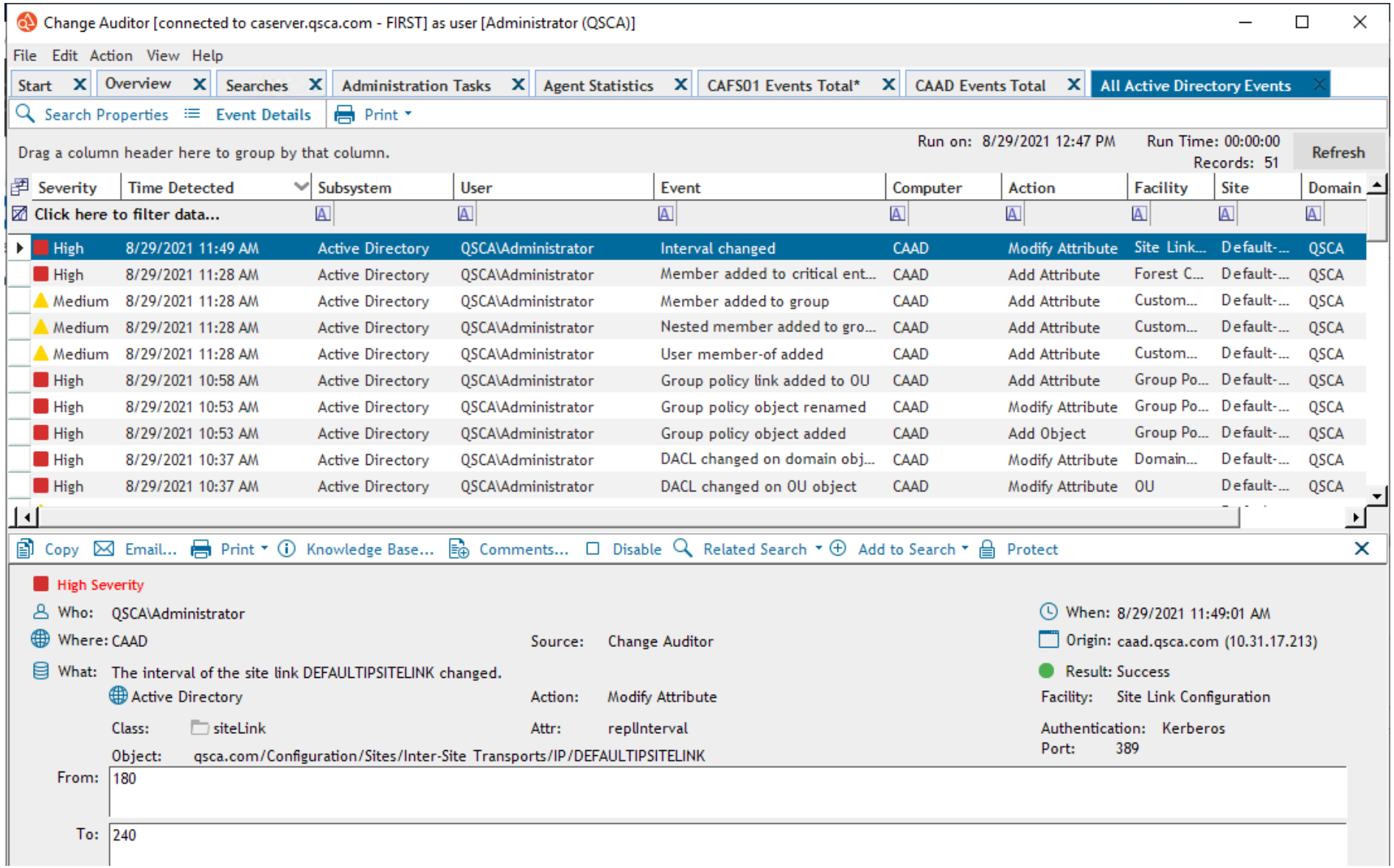
このセクションでは、Active Directory に変更を加えて後のインベント生成および表示の手順を説明します。

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DEFAULTSITELINK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)

