XDR (eXtended Detection and Response)
ESET Inspect 旧バージョンから
ESET Inspect バージョン 1.11 への
バージョンアップ手順書

第 1 版

2023 年 10 月 3 日

キヤノンマーケティングジャパン株式会社

改訂履歴

版数	発行日	改訂履歴
第 1 版	2023 年 10 月 3 日	初版発行

目次

1. はじめに

○ 本書は、XDR (eXtended Detection and Response)「ESET Inspect」をご利用になるお客さま向けで、旧バージョンから ESET Inspect V1.11 へバージョンアップをするための手順書となります。

○ 本書は、本書作成時のソフトウェア及びハードウェアの情報に基づき作成されています。ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに搭載されている機能及び名称が異なっている場合があります。また本書の内容は、将来予告なく変更することがあります。

○ 本書内における名称は以下の通りです

略称	正式名称
EI	ESET Inspect
EEI Agent	ESET Enterprise Inspector Agent
EI Connector	ESET Inspect Connector
EP	ESET PROTECT
ESMC	ESET Security Management Center
EM Agent	ESET Management Agent
EES	ESET Endpoint Security
EEA	ESET Endpoint アンチウイルス
ESSW	ESET Server Security for Microsoft Windows Server
EFSW	ESET File Security for Microsoft Windows Server
MSSQL	Microsoft SQL Server
SSMS	SQL Server Management Studio

○ ESET Enterprise Inspector より ESET Inspect に名称が変更になりました。
※EEI Agent についても ESET Inspect Connector に名称が変更になりました。
※プログラム名は ESET Inspect に変更となりました。

○ バージョン 8.0 以降では、ESET Security Management Center は ESET PROTECT に名称が変更されています。

○ バージョン 8.0 以降では、ESET File Security for Microsoft Windows Server は ESET Server Security for Microsoft Windows Server に名称が変更されています。

2. 本書における構成の前提

以下の構成を前提として、EI 旧バージョンから EI V1.11 へバージョンアップする際のフローや注意点を記載しております。

			バージョンアップ前 (Version)	バージョンアップ後 (Version)
サーバー (Windows Server 2019)	EI	EI Server	旧バージョン	**1.11**
		MySQL の場合	旧バージョン	**8.0.33 以降**
		MSSQL の場合	MSSQL 2017 以降	**MSSQL 2017 以降**
		EFSW/ESSW	7.3 以降	**10.0 以降**
	ESMC /EP	ESMC/EP Server	7.2 以降	**10.1 以降**
		EFSW/ESSW	7.3 以降	**10.0 以降**
クライアント (Windows 10)	EEI Agent/EI Connector		旧バージョン	**1.11**
	EES/EEA		8.0 以降	**10.0 以降**
	EM Agent		7.2 以降	**10.0 以降**

注意事項

バージョンアップ作業を始める前に以下の要件を満たしていることを確認してください。

満たしていない要件がある場合は、**必ず要件を満たす環境にしてからバージョンアップ作業を開始してください**。

(1) EP V10.1 以降を利用していること

(2) 各管理している端末では EM Agent V10.0 以降を利用していること

(3) 各クライアント端末では EES/EEA/ESSW V10.0 以降を利用していること

(4) MSSQL をご利用の場合、「手順 4.2.2 MSSQL のバックアップ取得」時に SSMS を使用します。

※ EES/EEA/EFSW のバージョンアップについては以下のサポートページを参照ください。
https://eset-support.canon-its.jp/faq/show/23035?site_domain=business

※ EM Agent のバージョンアップについては以下のサポートページを参照ください。
https://eset-support.canon-its.jp/faq/show/19162?site_domain=business

※ ESMC/EP のバージョンアップについては以下のサポートページを参照ください。
https://eset-support.canon-its.jp/faq/show/151?site_domain=business

3. バージョンアップの流れ

旧バージョンから EI V1.11 へバージョンアップを行う流れは以下の通りです。

注意事項

・データベースのバックアップを行う際、一時的に EI サーバーのサービスを停止させます。サービスが停止している間はログの収集は行えませんが、サービス起動後に EI エージェントが保持していたログが EI サーバーに送信されます。

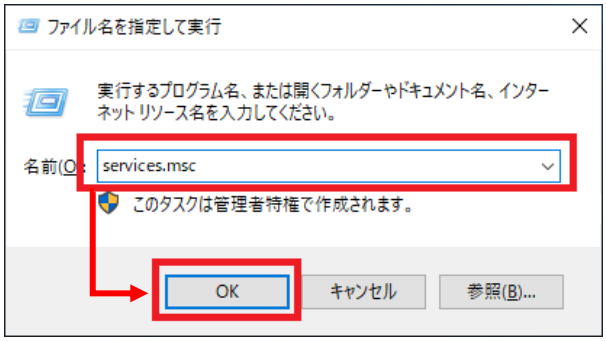
・EI V1.8 以降では MySQL のバージョン要件が変更になるため、MySQL をご利用のお客様向けに MySQL のバージョンアップ手順を記載しています。

4. データベースのバックアップ【EI 側作業】

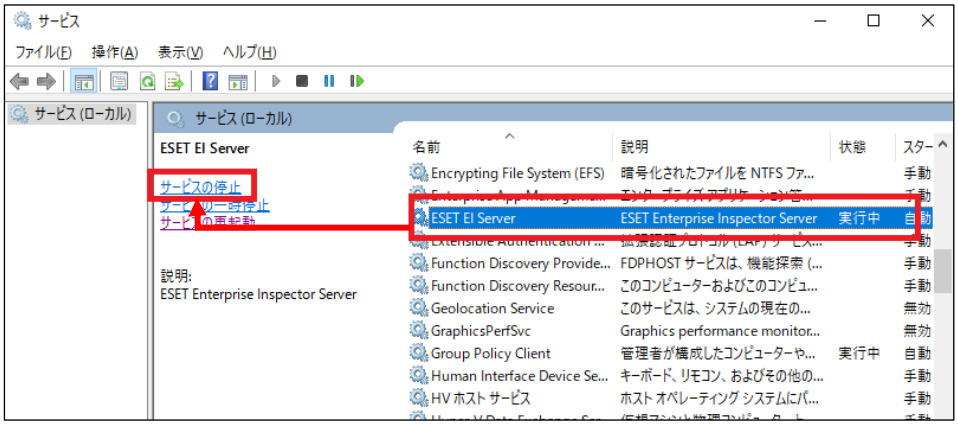
手順 4.2 以降ではご利用のデータベースの種類によってバックアップの取得方法が異なります。

4.1 EI Server のサービス停止

(1). EI サーバーが稼働しているサーバーにログインし、「Windows キー」＋「R」でファイル名を指定して実行させるウィンドウを開き「services.msc」と入力し、「OK」をクリックします。



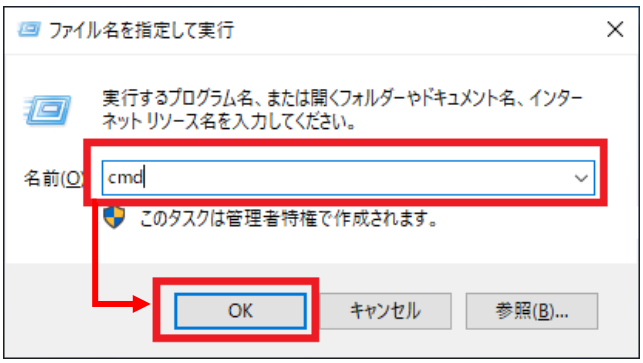
(2). 「ESET EI Server」サービスを選択し、サービスの停止をクリックします。



(3). 「ESET EI Server」サービスの状態が空欄になったことを確認します。

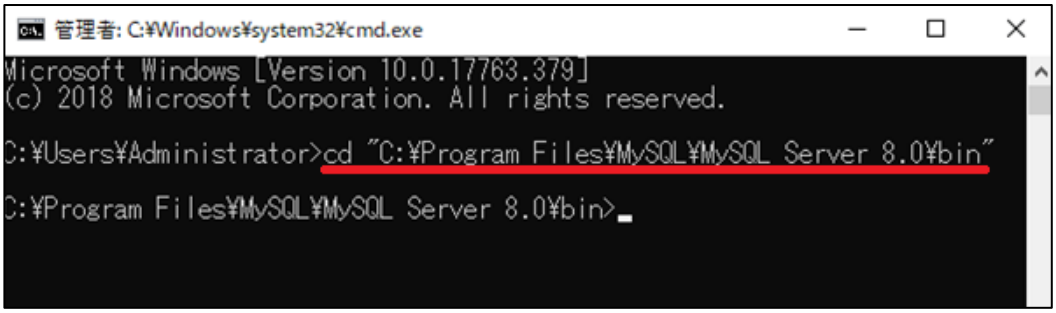
4.2.1 MySQL のバックアップ

(1). 「Windows キー」+「R」でファイル名を指定して実行させるウィンドウを開き「cmd」と入力し、「OK」をクリックします。



(2). コマンドプロンプトの画面にて、以下（ア）～（ウ）の操作を行い MySQL のバックアップを取得します。

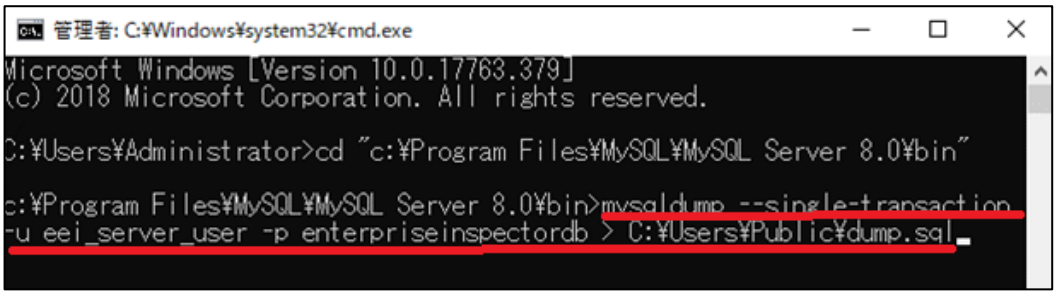
(ア) [cd “C:¥Program Files¥MySQL¥MySQL Server 8.0¥bin”]と入力し、enter キーを押します。



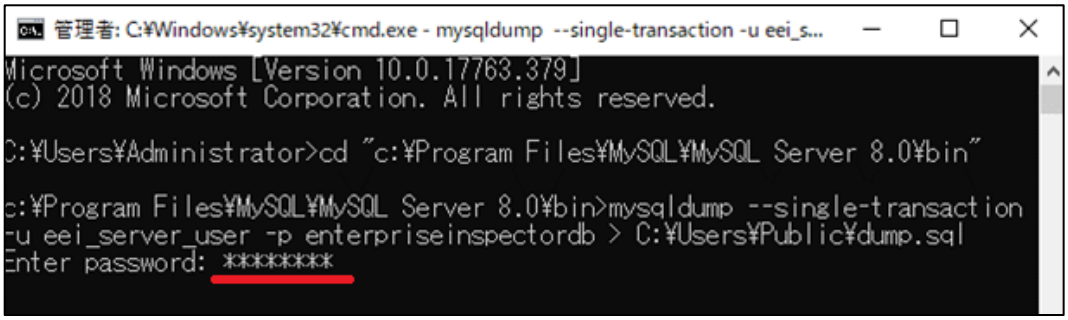
(イ) [mysqldump –-single-transaction –u データベースのユーザー名 –p データベース名 > 出力先ファイル名]と入力し、enter キーを押します。

