exterro®
Data Risk Management

MANAGED SITE SERVER OVERVIEW GUIDE

AUGUST 2025

Table of Contents

About Exterro

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Data Risk Management platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world's largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

1 Exterro Managed Site Server

1.1 What is Exterro Managed Site Server?

Exterro FTK has diligently supported the utilization of Site Servers[1], serving as a focal point for collecting and interrogating Off-Network Agents[2] before communicating with the application host (server).

Recognizing the evolving needs of growing enterprises, **Exterro has strategically engineered the new Managed Site Server in combination with the existing infrastructure,** not only resolving existing (Agent check-ins[3]) challenges faced by many organizations, but also ensures sustained efficiency and performance of the existing Public Site Server infrastructure.

[1] The Site Server component handles both communicating with the Agent component and managing Job telemetry data, including any information gathered by an Agent following the completion of a data collection Job.

[2] Collection Jobs are executed by the Exterro Agent ("Agent"), a modular application that is installed on computer endpoints and performs the secure forensic-level access, analysis, and collection of computer endpoint data.

[3] Check-ins are a feature set at the Agent level, enabling the Agent to automatically inform the Site Server of its new IP address whenever it changes while it is connected to the network. Additionally, this lets an agent automatically create a "computer" entry in the "Data Sources" area of the application without manual intervention.

1.2 Technological Outline

The Managed Site Server now utilizes the following technologies:

- RESTful API
- HTTPS

Exterro has significantly improved scalability by introducing a new RESTful API, which allows Public Site Servers to handle a substantially larger number of requests simultaneously. Communication is completed over HTTPS (Hypertext Transfer Protocol Secure) to handle off-network Agent check-ins.

1.2.1 PFX Certificate

The Managed Site Server requires a PFX certificate to take advantage of the new changes introduced.

What is a PFX Certificate?

A PFX certificate is a file format used to store a private key and a public certificate together, along with any intermediate certificates and root certificates needed to establish a complete trust chain. This file is encrypted and protected by a password to ensure the security of the sensitive information it contains. The format is widely supported across different platforms and can be used to transfer certificates and keys securely between systems or services.

Why is a PFX Certificate Required?

A PFX certificate is required for the Managed Site Server to utilize the HTTPS Protocol. Agents can be configured whether to require the Agent system to trust the HTTPS certificate presented by the Managed Site Server. To ensure HTTPS check-ins occur, the following certificate properties must be configured appropriately:

- Common Name (CN)
    - Must include the domain of the FTK Application host
- Certificate Authority (CA)
- Issuer
- Validity Dates

Valid CA Signed Certificates:

If a CA certificate is valid and trusted by an agent system, then the connection will be secured via HTTPS. A valid, CA Signed certificate can be provided to take advantage of the new Managed Site Server and its check-in scalability.

Invalid CA Signed Certificates:

If a CA certificate is not valid, then TCP (Pre-Managed Site Server behavior) will be used and the number of check-ins will be limited.

Establishing a Connection via HTTPS Without a Valid CA Signed Certificate:

Agents can be configured to establish connections with a Site Server without a valid CA Signed certificate. During the installation of an Agent, the setting "HTTPS_CER_ENABLE" is turned on by default (set to "1"), meaning it will be active even if this specific setting isn't explicitly included in the installation process. This setting determines if an agent is required to verify a CA (Certificate Authority) Signed certificate for HTTPS connections. If verification of a CA Signed certificate fails, the agent will switch to using TCP for its connections. Exterro does not advise users to pass this argument during agent installation, and users should consult the support team for more information.

1.2.2 Default Port Usage

- **TCP Port:**
  - By default, TCP (Transmission Control Protocol) connections will be handled in port 54545. If provided, the port value mentioned in the Public TCP Port field in the Site Server Configuration UI will be used.

Notes:

- The public Site Servers use the TCP port.
- The 54545 port is associated with the Exterro Site Server service.