目次に戻る



図：Active Directory イベント

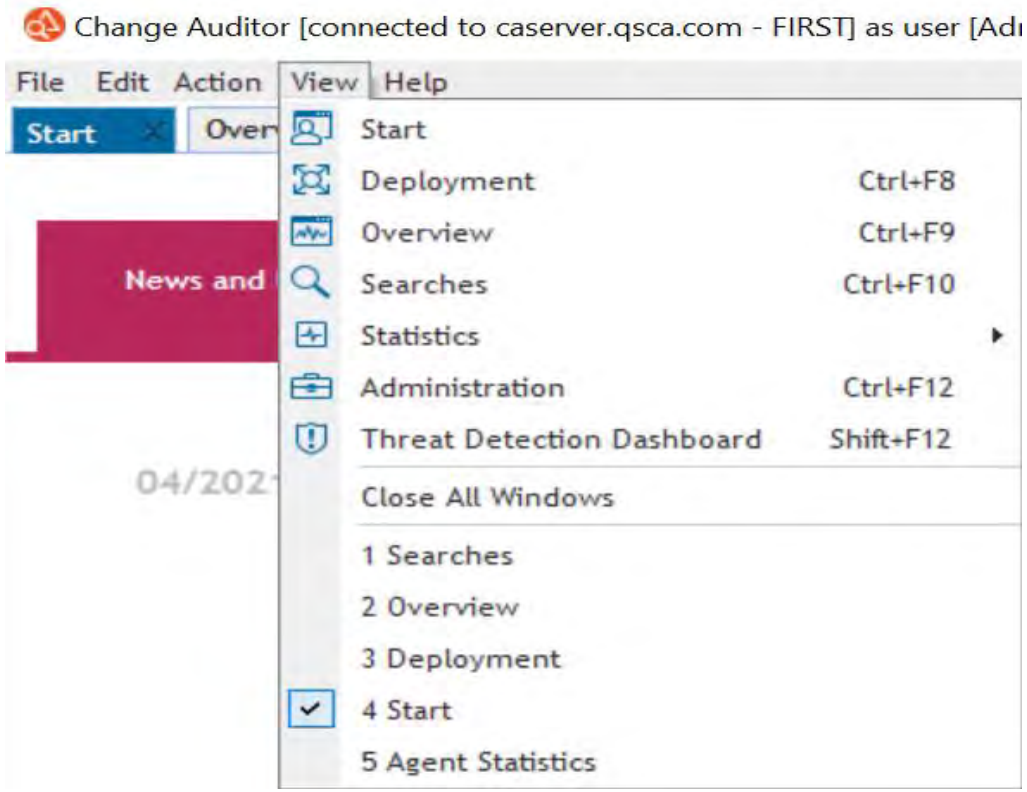
目次に戻る

Windows File System の監査

目次に戻る

File Systemのテンプレート設定

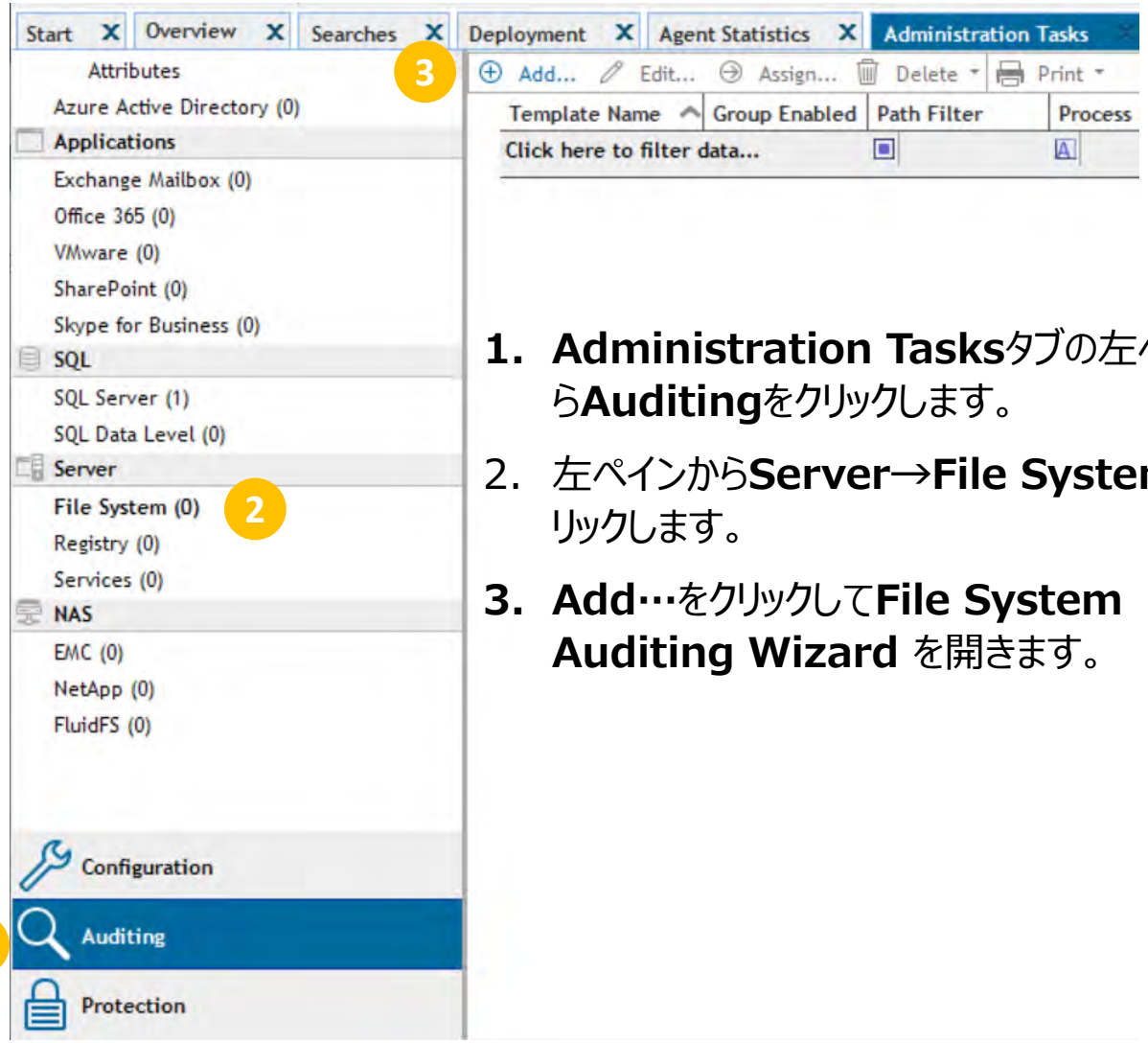
このセクションではFile Systemの監査に必要なテンプレートを作成する手順を説明します。