※データベースのユーザー名は EEI Server をインストール時に設定した値です。

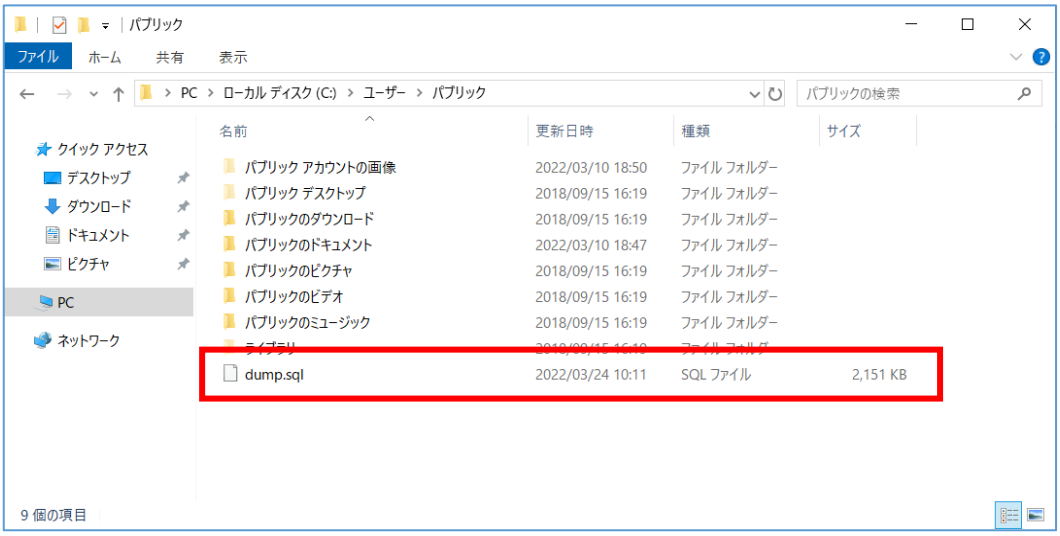
※データベース名は既定で「enterpriseinspectordb」です。



(ウ)「Enter password」にデータベースのユーザーのパスワードを入力し、enter キーを押します。



(3). 指定した出力先にバックアップファイルが作成されていることを確認します。



4.2.2 MSSQL のバックアップ

(1). 以下 URL より、SQL Server Management Studio 19 をダウンロードし、サーバーへインストールしてください。

<SQL　Server　Management Studio ダウンロードサイト>

https://docs.microsoft.com/ja-jp/sql/ssms

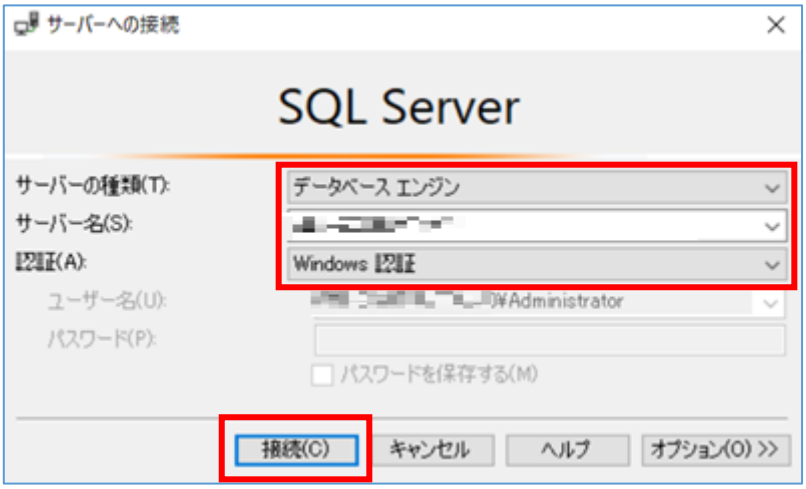
※インストール後、再起動が要求された場合は再起動します。

(2). 「Microsoft SQL Server Management Studio19」を起動します。

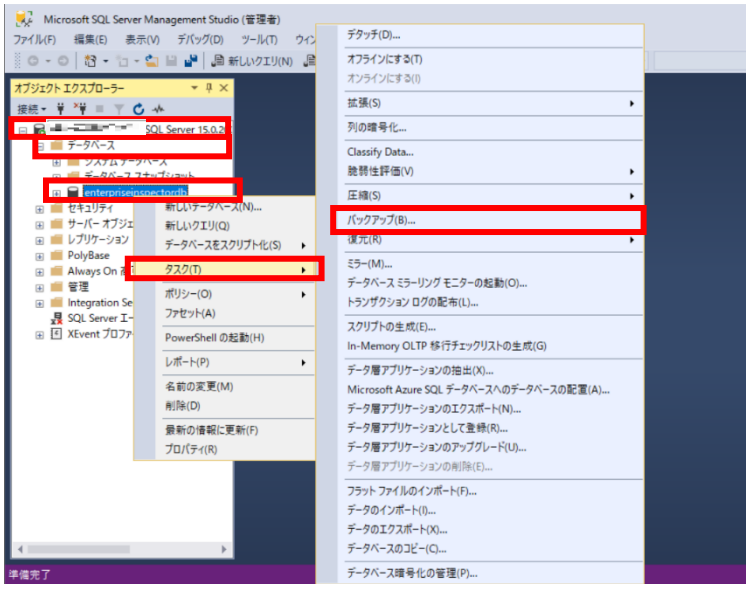
※初めて起動する場合、起動に少々お時間がかかります。

(3). サーバーへの接続画面で、以下の通り項目を確認して[接続]ボタンをクリックします。

サーバーの種類	データベースエンジン
サーバー名	EI サーバー名
認証	Windows 認証

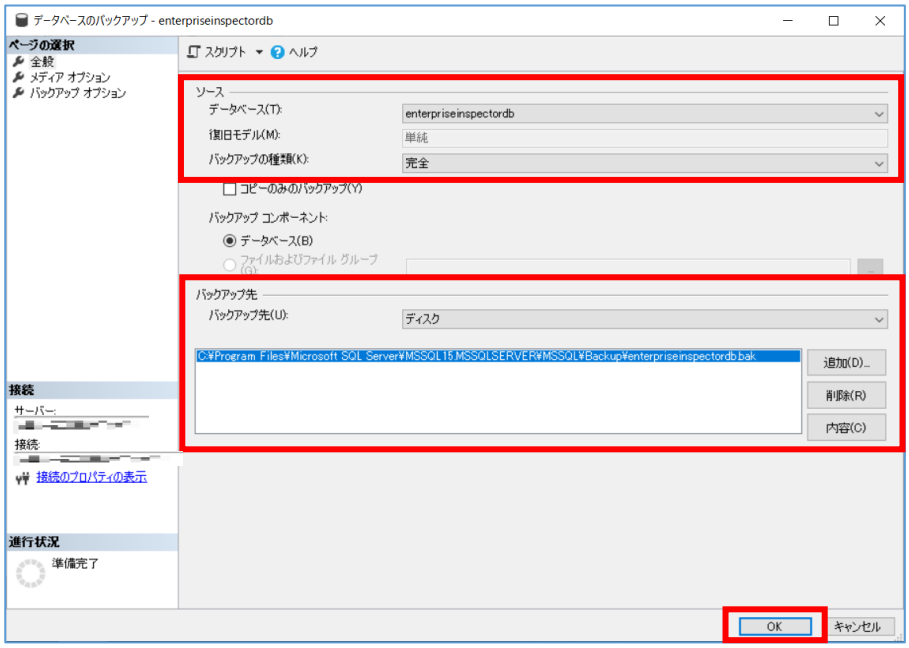


(4). オブジェクトエクスプローラーより、[インスタンス名]-[データベース]-[enterpriseinspectordb]へ移動します。「enterpriseinspectordb」を右クリックし、[タスク]-[バックアップ]をクリックします。

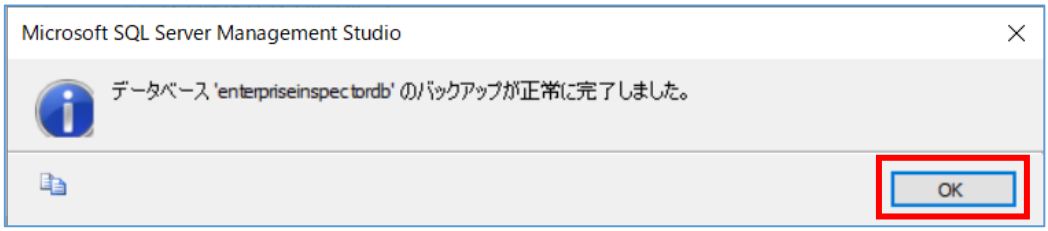


(5). データベースのバックアップ画面で、以下の通り設定し、[OK]ボタンをクリックします。

データベース	enterpriseinspectordb
バックアップの種類	完全
バックアップ先	ディスク



(6). 以下のメッセージが表示されたらバックアップは正常に終了しています。
[OK]ボタンをクリックして、閉じます。



※「アクセスが拒否されました」といったエラーが出力された場合は、バックアップファイルの出力先にアクセス権限があるかご確認ください。

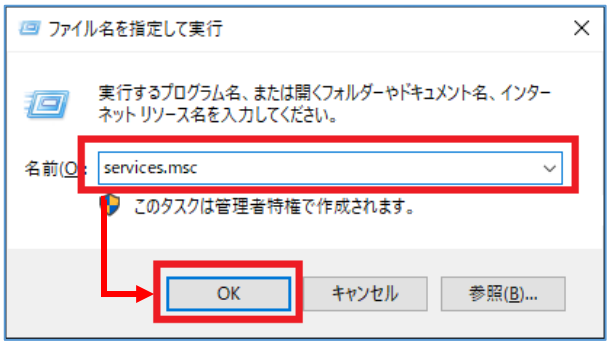
(7). 手順 5 で作成したバックアップファイルが指定の場所に格納されていることを確認します。

5. MySQL のバージョンアップ【EI 側作業】

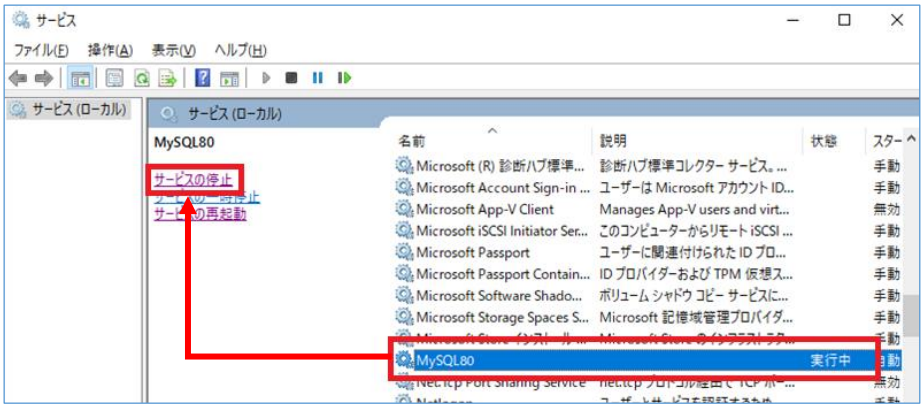
MSSQL を使用して EI Server を構築している場合は、「6. EI Server のバージョンアップ【EI 側作業】に進んでください。

5-1 MySQL のサービス停止

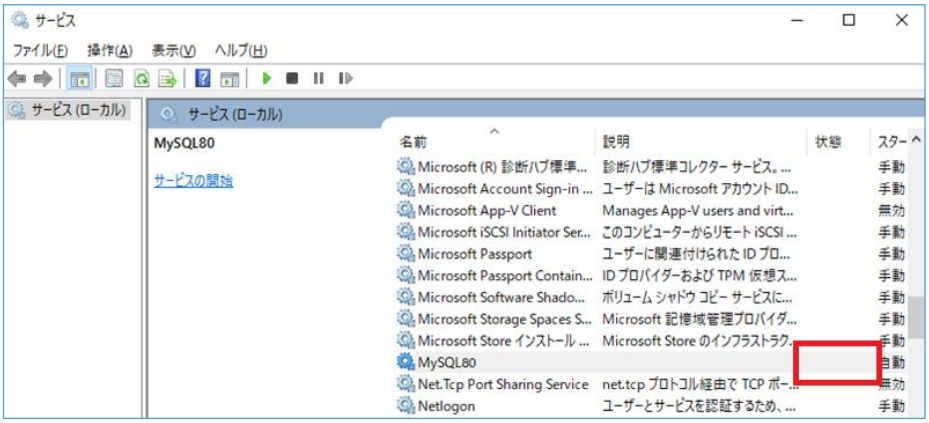
(1).「Windows キー」＋「R」でファイル名を指定して実行させるウィンドウを開き「services.msc」と入力し、「OK」をクリックします。



(2).「MySQL80」サービスを選択し、サービスの停止をクリックします。



(3).「MySQL80」サービスの状態が空欄になったことを確認します。



5-2　MySQL のバージョンアップ

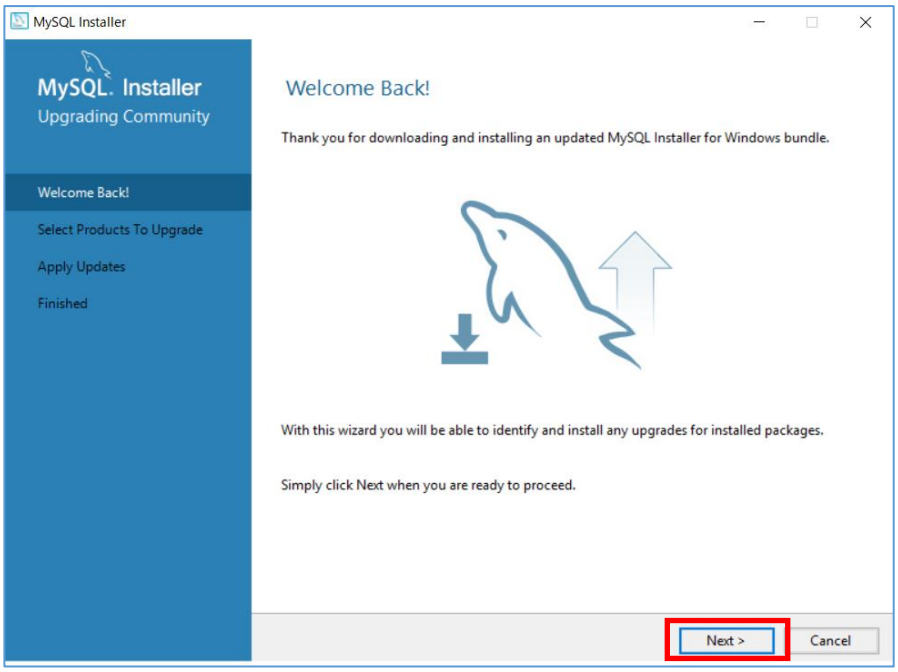
(1).「Microsoft Visual C++ 2015-2019 redistributable Package(x64)」インストールされていない場合は、以下 URL よりダウンロード、およびインストールを完了させてください。

https://support.microsoft.com/ja-jp/help/2977003/the-latest-supported-visual-c-downloads