- **A TCP Port will be used to handle:**
  - Check-in Interval (Phone Home) value updates.
  - All Agent related jobs.
  - Live Preview related connections.
  - Agent check-ins if a CA Signed certificate cannot be verified.

- **HTTPS Port:**
  - By default, HTTPS will be handled in the port 443 (default value). If provided, the value mentioned in the HTTPS Port field in the **Agent Check-ins settings** section of Site Server Configuration UI will be used.

Note: The 443 is the default port associated with the Exterro Site Server Managed API service.

- **A HTTPS port will be used to handle:**
  - Agent check-ins when a CA (Certificate Authority) Signed certificate has been successfully validated.
  - Agent check-ins if the Agent has been set up to use HTTPS connections even without a validated CA Signed certificate.

Warning: *The port numbers of Public HTTPS and Public TCP should always be unique.*

- ***Firewall Rules:***
  - *Firewall rules for port 54545, or any other port chosen for TCP connections, are automatically added to the Windows Firewall by the Site Server once changes are implemented. If other firewall systems are in use, these exceptions need to be configured manually.*
  - *In contrast, the port used for HTTPS uses a generalized port (443) by default and is open by most firewalls. If customized ports are used for HTTPS, connections must be manually configured to allow incoming traffic in any firewall, as this setup is not automated.*

1.3 Minimum Hardware Requirements

Exterro suggests the following minimum hardware specifications to ensure the best performance:

Component	Processor	Memory
Site Server	4 Core	8GB RAM

1.4 Benchmark Results (Check-ins)

Exterro conducted tests within a controlled environment using the minimum hardware specifications, we observed 20,000 successful check-ins by Agents to the Managed Site Server.

Hardware Utilized for Benchmarking	Agent Count	Time to Complete Last Check-in in the database (in mins)	Check-in Interval Tested (in mins)	Average Check-ins per minute
Processor: 4 Core	5000	17	30	291
RAM: 8 GB	10000	35	5	
	15000	50	5	
	20000	70	5	

Note: These metrics relate to check-ins only with the default configurations. The results can be extrapolated by increasing the 'Max Incoming Threads' parameter in the Site Server UI.

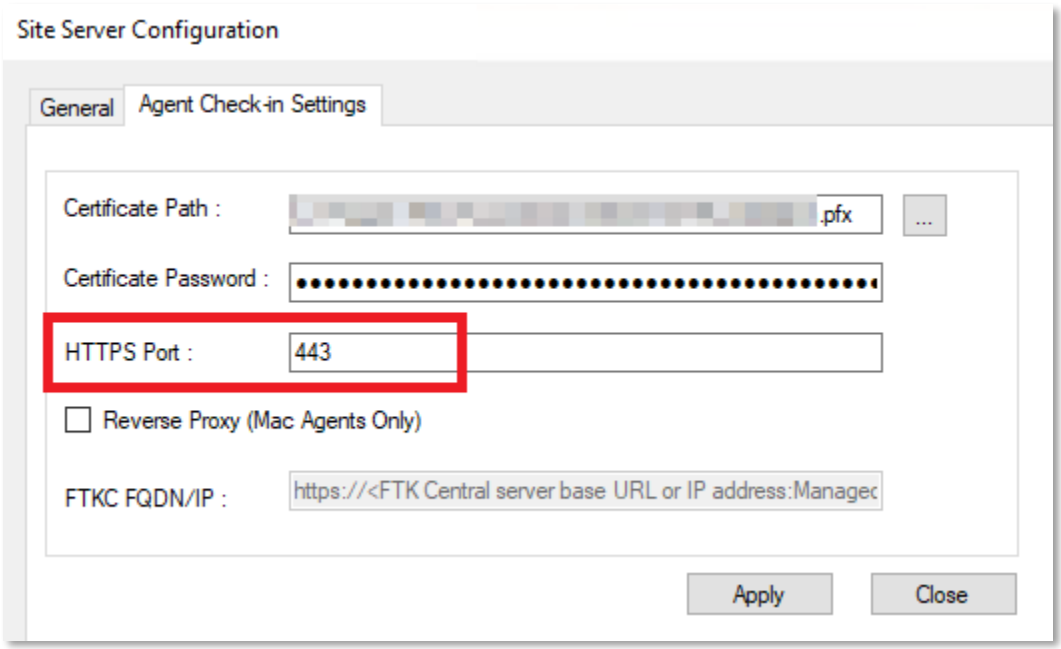
***For example**, increasing the default Max Incoming Thread count from 50 to 100 will double the number of agent check-ins.*