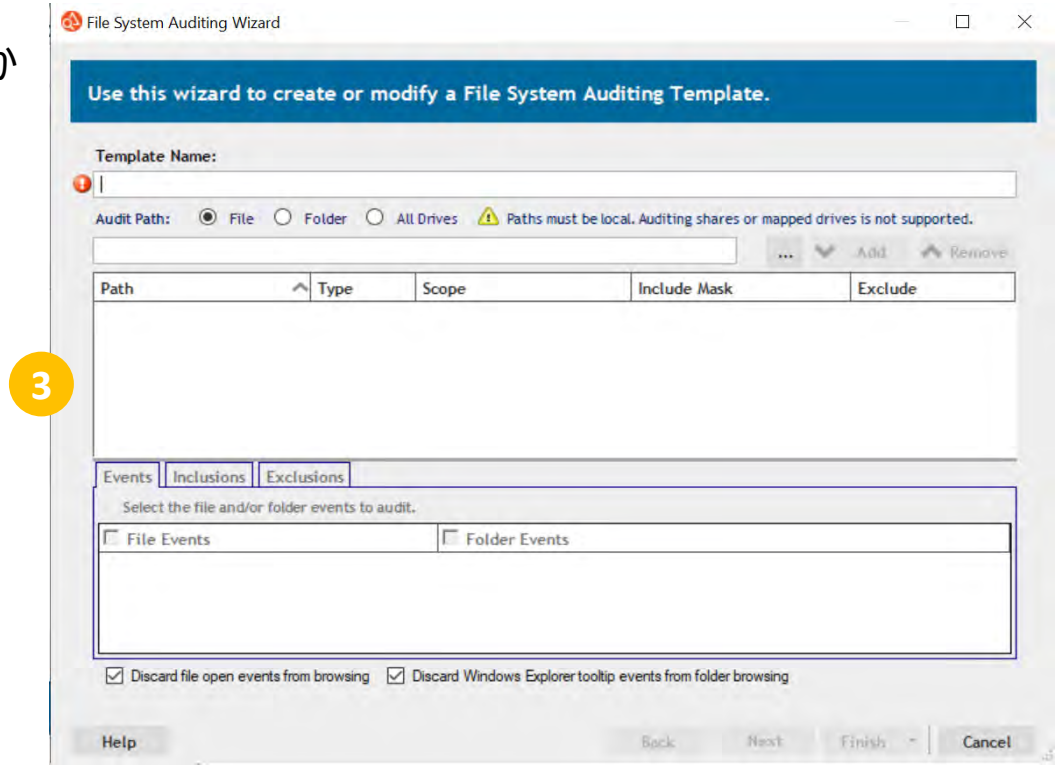
View →Administrationを選択します。

目次に戻る

File Systemのテンプレート設定

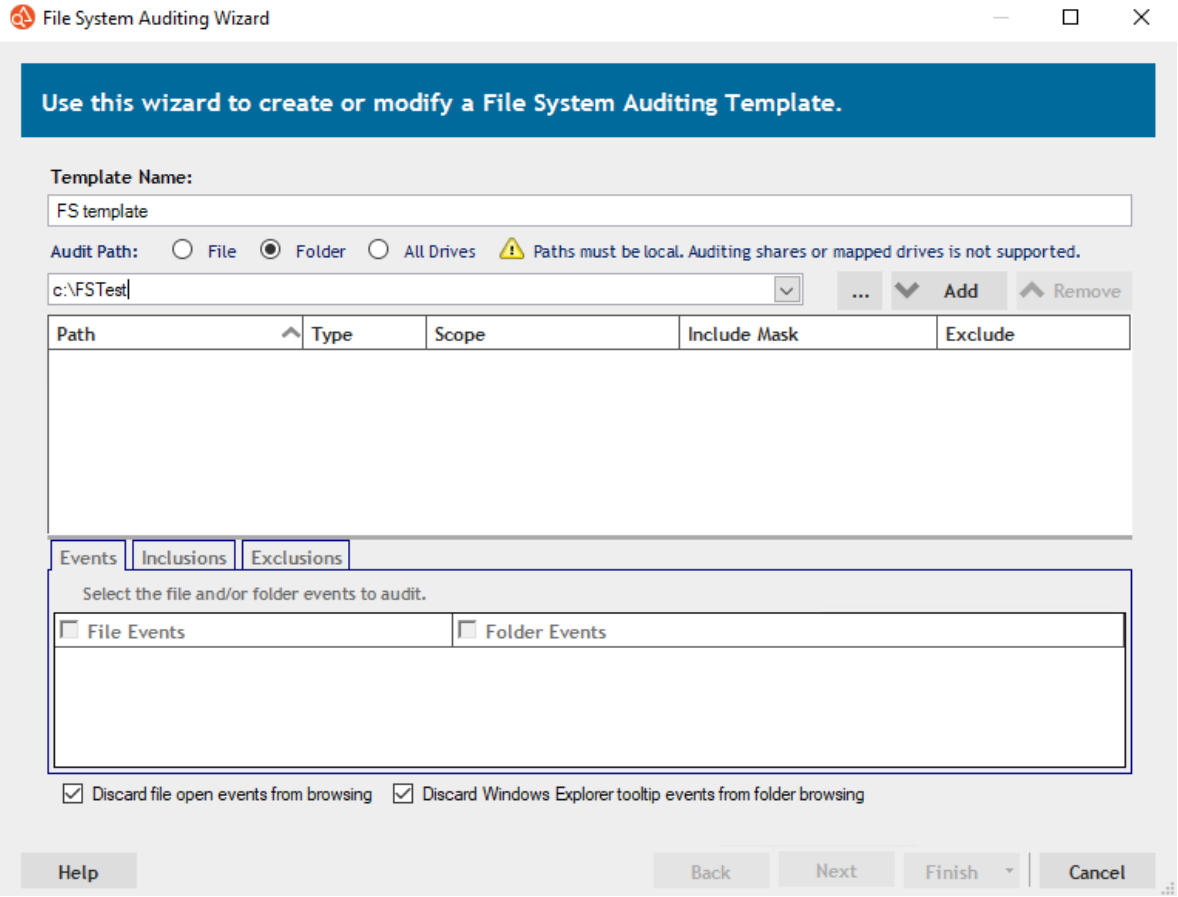


1. **Administration Tasks**タブの左ペインから**Auditing**をクリックします。
2. 左ペインから**Server→File System**をクリックします。
3. **Add…**をクリックして**File System Auditing Wizard** を開きます。