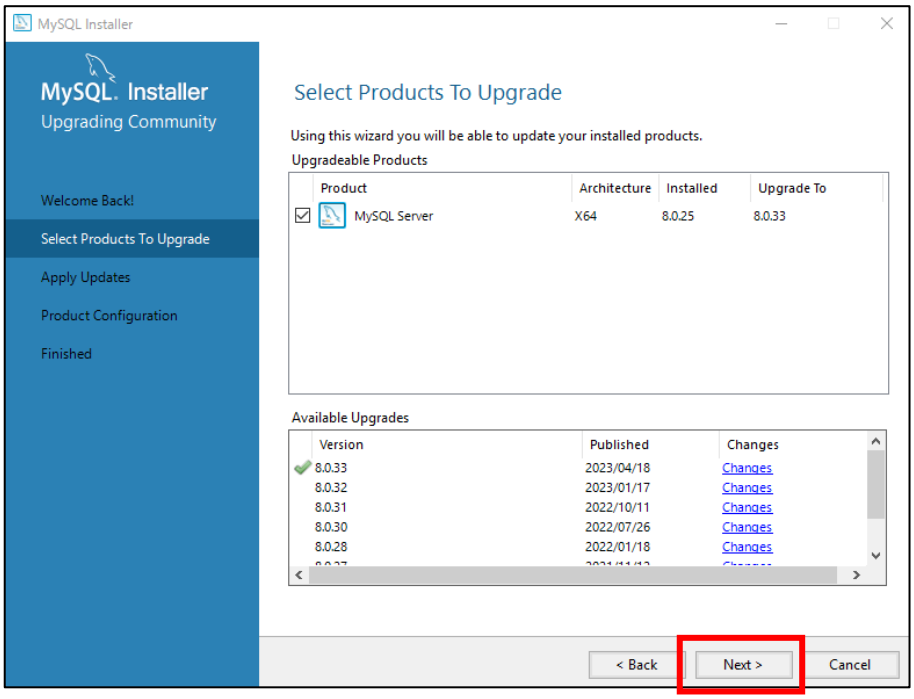
(2).以下 URL より、MySQL のインストーラー(mysql-installer-community-8.0.xx.msi)をダウンロード、およびインストールを開始します。

https://dev.mysql.com/downloads/windows/installer/8.0.html

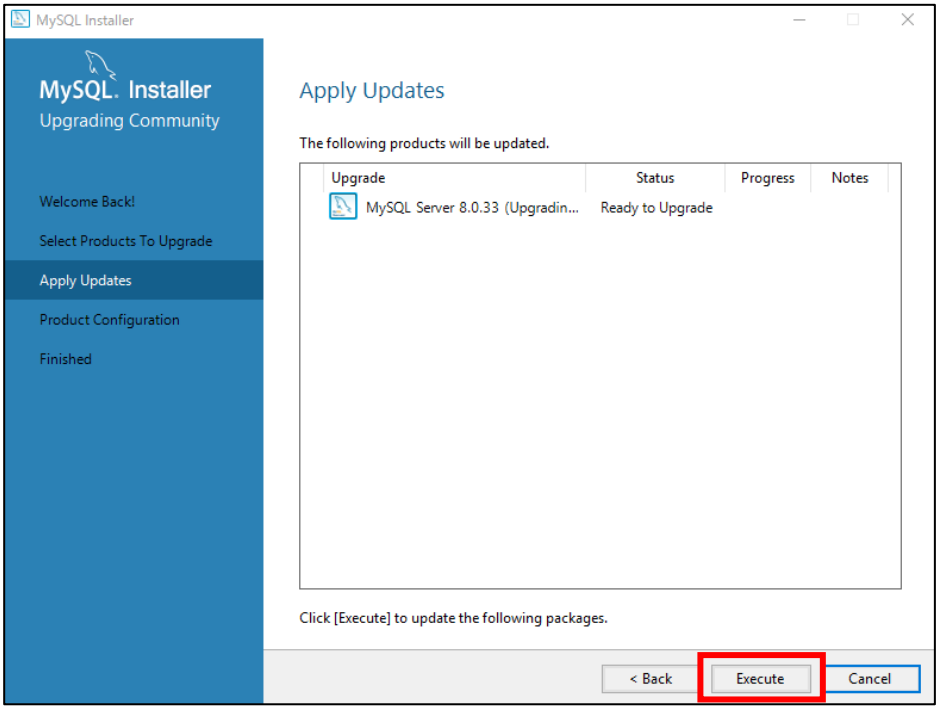
(3).Welcome back! 画面で、[Next]をクリックします。



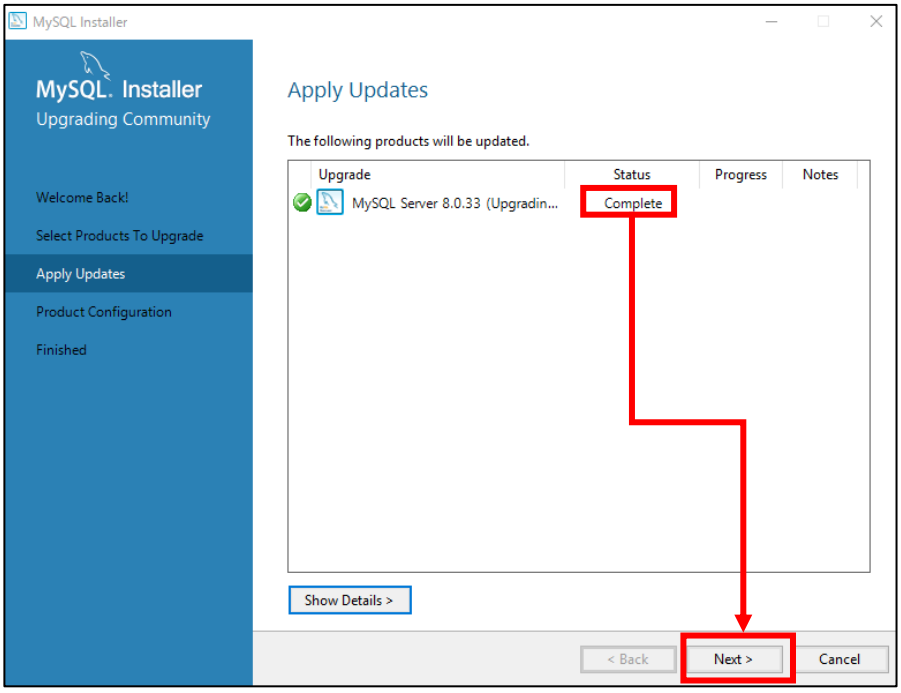
(4).Select Products To Upgrade 画面で、[Next]をクリックします。



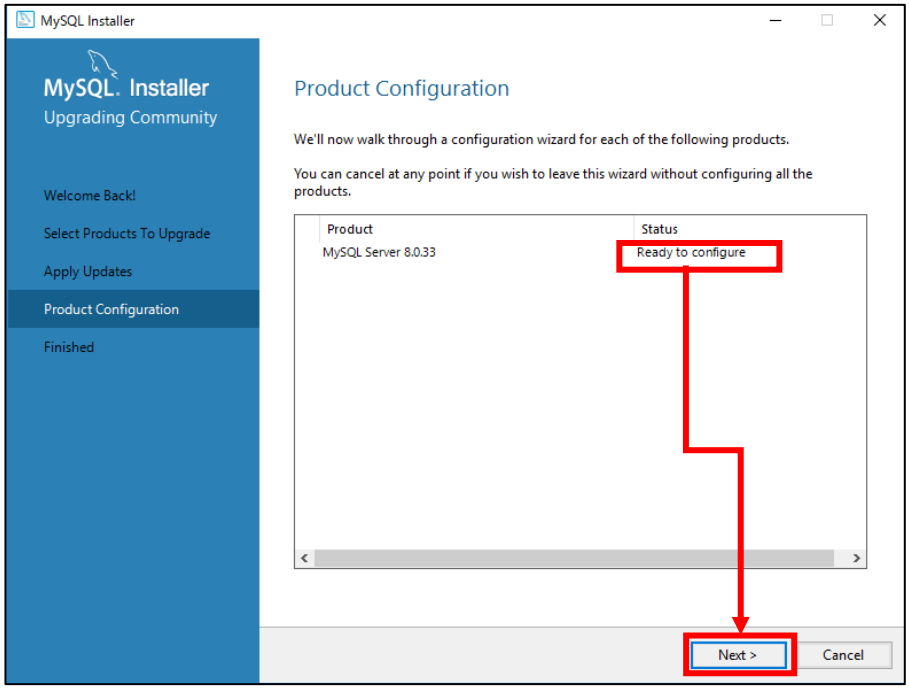
(5).Apply Updates 画面で、[Execute]をクリックします。



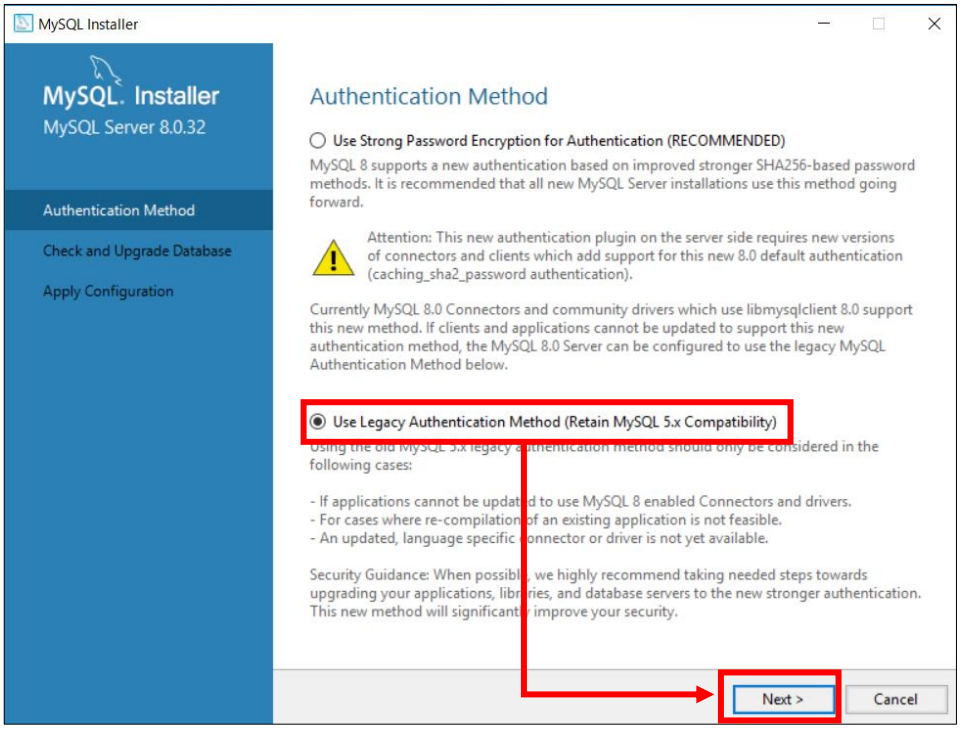
(6).Status 欄が「Complete」 であることを確認し、[Next]をクリックします。



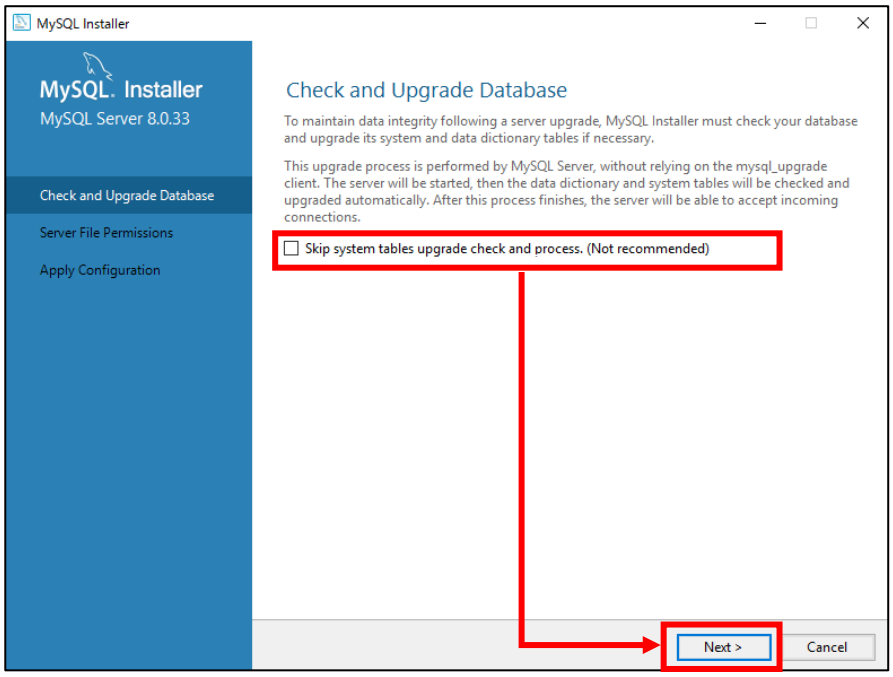
(7).Product Configuration 画面で、Status 欄が「Ready to configure」と表示されたら、[Next]をクリックします。



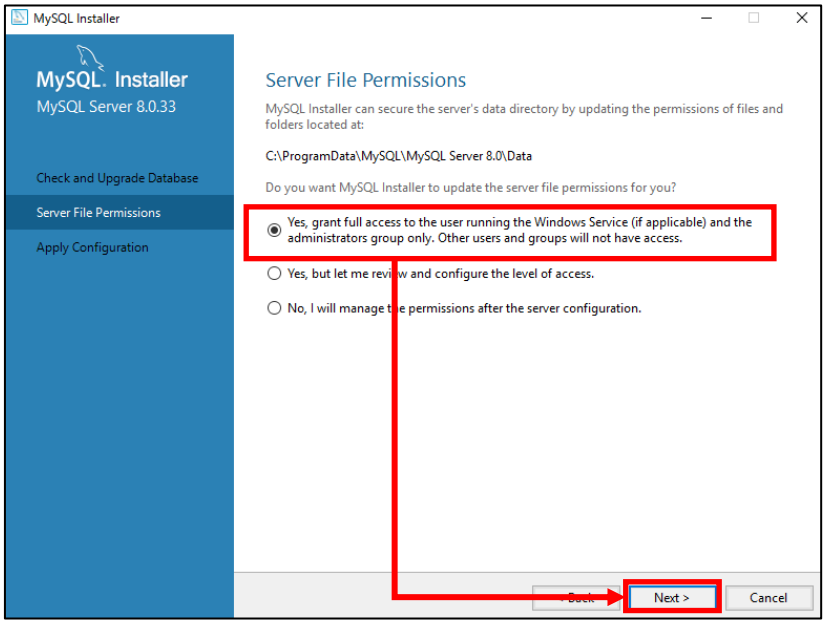
(8).Authentication Method 画面で、[Use Legacy Authentication Method(Retain MySQL 5.x Compatibility)]を選択し、[Next]をクリックします。