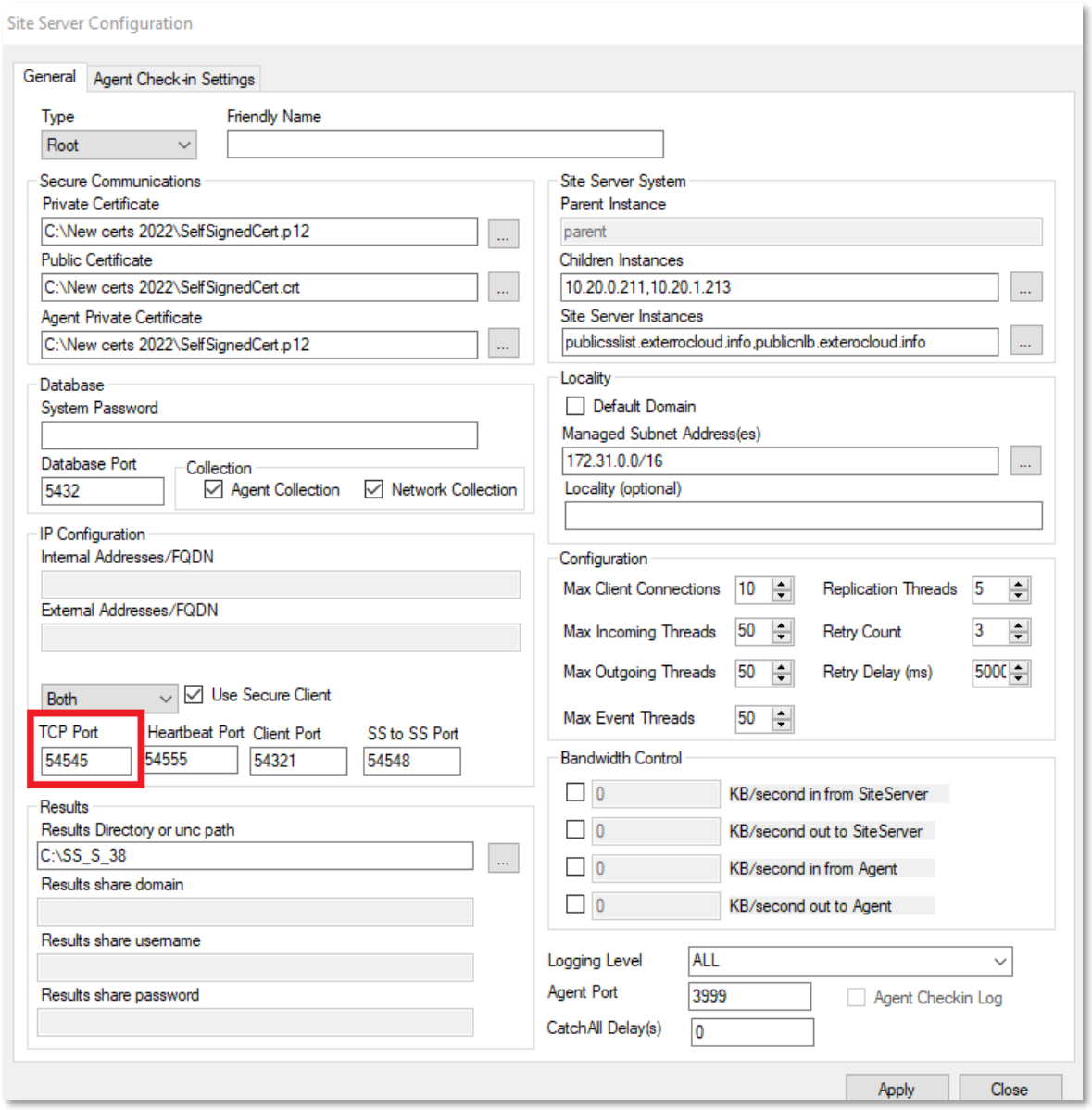
1.5 Installation and Configuration Options