目次に戻る

File Systemのテンプレート設定

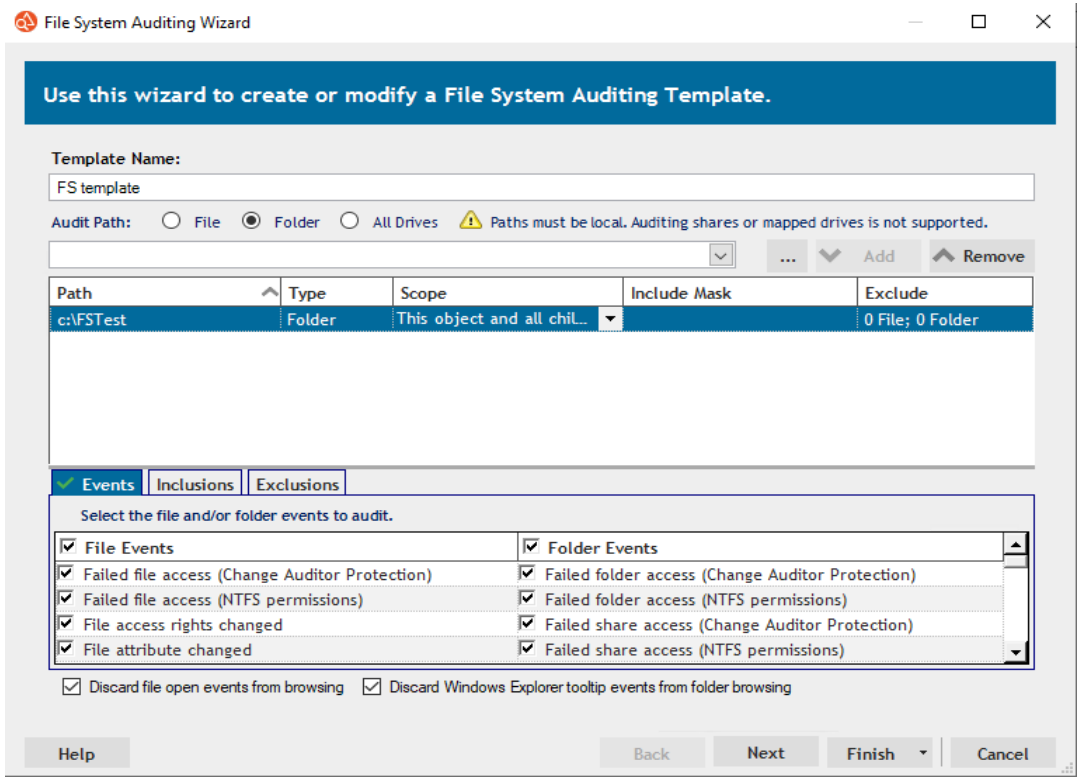


1. **Template**名を入力します。
2. **Audit Path**で**Folder**rを選択し、パスを指定します。**Add**をクリックしてパスを追加します。

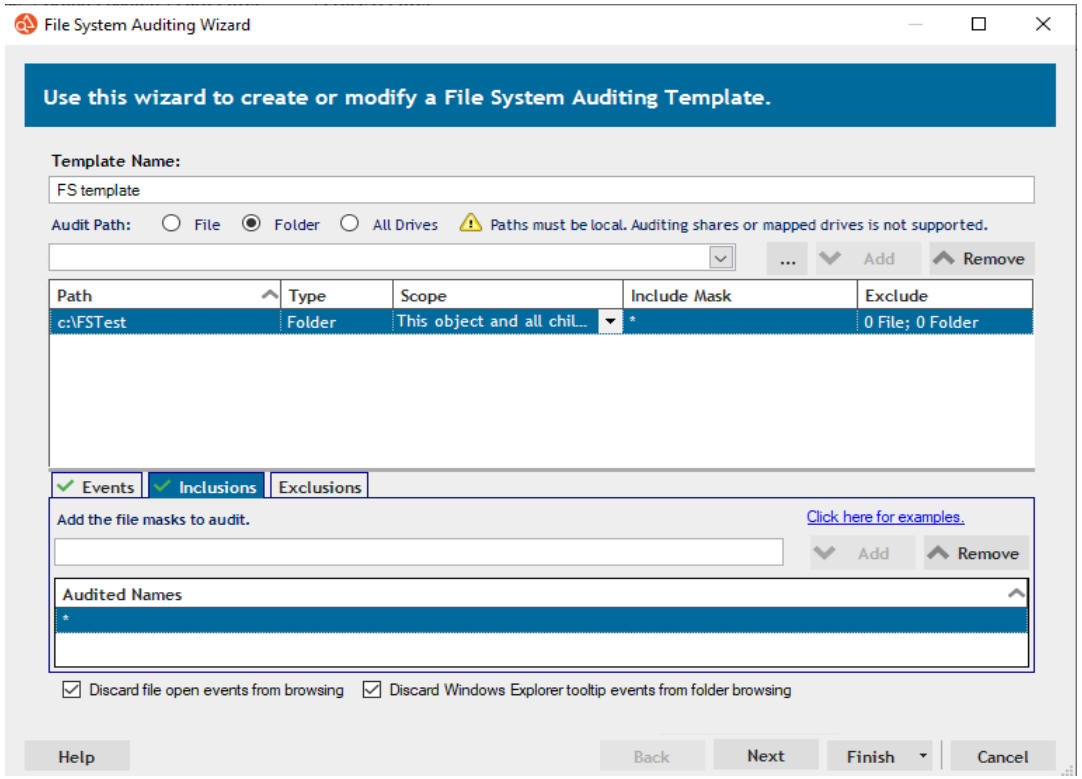
注：ファイルサーバー上のローカルのパスを指定します。共有もしくはマップしたドライブは未対応です。