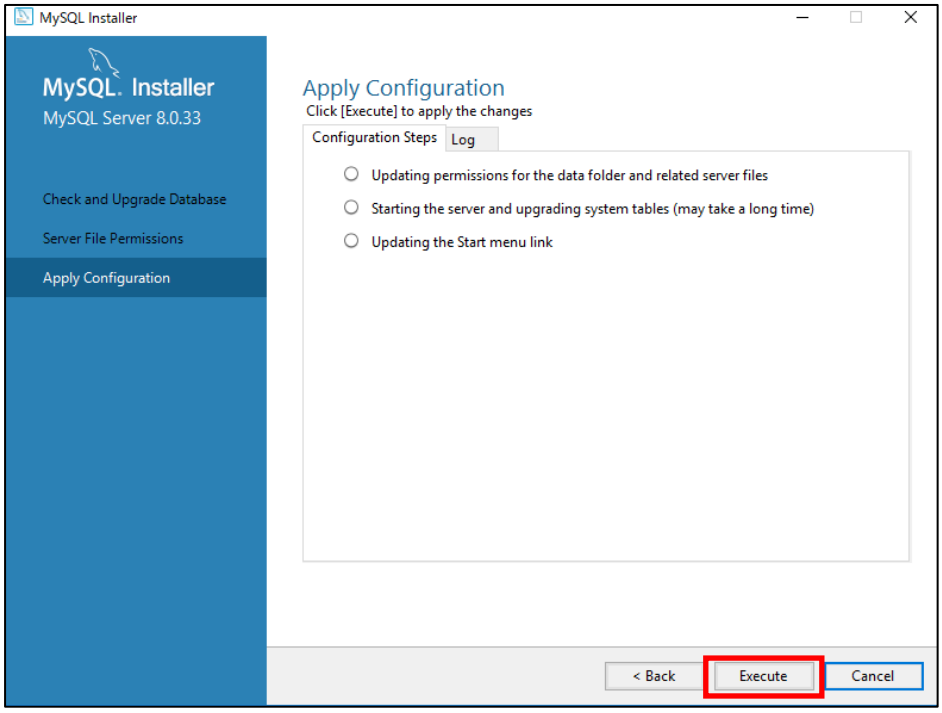
(9).Check and Upgrade Database 画面で、[Skip system tables upgrade check and process.(Not recommended)]のチェックが外れていることを確認し、[Next]をクリックします。



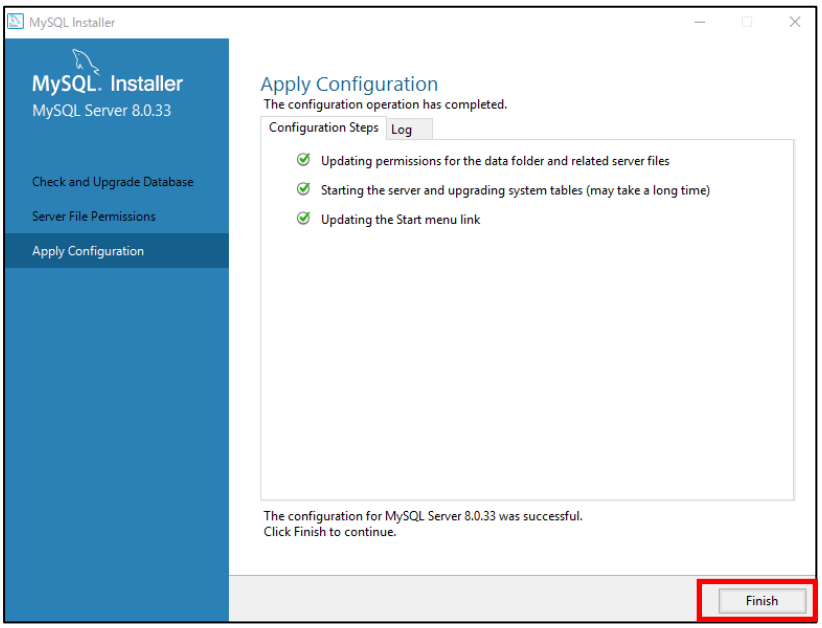
(10).Server File Permissions 画面で、[Yes, grant full access to the user　running the Windows Service ~]を選択し、[Next]をクリックします。



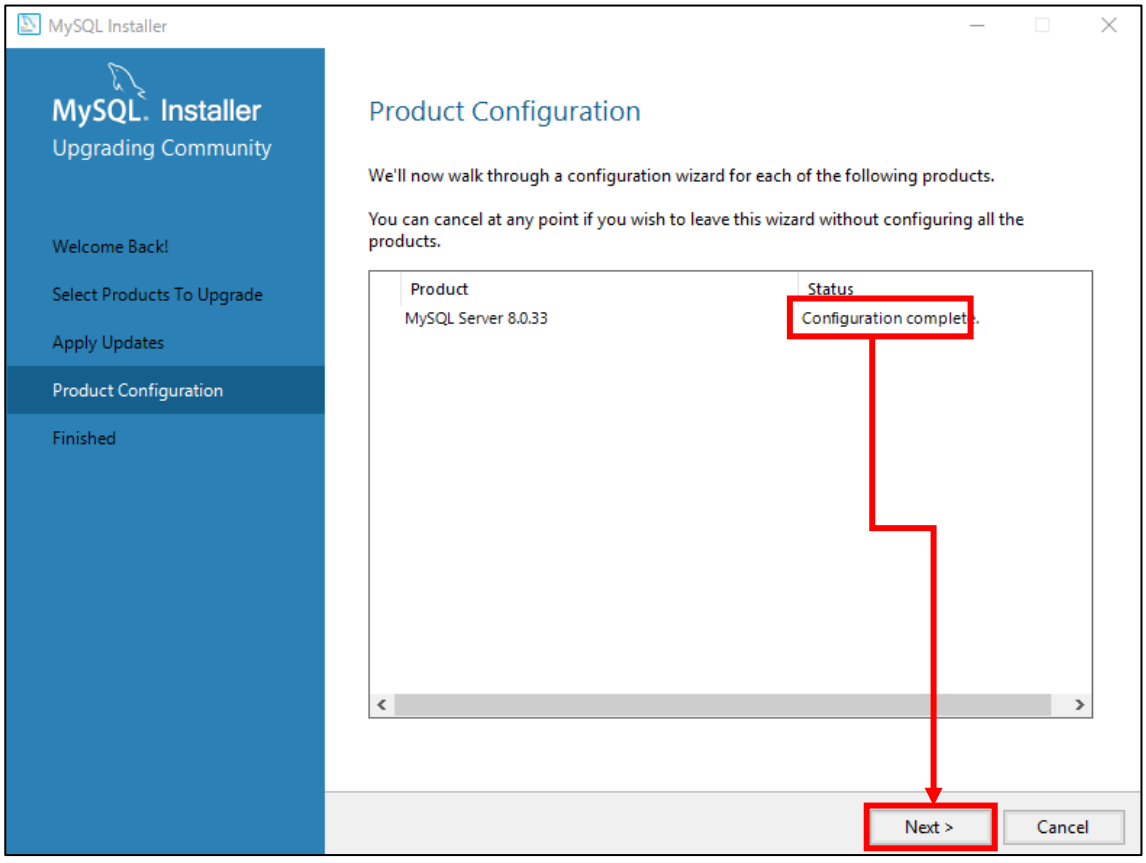
(11).Apply Configuration 画面で、[Execute]をクリックします。 進捗が表示されるのでしばらく待ちます。



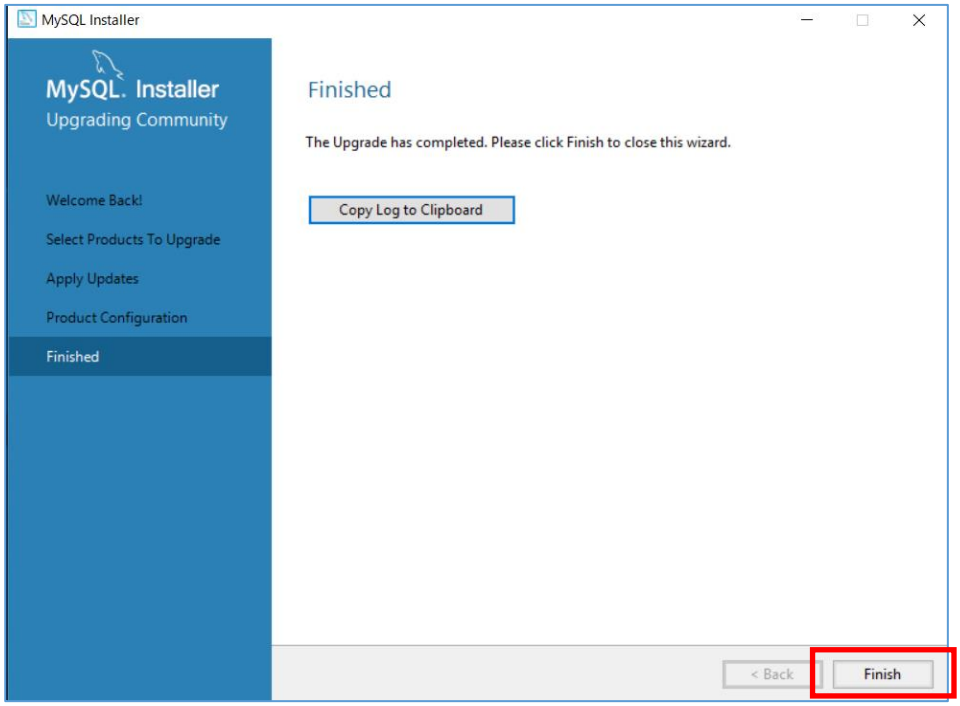
(12).Apply Configuration 画面で、[Finish]をクリックします。



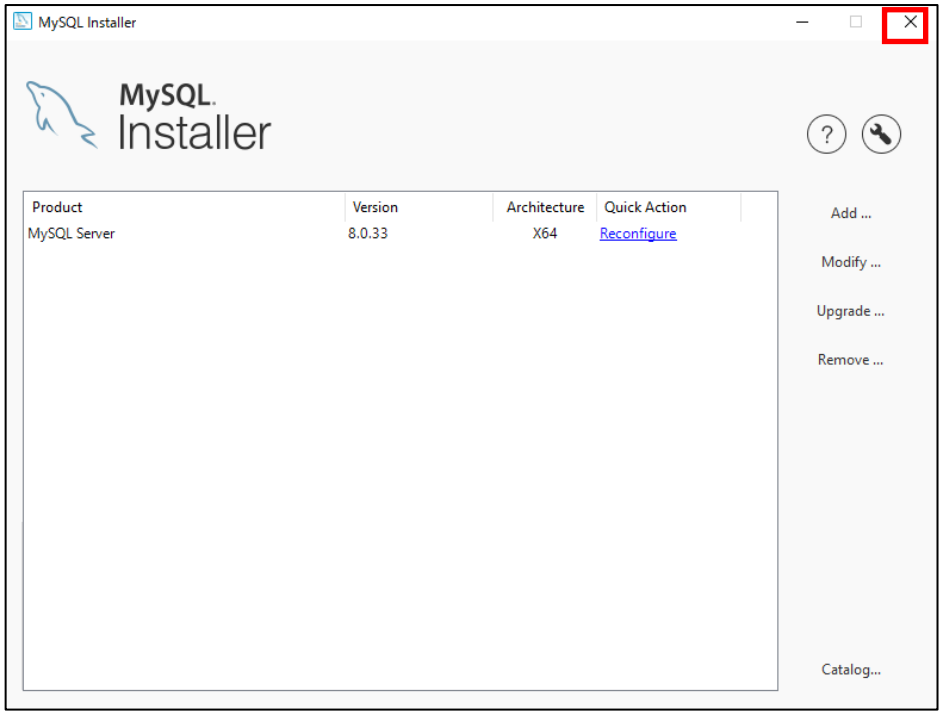
(13).Product Configuration 画面で、Status 欄が「Configuration complete.」となっていることを確認し、[Next]をクリックします。



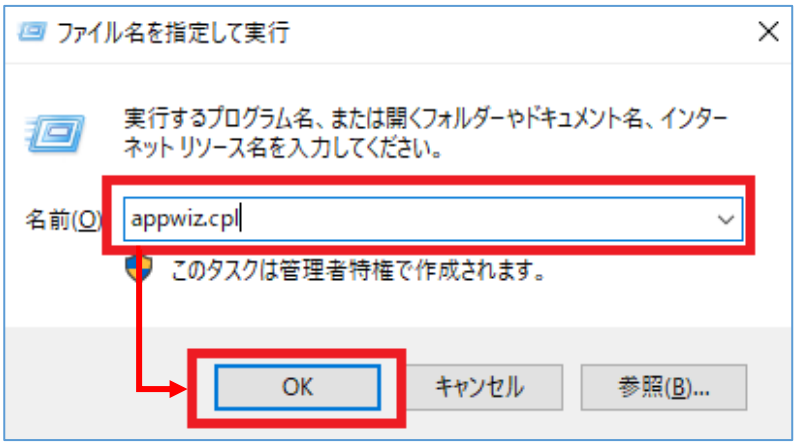
(14).Finished 画面で、[Finish]をクリックし、MySQL のバージョンアップを終了します。



(15).MySQL Installer 画面で、右上の[X]をクリックし、インストーラーを閉じます。



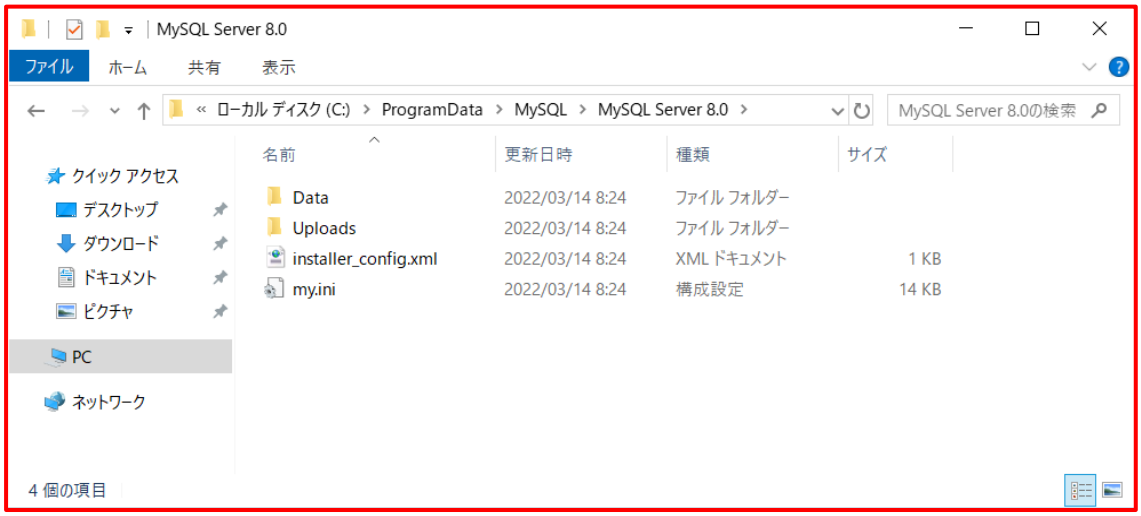
(16).「Windows キー」＋「R」でファイル名を指定して実行させるウィンドウを開き「appwiz.cpl」と入力し、「OK」をクリックします。