1.5.1 Newly Introduced Configuration Options

The Managed API configuration options have been moved from the JSON file into the newly introduced **Agent Check-in Settings** section of the **Site Server Configuration** pop-up. Moreover, the Managed API service will be started automatically upon configuring and saving the **Agent Check-in Settings** section (previously, it was applicable only for public site servers).

Note: Refer to the Upgrading the Site Server section for more information related to upgrading the Site Server.





Notes:

- For Site Servers to work with Network-Level load balancers, the FQDN or DNS name of the network-level load balancer must be mentioned in the 'Public Instance' field along with the public TCP port number.
- In order to resume a job interrupted in the network load balancer, the user has to configure the same result directory or UNC path for all the site servers in the network load balancer (NLB).

1.5.1.1 Rebuilding the Site Server Database

For the site server to function properly after making changes to it, the Site Server's database should be rebuilt.

Steps:

The following steps should be performed on each Site Server:

1. Open a Command Prompt.
2. Change directory ("cd") to the PostgreSQL BIN folder (typically "C:\Program Files\AccessData\PostgreSQL\14.0\bin").
3. Log in to the PostgreSQL using the following command syntax:

```
psql -p [port] -U postgres
```

4. Enter the Postgres password when prompted.
5. At the postgres=# prompt, drop the "ssdb" database using the following command:

```
DROP DATABASE IF EXISTS ssdb WITH (FORCE);
```

6. At the postgres=# prompt, drop the "siteserver" user using the following command:

```
DROP USER IF EXISTS siteserver;
```

7. Open the Site Server Configuration tool.
8. Provide the **System Password** and **Database Port** for PostgreSQL.

9. Click **Apply**.
10. Close the Site Server Configuration tool.

1.5.1.2 Configuring the Site Server to Use a PFX Certificate

To take advantage of Managed Site Server HTTPS check-ins, users must configure a .PFX certificate and any associated certificate password.

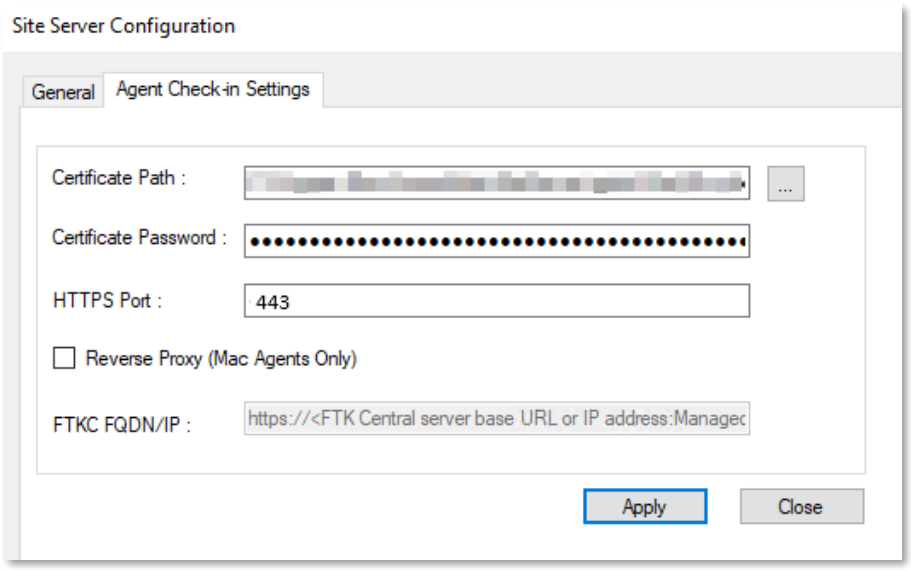
The **Agent Check-in Settings** section can be configured to initiate reverse proxy or HTTPS check-ins.