目次に戻る

File Systemのテンプレート設定



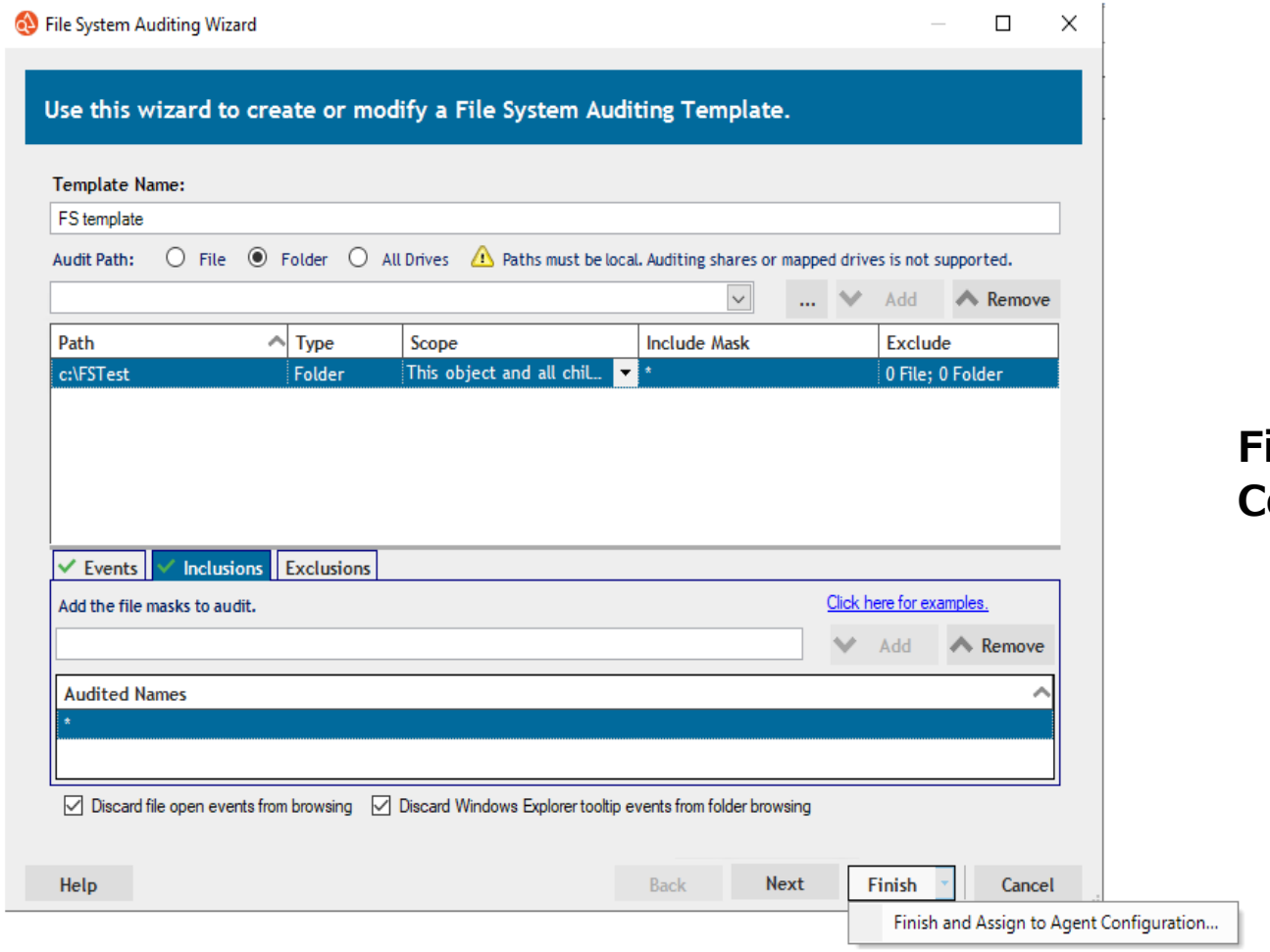
Eventタブで**File Events**と**Folder Events**を選択します。