(17).「MySQL Server 8.0」のバージョンが上がっていることを確認します。

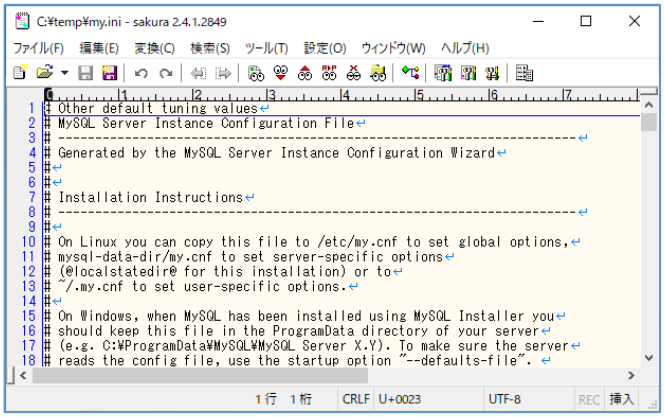
(18).C:¥ProgramData¥MySQL¥MySQL Server (バージョン番号)¥my.ini をテキストエディタで開きます。

※「ProgramData」は隠しフォルダのため、「表示」タブより「隠しファイル」にチェックをして表示させてください。



(19).my.ini ファイル内の以下の設定項目の記述を以下のように変更します。存在しない設定値は追記してください。また、my.ini ファイルを編集する際、使用するテキストエディタは Windows のメモ帳以外のエディタを使用します。

※追記済みの内容であれば対応は不要です。



[my.ini]ファイル

***** Group Replication Related *****

max_connections=300

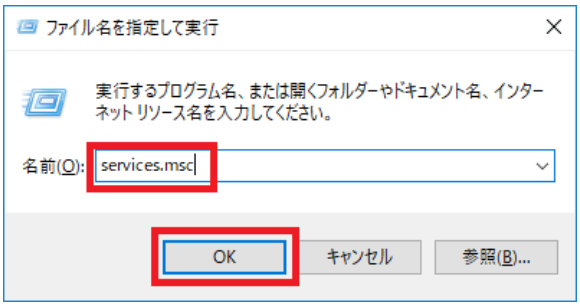
*デフォルトでは以下設定項目の記載が無いため、[mysqld]セクションの最終行に値を追記します。

wait_timeout=900

(20).my.ini を保存してテキストエディタを閉じます。

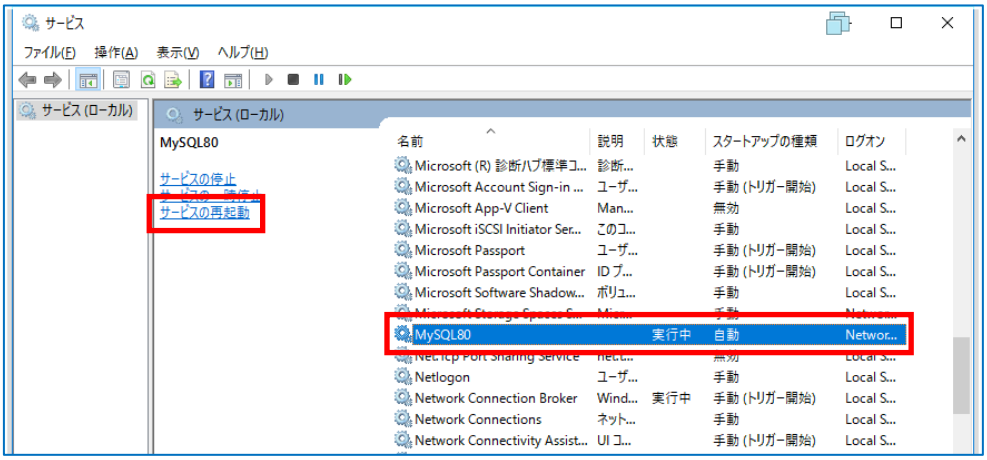
「Windows キー」＋「R」を押下、「ファイル名を指定して実行」ダイアログで、

「services.msc」と入力し、「OK」をクリックします。



(21).MySQL80 を選択し、[サービスの再起動]をクリックします。

MySQL80 サービスの状態が、起動中であることを確認します。



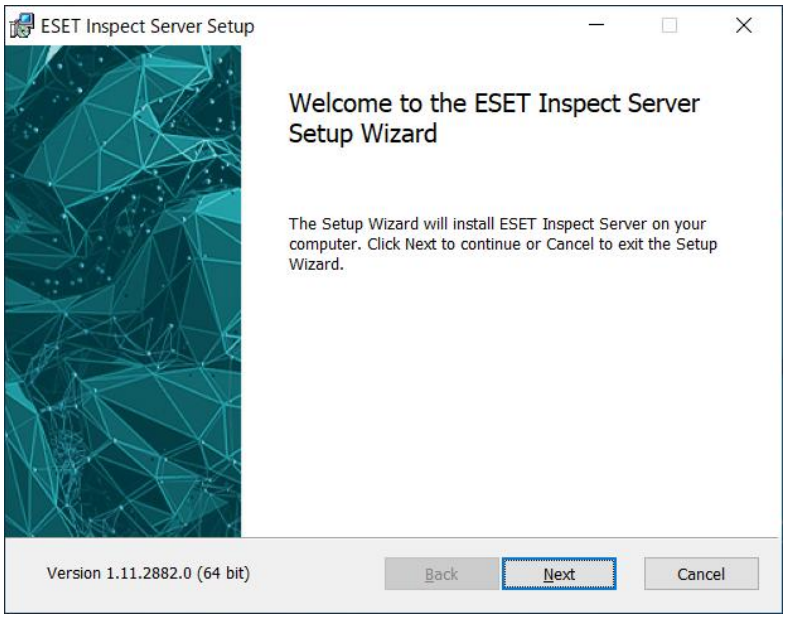
※MySQL サービスが正常に再起動しない場合は、my.ini の記述が正しいか確認してください。

6. EI Server のバージョンアップ【EI 側作業】

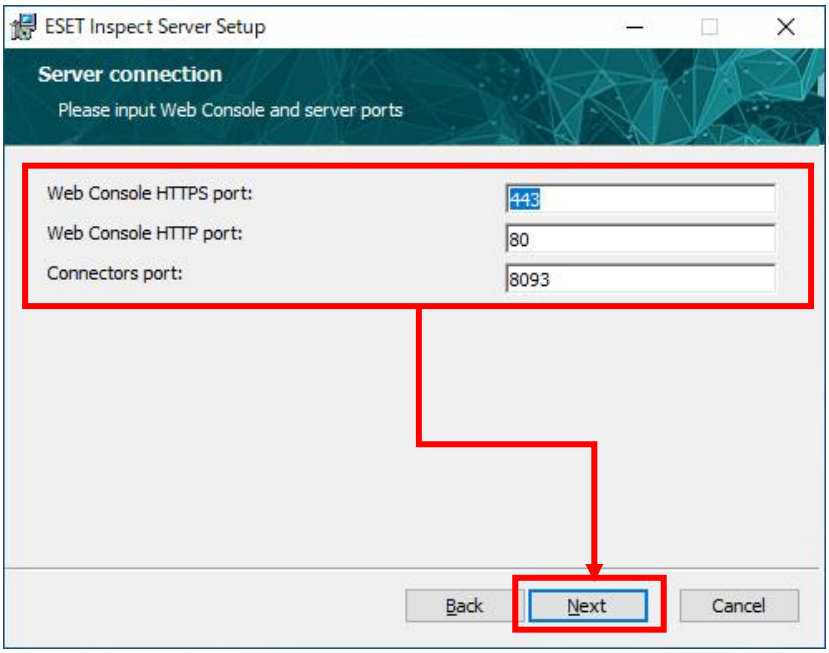
1-1 EI Server のバージョンアップ

(1). EI Server V1.11 のインストーラー（ei_server_nt64_ENU.msi）を使用し、インストールを開始します。

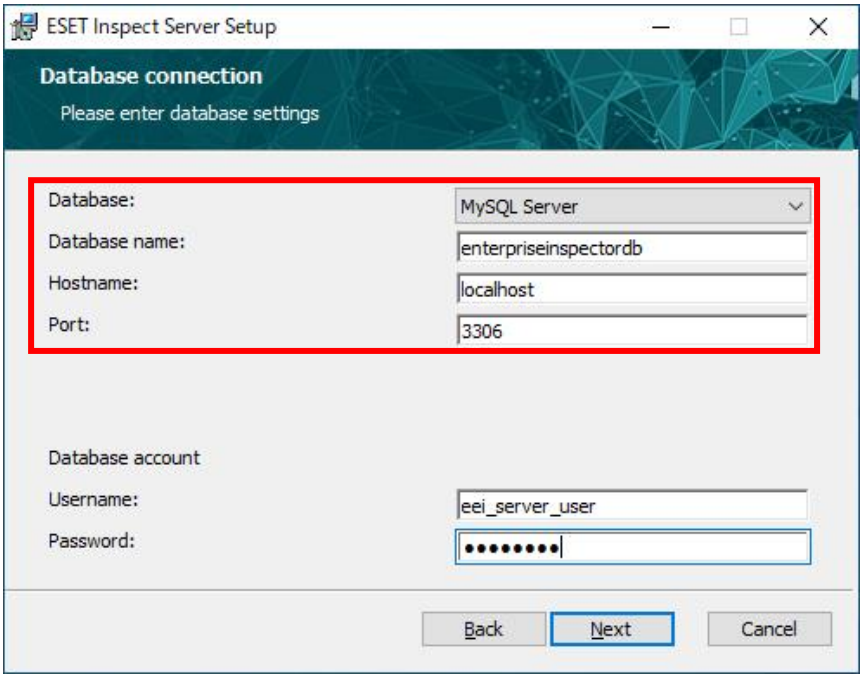
(2). Welcome to the ESET Inspect Server Setup Wizard 画面で、[Next]をクリックします。



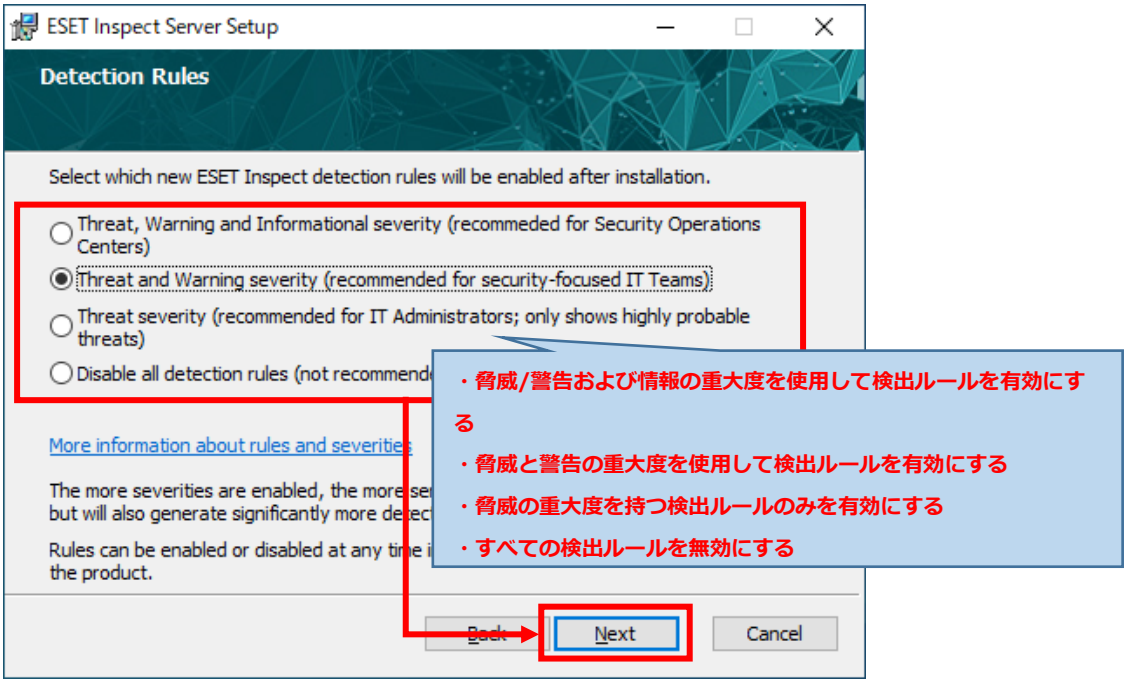
(3). Sever connection 画面で、Web Console および Agent の接続ポート情報が入力されていることを確認し、[Next]をクリックします。