Important Note: The following fields should be configured for the corresponding Agents:

Agent Type	Fields to be configured
Off-Network Windows Agent	• Certificate Path • Certificate Password • HTTPS Port
Off-Network Mac Agent	• Certificate Path • Certificate Password • HTTPS Port • Reverse Proxy (Mac Agents Only) • FTKC FQDN/IP
Both Off-Network Windows and Off-Network Mac Agents	• Certificate Path • Certificate Password • HTTPS Port • Reverse Proxy (Mac Agents Only) • FTKC FQDN/IP

Steps:

1. Install the Site Server.
2. From the **Site Server Configuration** pop-up, select the **Agent Check-in Settings** section.



3. Browse and select the required certificate from the **Certificate Path** field.
4. Provide the **Certificate Password.**

Note: Passwords must be provided in plain text and will be encrypted automatically when the Site Server service is restarted.

5. The value for **HTTPS Port** is updated as **443** by default. However, you can change it based on your preference.

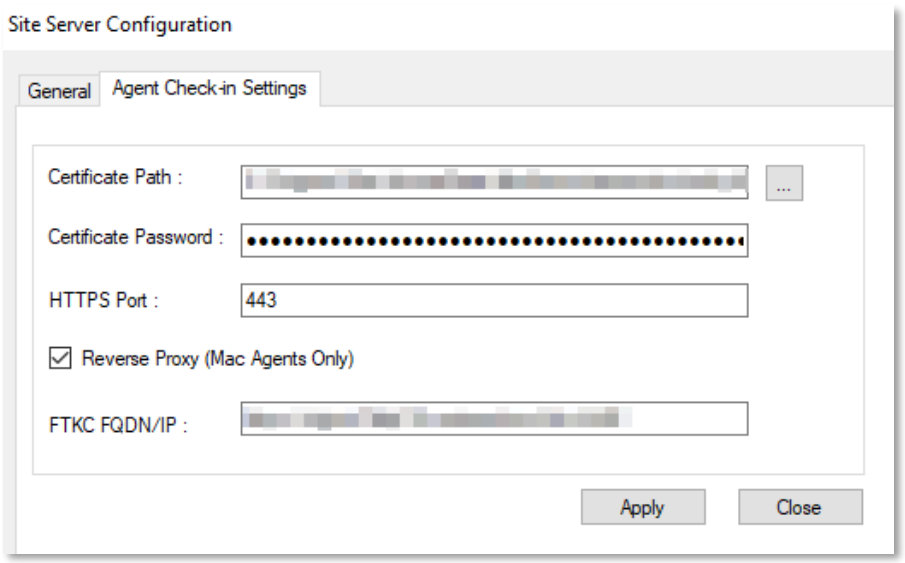
Note: The value in **HTTPS Port** determines the managed site server service's running port.

6. Check the **Reverse Proxy (Mac Agents Only)** option for reverse proxy Mac agents.

7. Provide the value in the below syntax for the **FTKC FQDN/IP** field:

```
<FTK Central application URL>:<managed API Port>
```

Note: The FTKC FQDN/IP field will be enabled only upon checking the **Reverse Proxy (Mac Agents Only)** field.



8. Click on **Apply** to save the configurations made in the **Agent Check-in Settings** section.

Upon clicking on **Apply**, the Exterro Site Server Managed API will be restarted.