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

目次に戻る

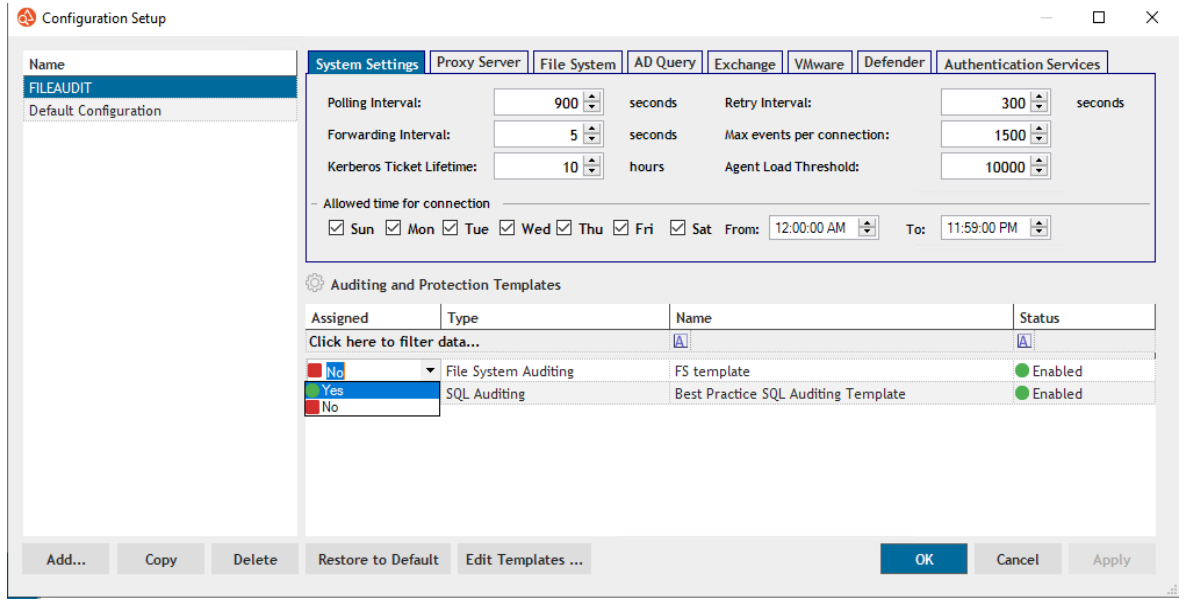
File Systemのテンプレート設定



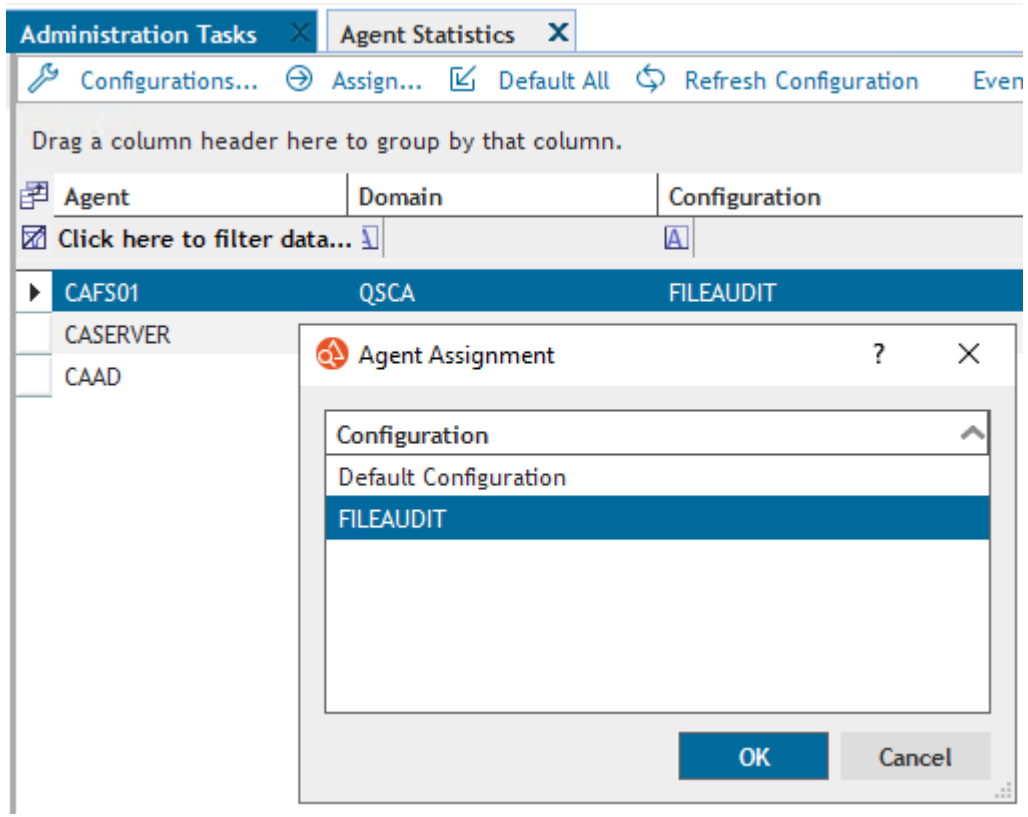
Finishボタンから**Finish and Assign to Agent Configuration…**を選択します。