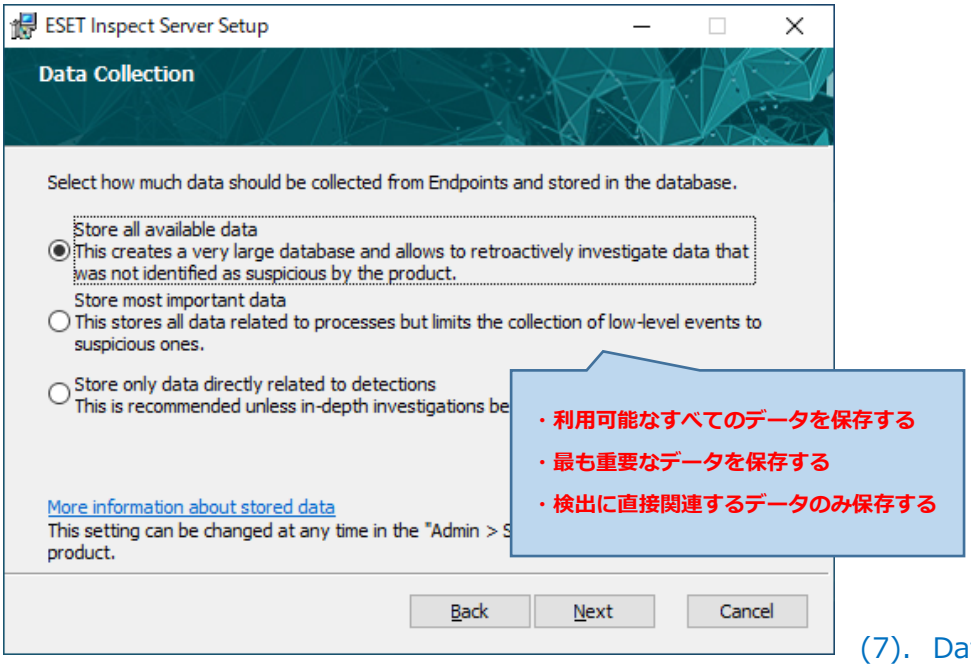
(4). Database connection 画面で、データベースの接続情報が入力されていることを確認し、[Next]をクリックします。



(5). Detection Rules 画面で、４つの重大度レベルに基づいて有効にするルールを選択します。本手順で選択した内容により、EI バージョンアップ後に既定で有効になるルールが変わります。

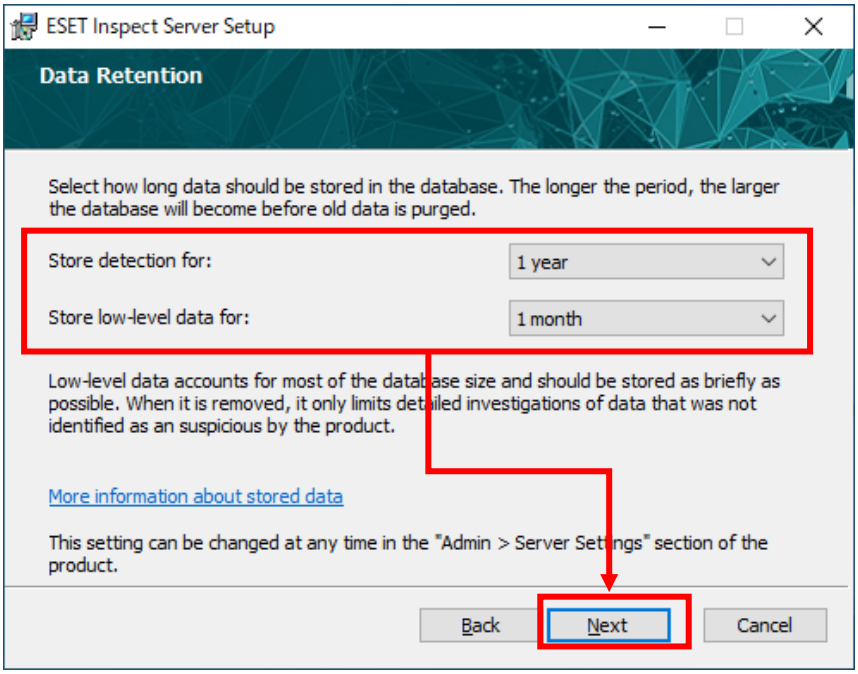


(6). Data Collection 画面では、EI でのデータ収集オプションを設定します。本手順で選択した内容により、データがデータベースに保存される方法を設定します。EI で表示されるプロセスツリーの情報量に影響します。

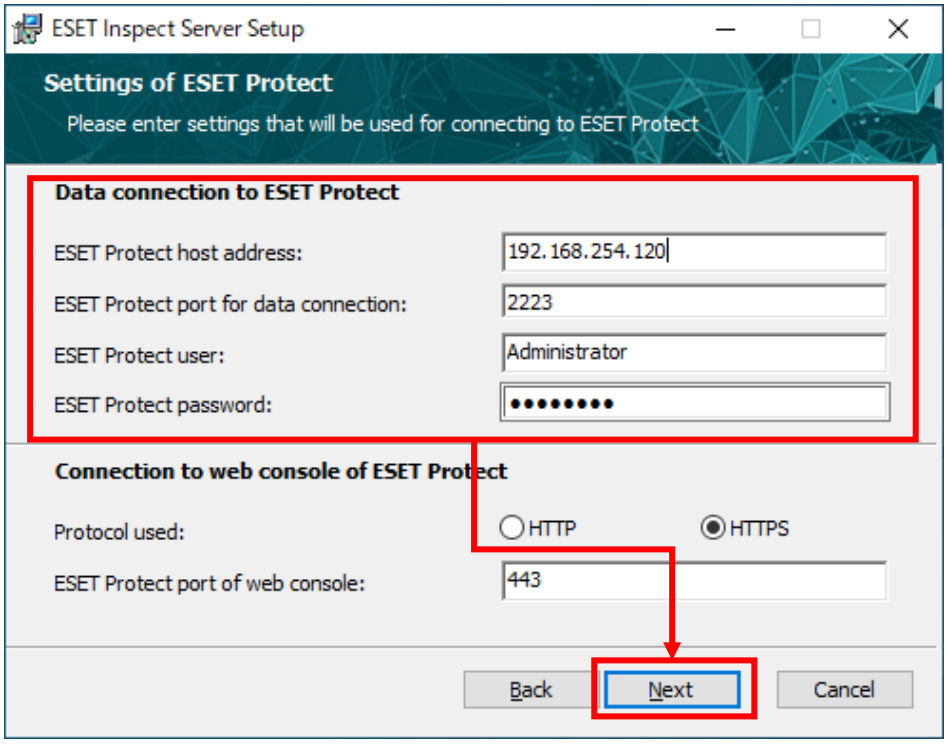


(7). Data Retention 画面では、EI でのデータの保持期間を選択します。本手順では、検出データや低レベルデータの保持期間を設定します。

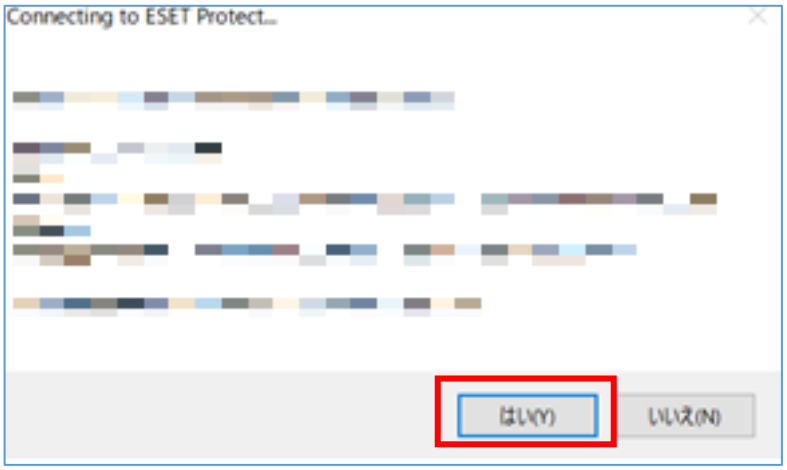
※本設定は EI バージョンアップ後にも設定変更が可能です。



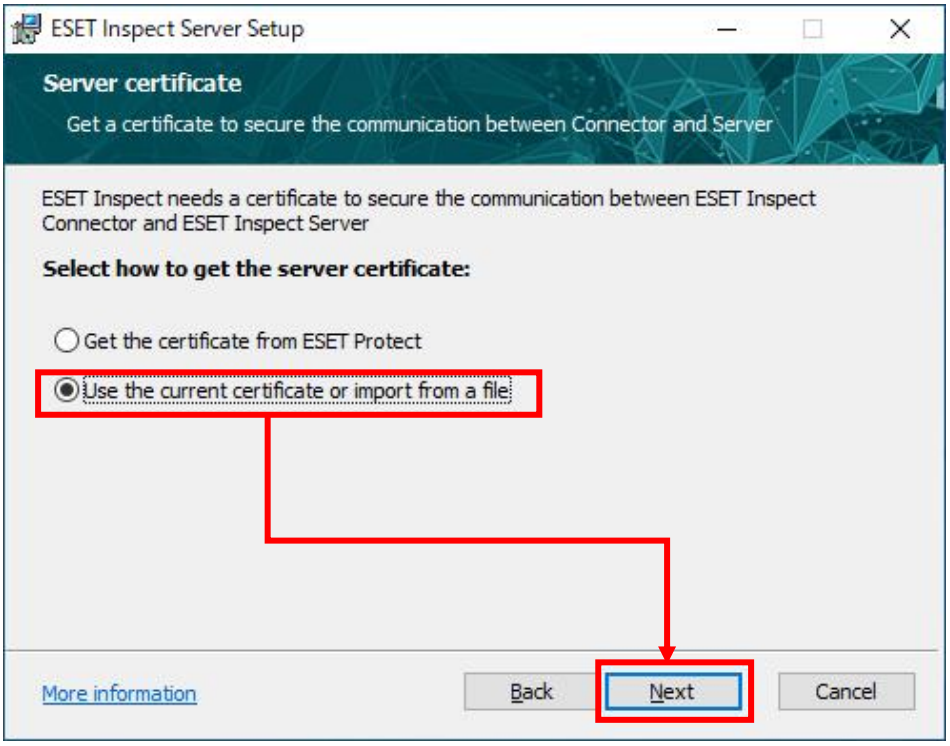
(8). Settings of ESET Security Management Center 画面で、EP の接続情報が入力されていることを確認し、[Next]をクリックします。



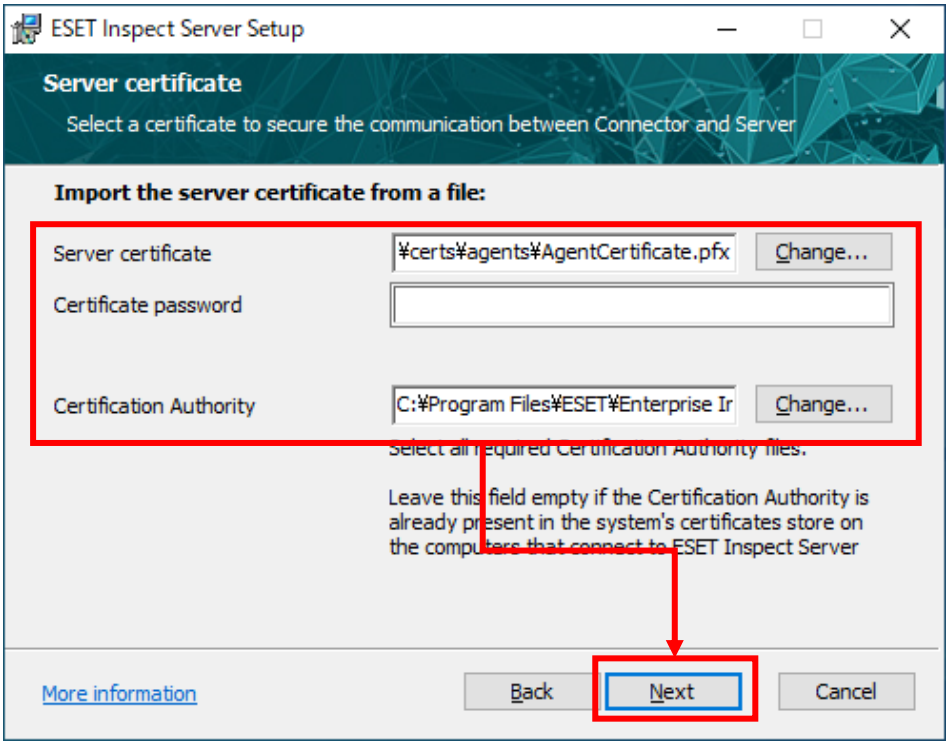
(9). Connecting to ESET Security Management Center ダイアログが表示されるので、［はい］を選択します。



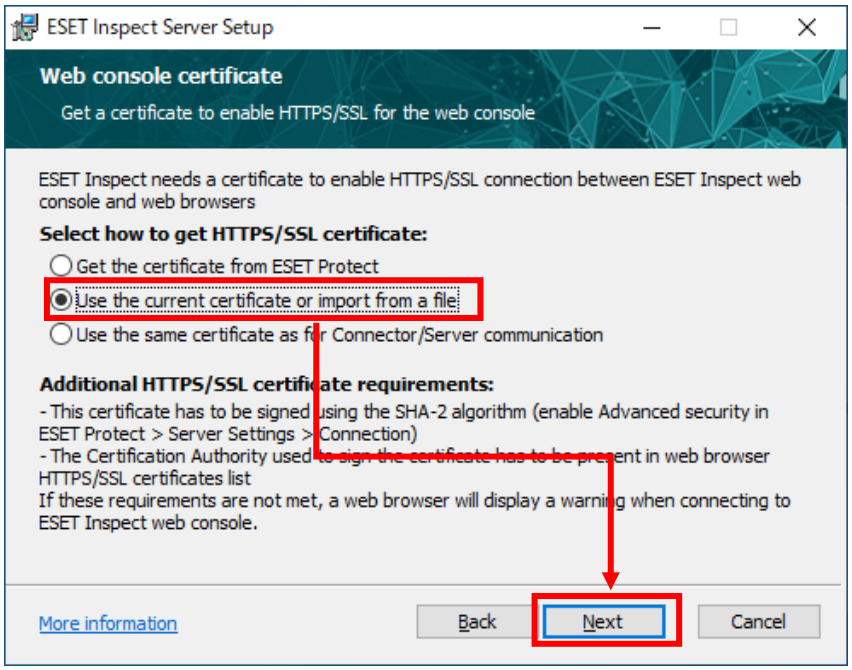
(10). Server certificate 画面で、[Use the current certificate or import from a file]を選択し、[Next]をクリックします。