1.6 Installation Script for Off-Network Agents

The script provided below serves as a template for installing an agent:

```
msiexec /I "Full_Agent_Path" CER="Full CertificatePath" SSLIST="<IP/FQDN/URL_of_SiteServer>"
HTTPSPORT=443 TCPPORT=54545
```

Notes:

- If the agent installation uses the same Fully Qualified Domain Name (FQDN) or IP address for the PUBBSS parameter (formatted as PUBSS_FQDN/IP:443), the HTTPS_HOST_PORT argument is optional. In other words, if the values are unique, then the HTTPS_HOST_PORT argument is mandatory.
- By default, port 443 is designated for all HTTPS check-ins. To use a different port, you must specify the HTTPS_HOST_PORT argument during the agent installation process.
- TCP connections and HTTPS connections cannot be configured to use the same port. The port numbers should always be unique.
- If the agent cannot connect using HTTPS due to issues with the domain or port, it will default to using TCP.
- The PUBSS parameter should be changed to SSLIST and the HTTPS_HOST_PORT argument should be changed to HTTPSPORT.

Agent Installation Parameters:

The following are the commonly used parameters for Off-Network Agent installations.

Note: The complete list of parameters can be found here.

Parameter	Value	Default Value	Required	Description
CER=		N/A	Yes	Full path to the public certificate. The path must be enclosed in quotes if it contains spaces. Acceptable certificate formats are P7B, P7C, DER, CER, and CRT.
PORT=		3999	No	The port that the agent will be listening on. If not specified, the default value is assumed.
PING_SIZE		5242880	No	The Ping Size represents the number of bytes of data transferred for checking Latency.
TCPPORT	54545	54545		The Public TCP Port number. ***Note:*** *Only a single value can be provided for this parameter. For the users with multiple regions, the same Public TCP Port number should be used across all*
HTTPSPORT	443	443		The HTTPS Check-in port number. ***Note:*** *Only a single value can be provided for this parameter. For the users with multiple regions, the same check-in port number should be used across all available regions of the Site Server.*

1.7 Site Server Log Information

The following table provides the list logs relating to the Site Server, its location, and its contents.

Component	Location	Log Contents
Site Server	***C:\Program Files\AccessData\SiteServer***	The site_server log will only contain information about Agent jobs. **This log file should be used to troubleshoot Off-Network Agent issues, except check-ins (unless done via TCP).**
Agent Check in logs	***C:\Program Files\AccessData\SiteServer***	The PUBSSLogging log will contain information about check-ins completed in TCP and the last updated contact.
Managed Site Server	***C:\Users\Public\Documents\AccessData\AccessDataLogs*** ***Note:*** *By default, the above location will be used. However, you can configure this location from the file present in the below location:* ***C:\Program Files\AccessData\SiteServer\ManagedApi\log4net.config***	The SiteServerManagedHostLog log will contain information about agent check-ins via HTTPS, last updated contact, and available task check. **This log file should be used to troubleshoot Off-Network Agent check-in issues.**

1.8 Automatic Agent Updates (Windows)

With the release of FTK 8.2, Windows Agents now automatically update during upgrades. The upgrade process leverages a .cab file (signed by Exterro) located in the Agent directory:

```
C:\Program Files\AccessData\SiteServer\Agent
```

The solution leverages an agent.ini file to store installation arguments and ensures that the agent is updated by checking for newer versions (specifically the last 3 digits) available on a site server. If a new release includes an update for an Agent, a .cab file (which can consist of the agent installer and other components) will be updated accordingly and automatically copied to the designated Results folder (configured within the Site Server).

General Flow:

1. The Managed Agent makes a call to the public site server via the API endpoint:

   ```
   PublicAgent/CheckInAgentUpdate
   ```

2. The response from this call contains the current agent version stored in the Site Server's Agent folder.
3. This version received from the site server is compared to the version of the currently installed agent on the client machine.
4. If the installed version matches the public site server version, no update process will occur.
5. If a newer version is available, the agent will initiate an update process and silently install the agent using previously used installation parameters.

Note:

It is to be noted that this functionality is only supported by Agents in releases FTK 8.2 and later. It is not compatible with Agents from earlier versions. Users are required to uninstall pre-8.2 Agent versions before taking advantage of this functionality. In addition, all site servers involved must be updated for this functionality to operate.