目次に戻る

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。

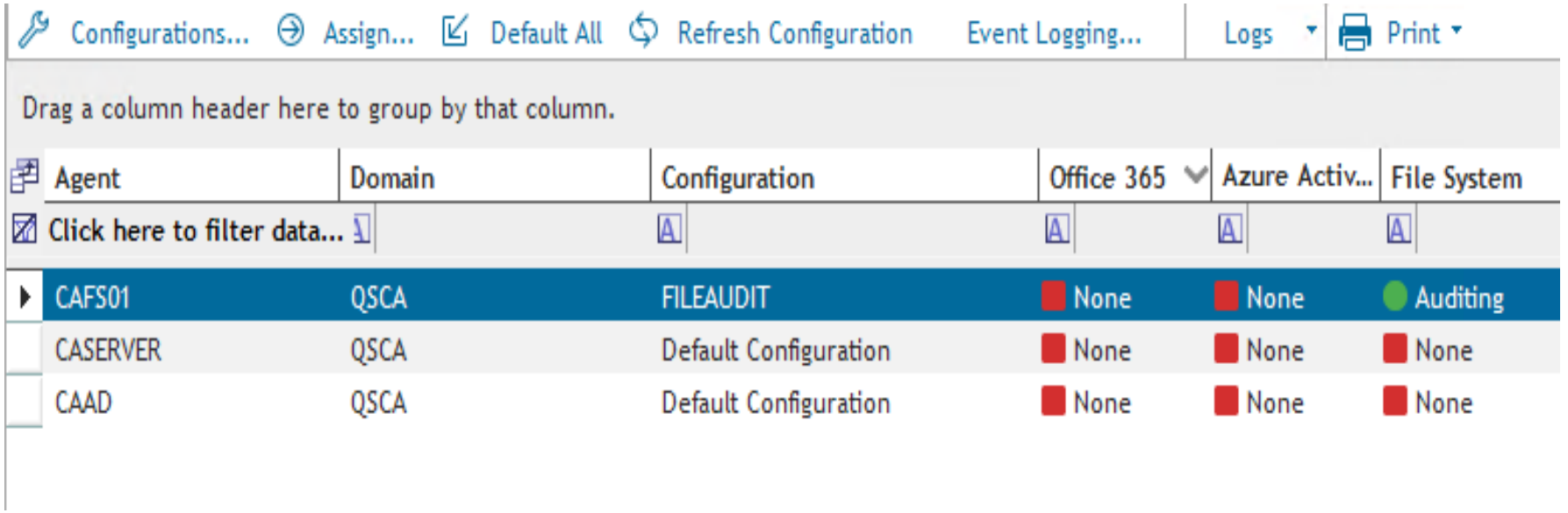


エージェントを選択し、**Assign…**をクリックして**Agent Assignment**を開きます。

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。

目次に戻る

File Systemのテンプレート設定



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。

目次に戻る

Windows File System の変更の監査例

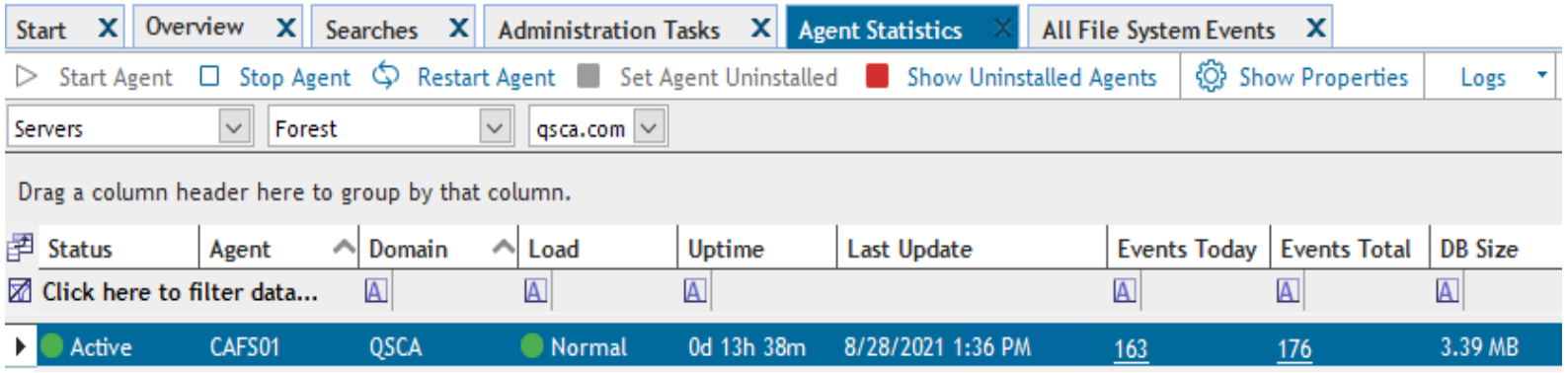