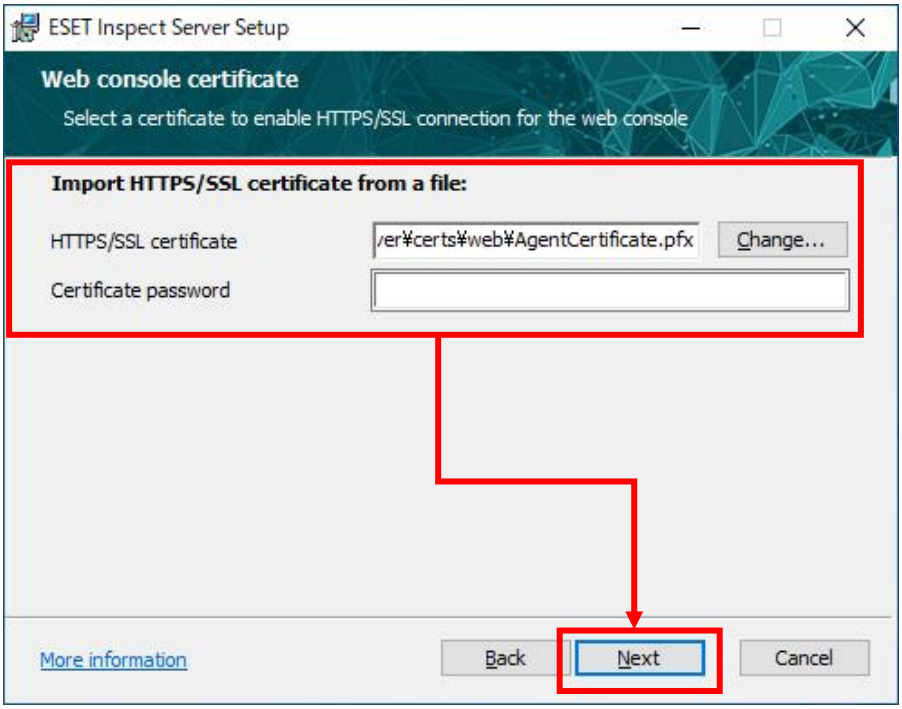
(11). Server certificate 画面で、証明書情報が入力されていることを確認し、[Next]をクリックします。



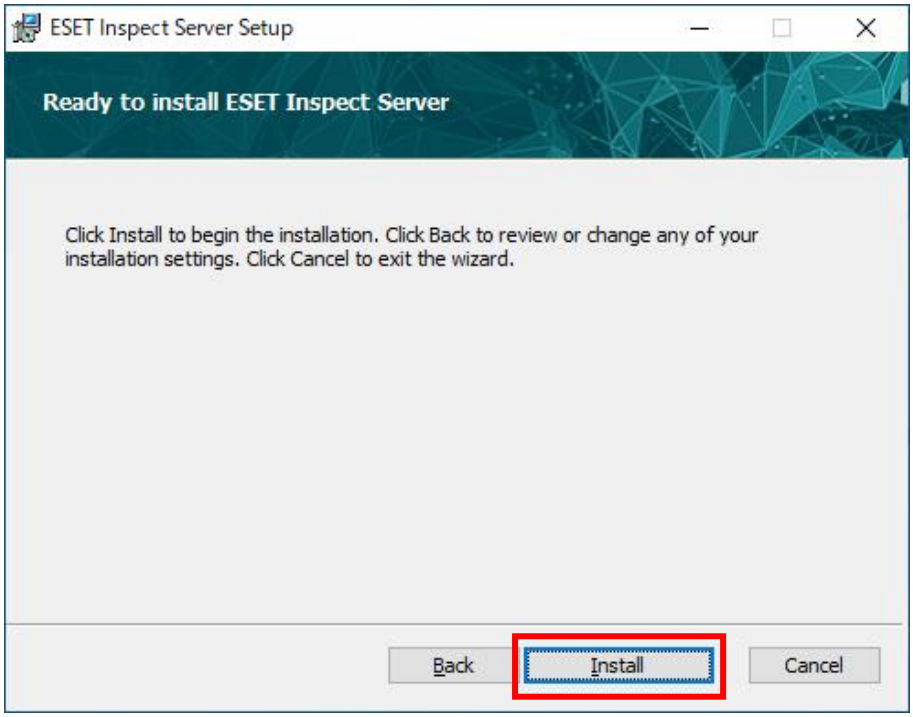
(12).Web console certificate 画面で、[Use the current certificate or import from a file]を選択し、[Next]をクリックします。



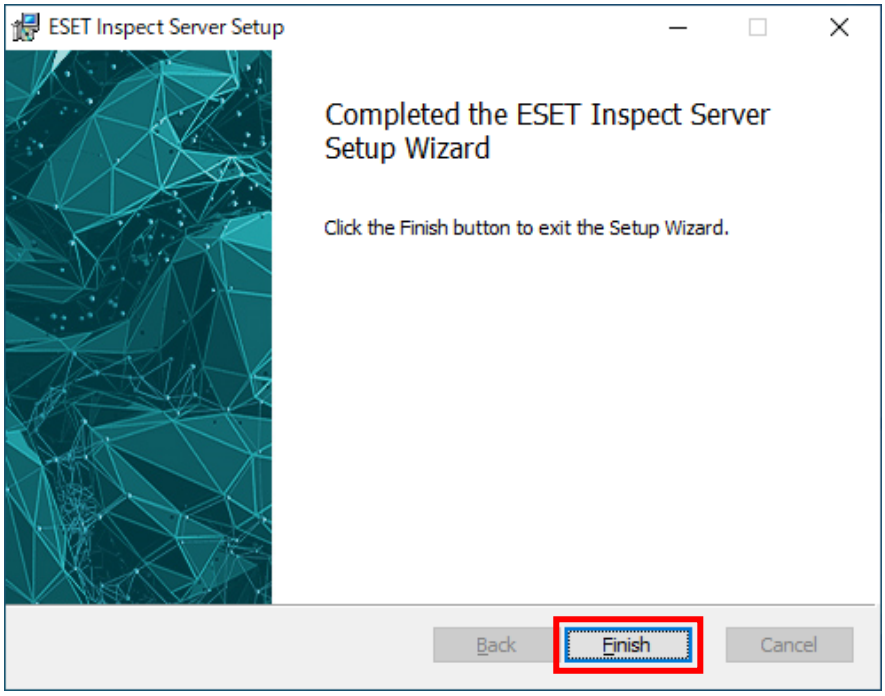
(13).Web console certificate 画面で、証明書情報が入力されていることを確認し、[Next]をクリックします。



(14).Ready to install ESET Enterprise Inspector Server 画面で、[Install] をクリックします。

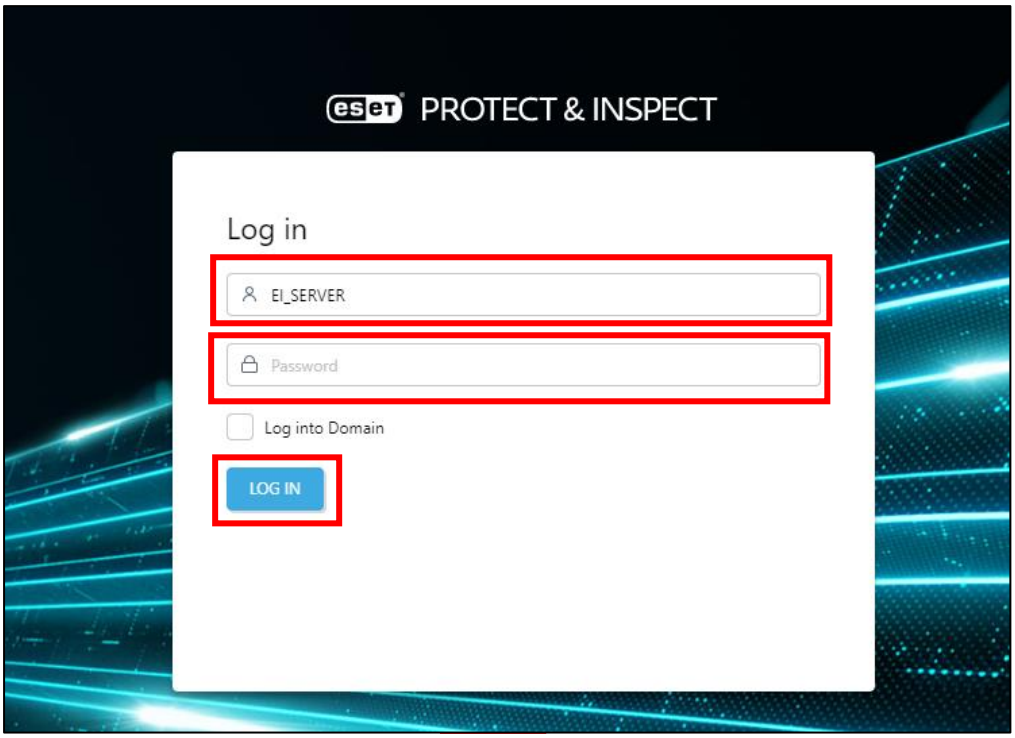


(15).Completed the ESET Enterprise Inspector Server Setup Wizard 画面で、[Finish] をクリックし、EI Server のバージョンアップを終了します。

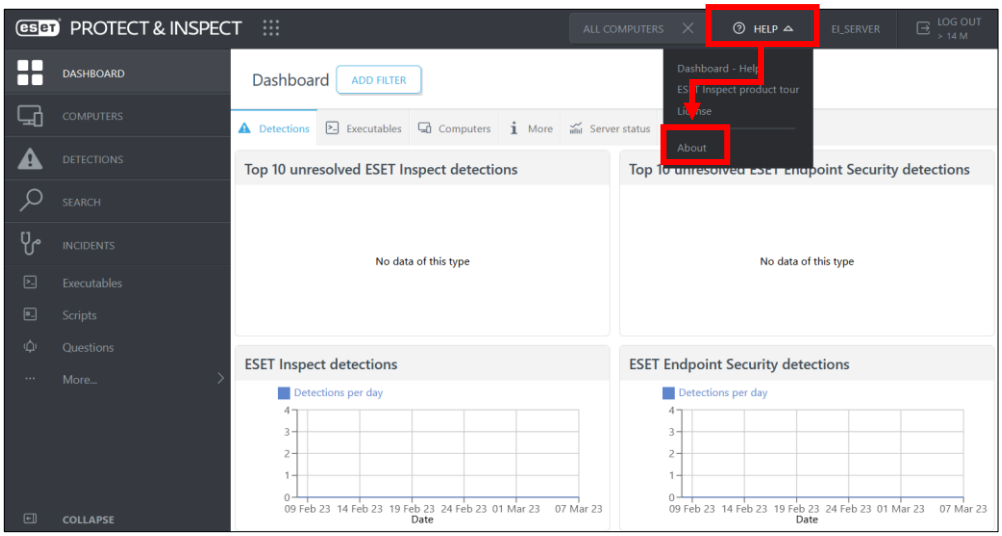


(16).[https://(EI Server を導入したサーバーの IP アドレス)]にアクセスします。

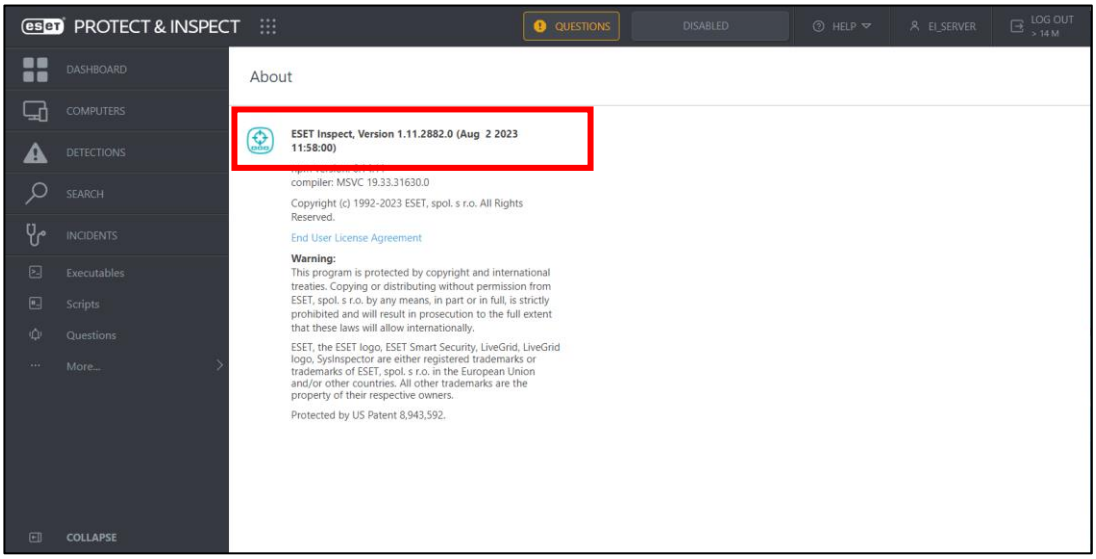
EI Web Console にログインする、ユーザー名とパスワードを入力し、[LOG IN]をクリックします。



(17).コンソール画面の右上の「HELP」から「ABOUT」をクリックします。



(18).EI が V1.11 になっていることを確認します。

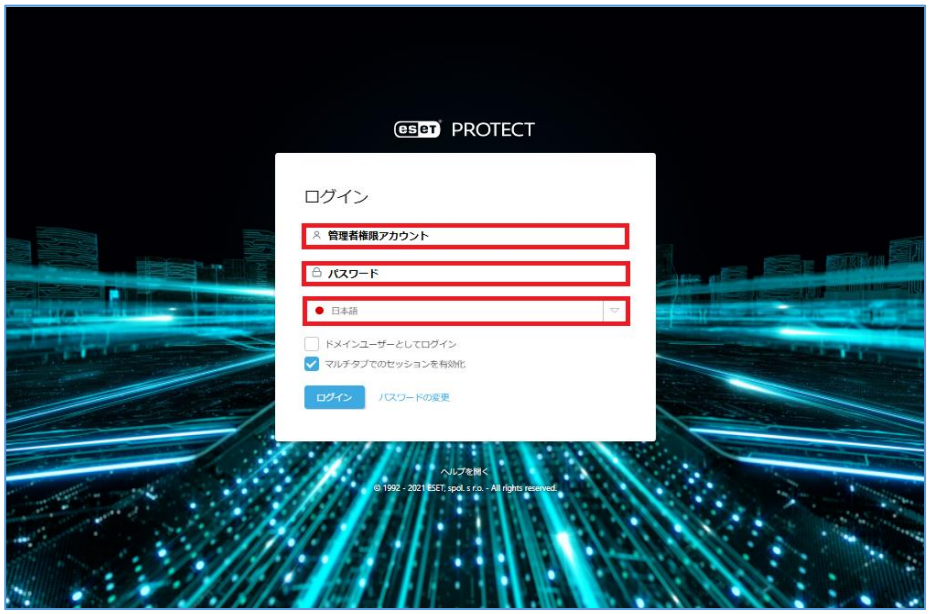


7. EI Connector のバージョンアップ【EP 側作業】

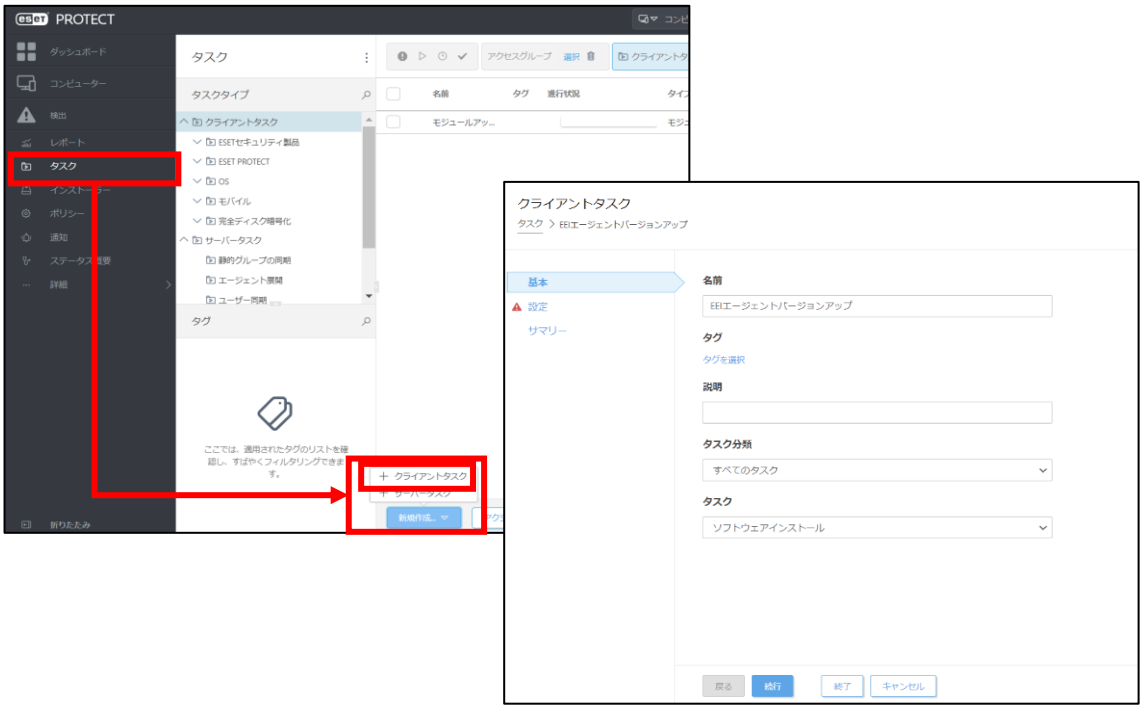
1-2　クライアントタスクによる EI Connector のバージョンアップ

(1). https://(EP の IP アドレス)/era にアクセスし、EP Web Console に管理者権限のあるアカウントでログインします。

「日本語」を選択して、「ログイン名」・「ログインパスワード」を入力し、「ログイン」をクリックします。



(2). [タスク]->[新規作成]-> [クライアントタスク]にて次の通り設定し、[終了]をクリックします。



■[基本]セクション

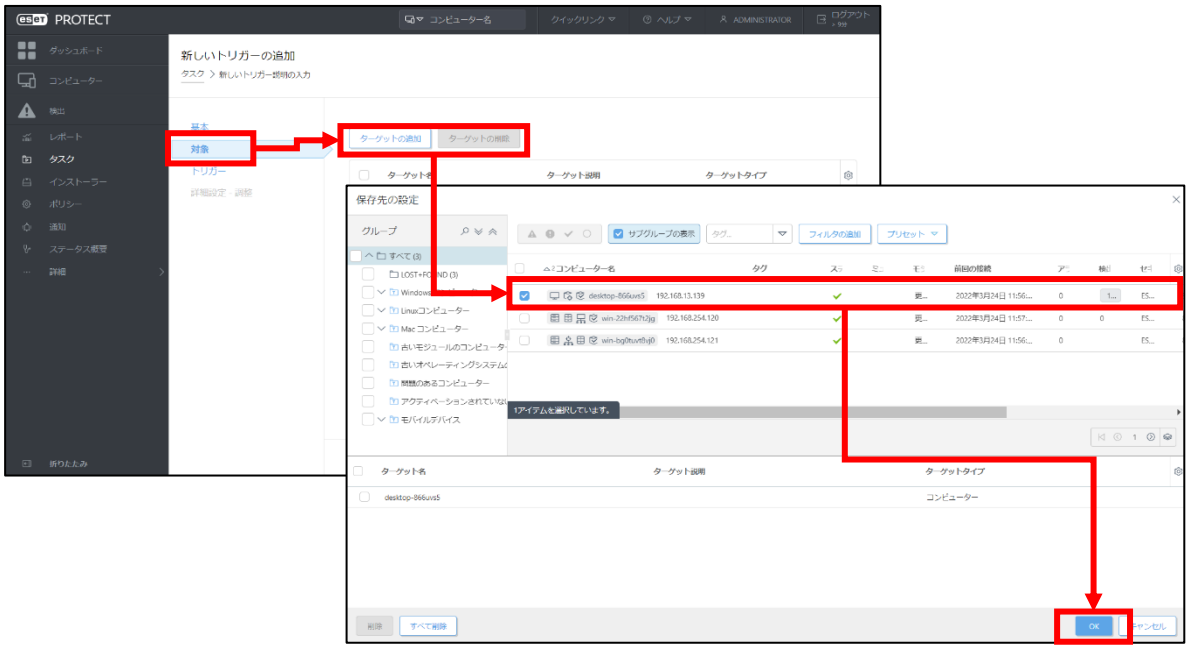
名前：	任意の名前を設定します
タグ：	任意にタグを設定します
説明：	任意の説明を記載します
タスクの分類：	すべてのタスク
タスク：	「ソフトウェアインストール」を選択します

■[設定]セクション

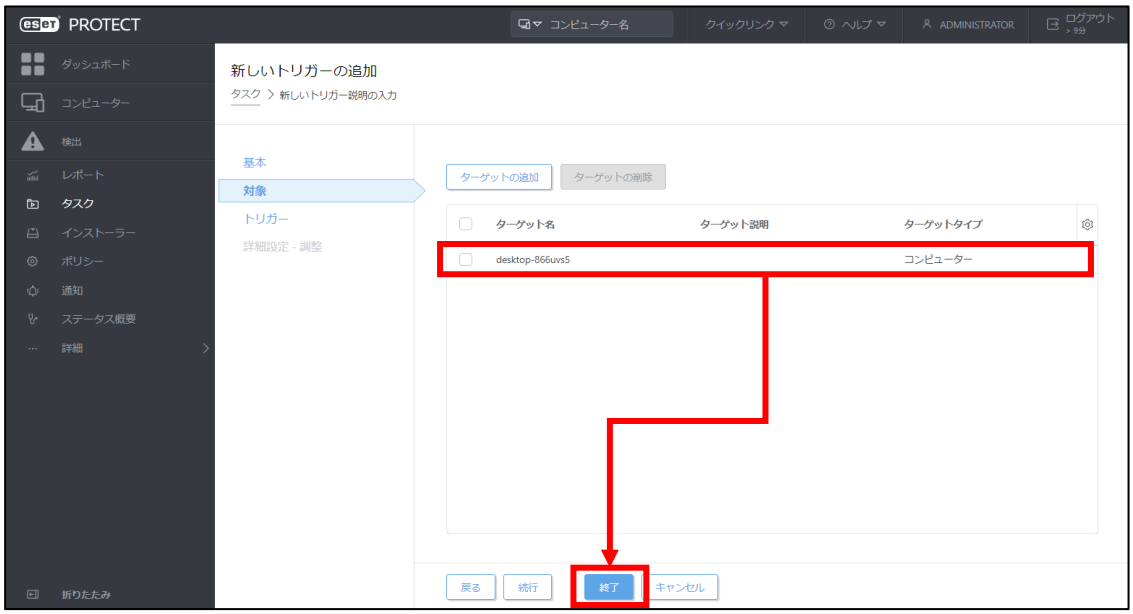
ESET ライセンス：	登録した EI ライセンスを選択
インストールするパッケージ：	[リポジトリからパッケージをインストール]を選択
	<パッケージの選択>：EI Connector V1.11 を選択
[アプリケーションエンドユーザー使用許諾書の...]	チェックを入れます
インストールパラメータ：	なし
必要なときに自動的に再起動	チェックなし

(3).[トリガーの作成]をクリックします。

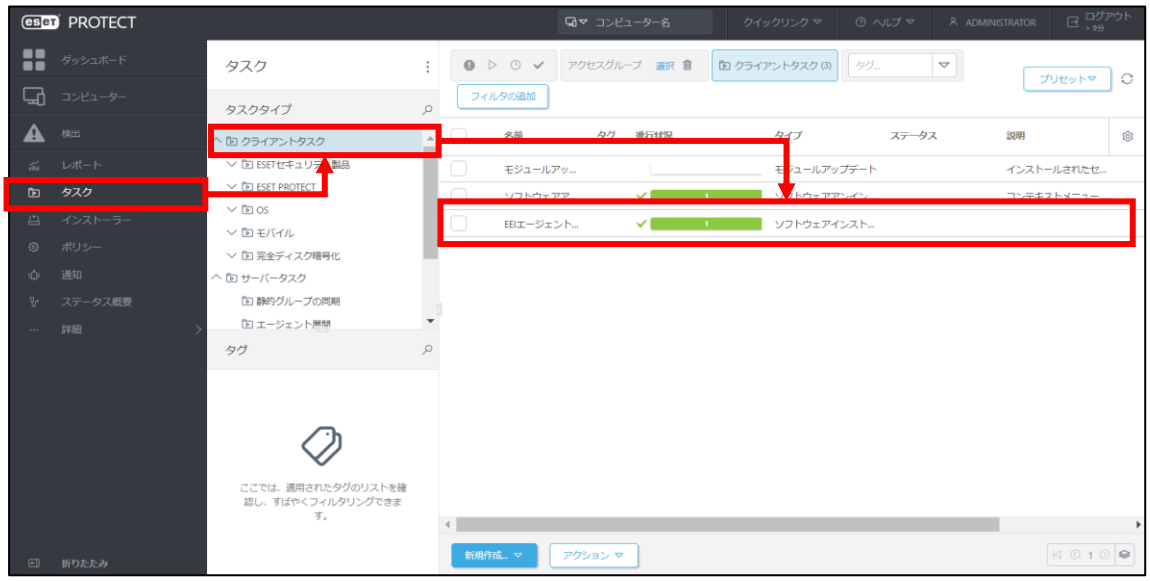
(4). [対象]セクションで、[コンピューターの追加]または[グループの追加]をクリックし、
EI Connector をバージョンアップする対象を選択後、[OK]をクリックします。



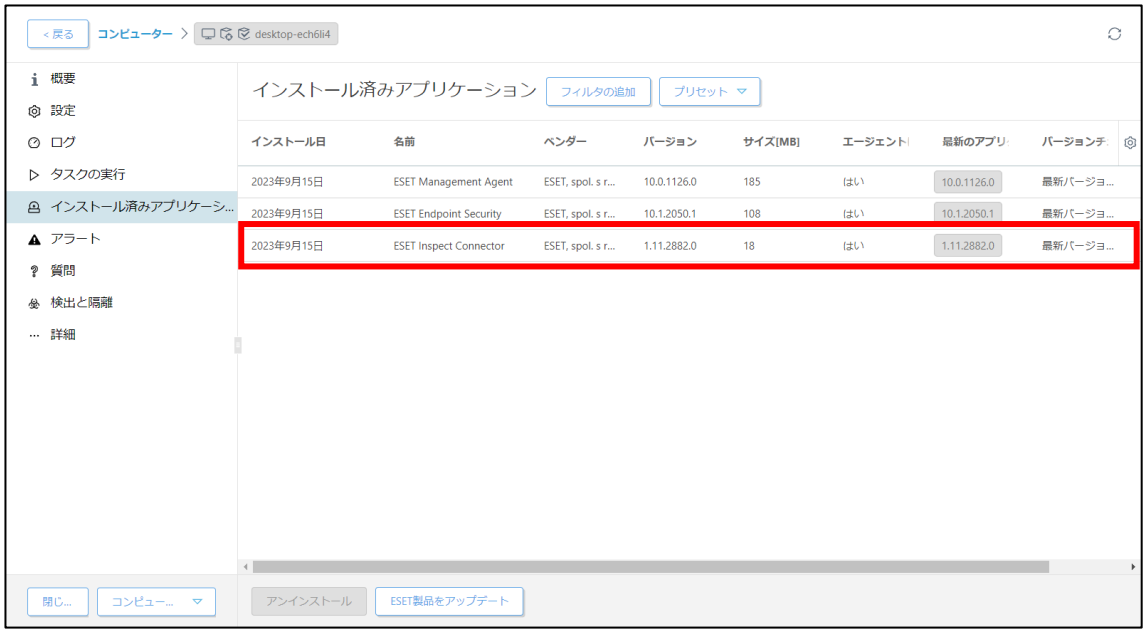
(5). [終了]をクリックします。



(6). 該当タスクの進捗状況が緑色に遷移したらタスクが成功です。



(7). [コンピューター]より対象のコンピューターを選択して[詳細を表示]-> [インストール済みアプリケーション]で「ESET Inspect Connector V1.11」にバージョンアップされていることをご確認ください。



以上でバージョンアップは完了です。