ここでは、File　Systemの簡単なテスト手順を説明します。

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。

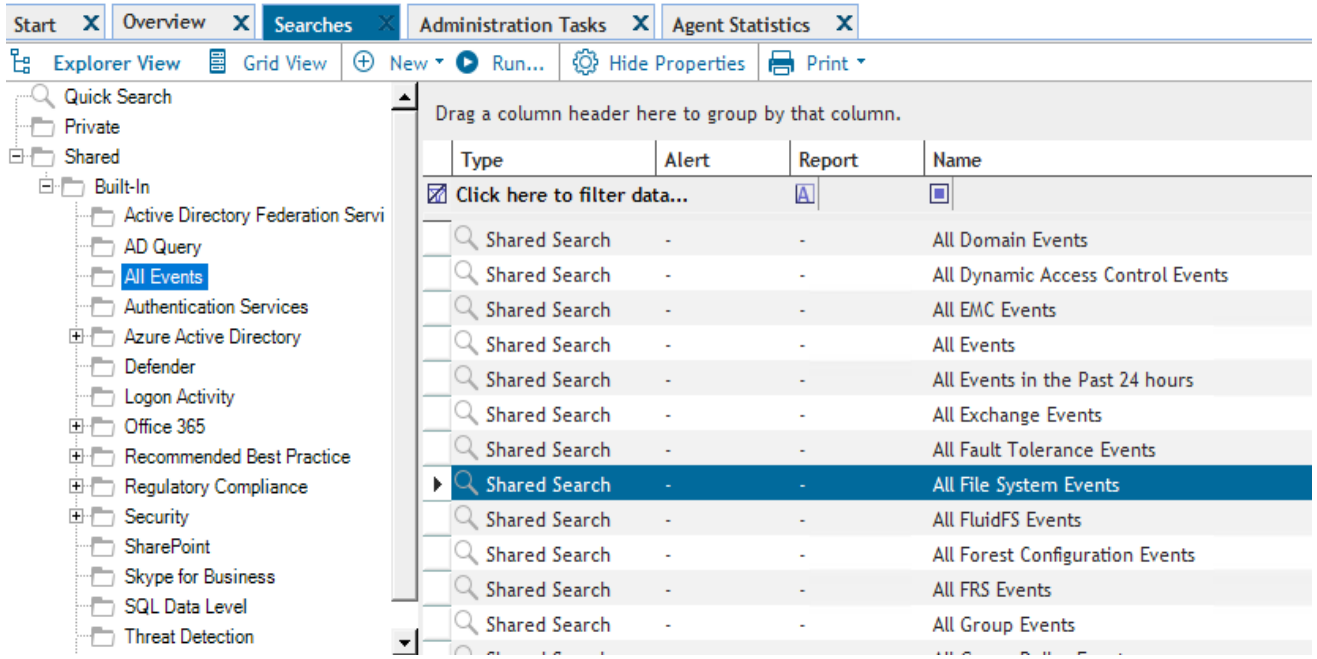


目次に戻る

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。

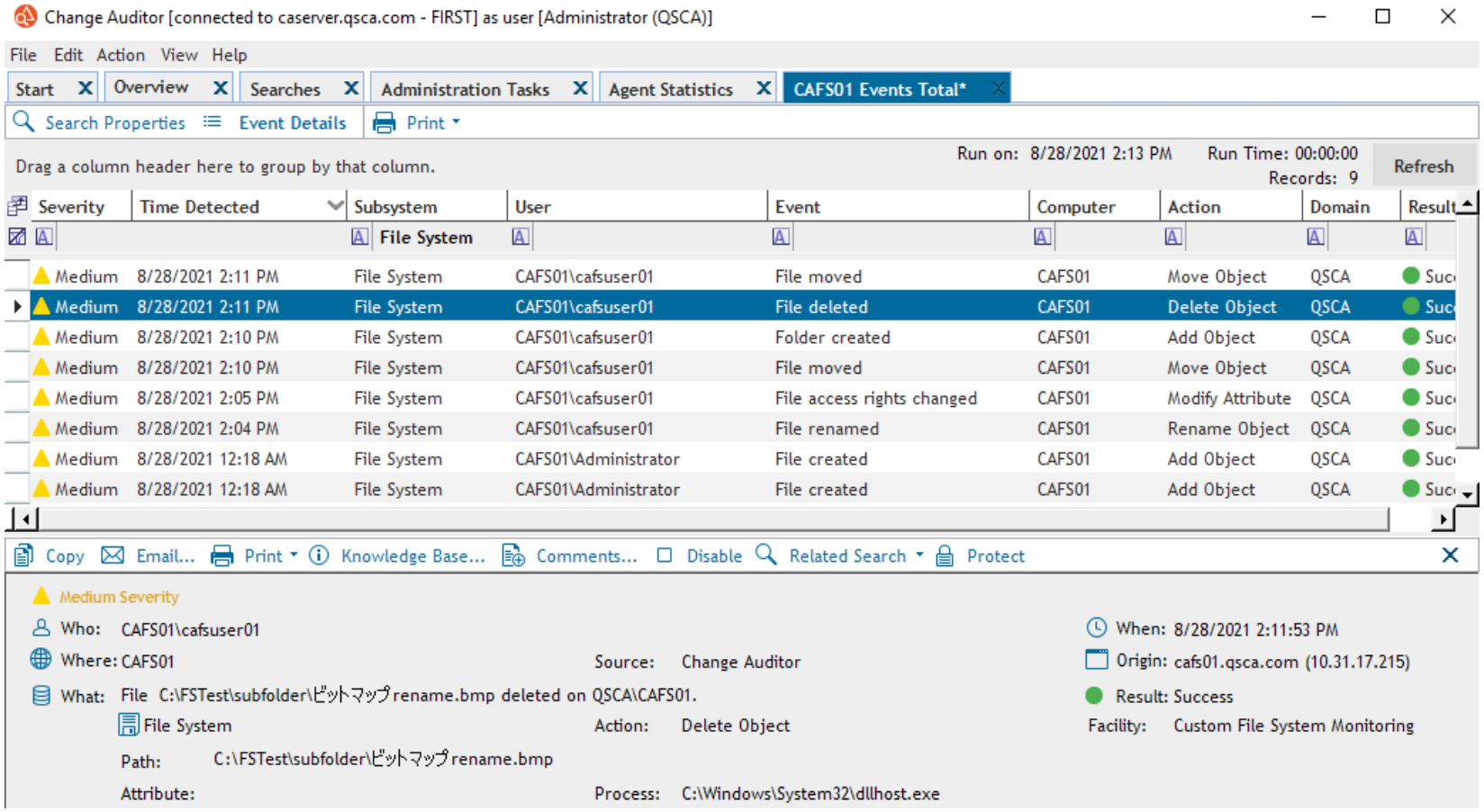


目次に戻る

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。



目次に戻る

目次に戻る

Quest

Where Next Meets Now.