1.9 Upgrading/Fresh Installing the Site Server

Notes:

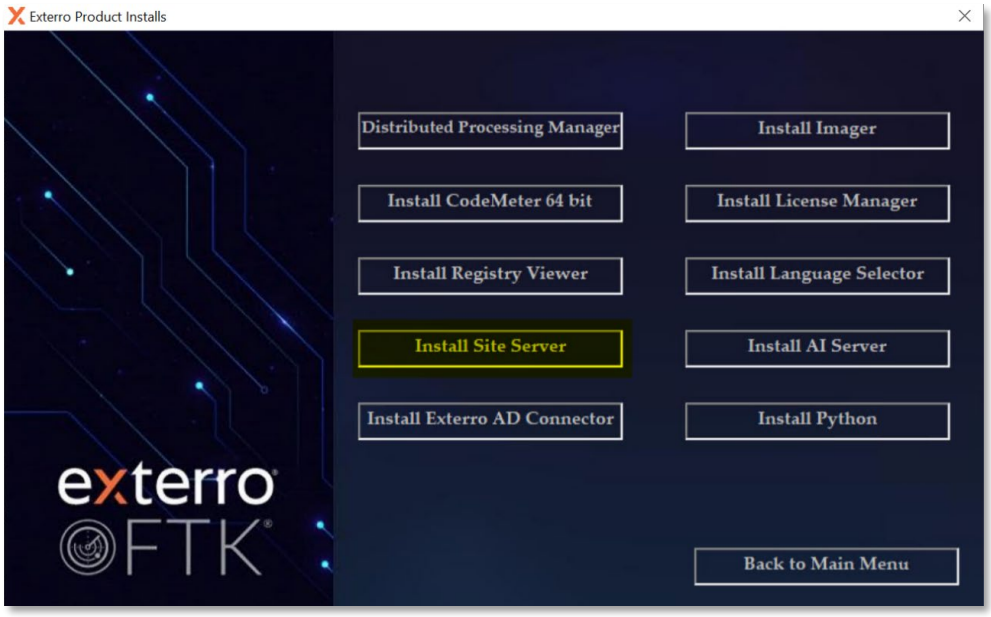
- Upgrading the Site Server should be done only on machines running the site server released versions of 8.0, 8.1, 8.2 or their service packs. It is mandatory to install the PostgreSQL 14.17 version before installing the Site Server.
- Enable the 'Add Installation File Path to Windows Defender Exclusion List' option to incorporate all installation file paths into the Windows Defender (Windows Security) application.

***Warning**: The file paths will not be added in Windows 10 or Windows 11 instances where the Microsoft Defender Antivirus service is not running.*

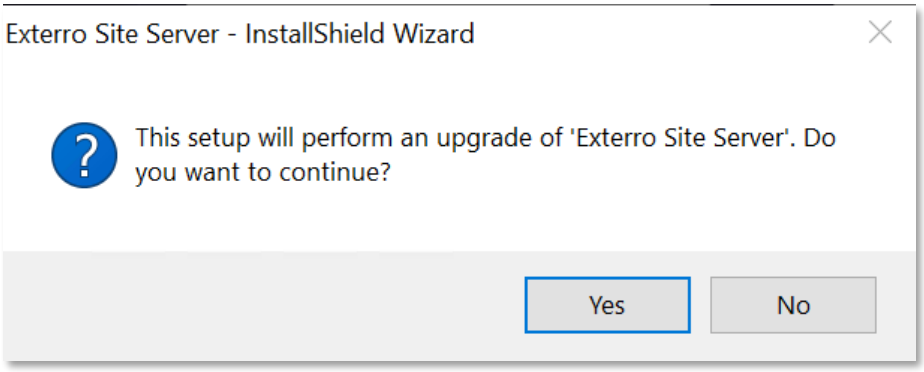
The following steps must be followed on all machines running a Site Server:

Steps:

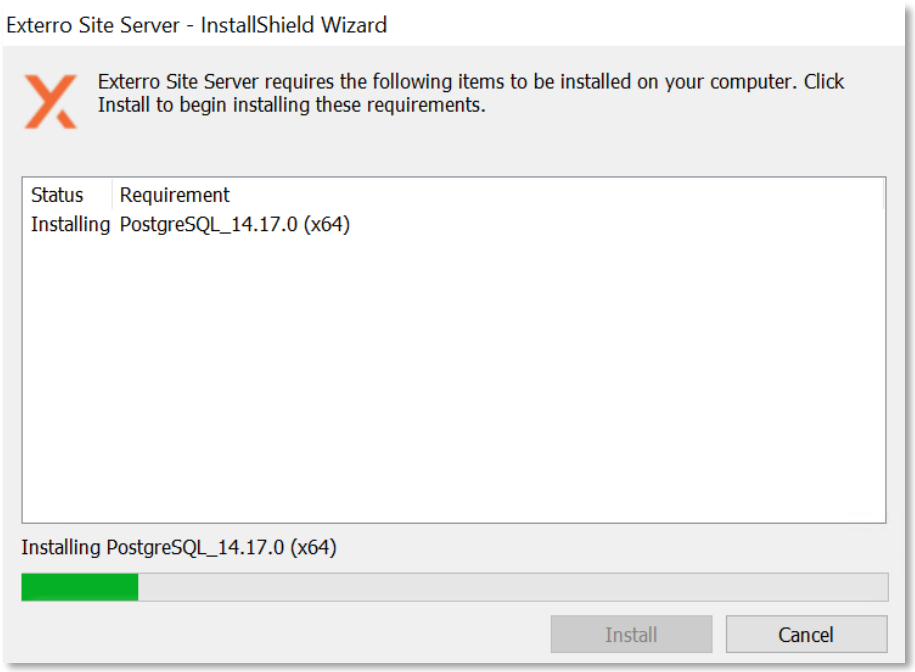
1. Go to the **Site Server Results** folder and delete all the contents inside it.
2. Download the ISO from the ***Exterro Downloads page***.
3. Mount the ISO and run **AutoRun.exe** as Administrator.
4. Select the **Install Site Server** product.



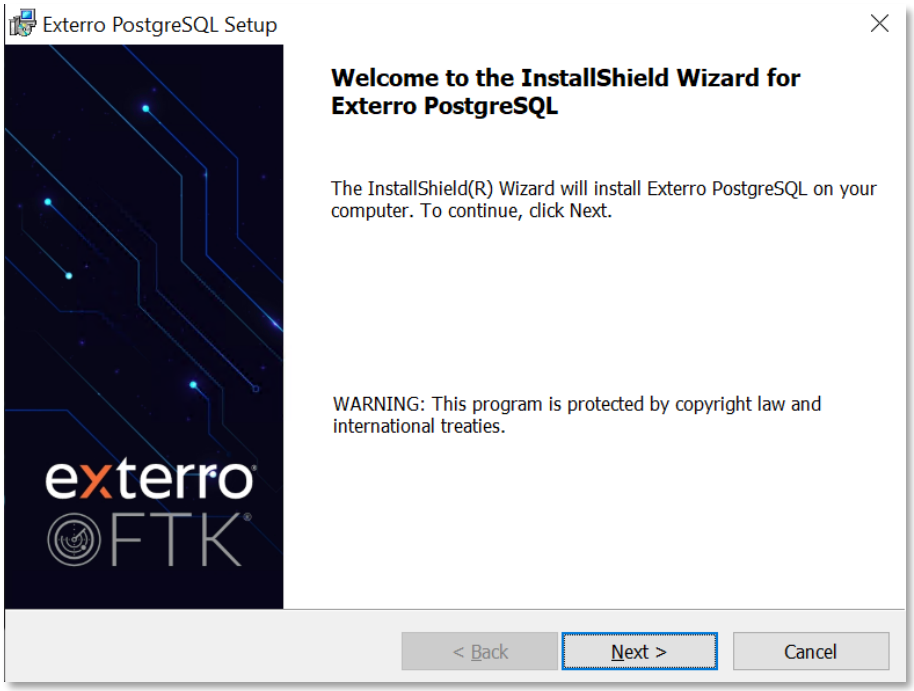
- The following page is displayed.



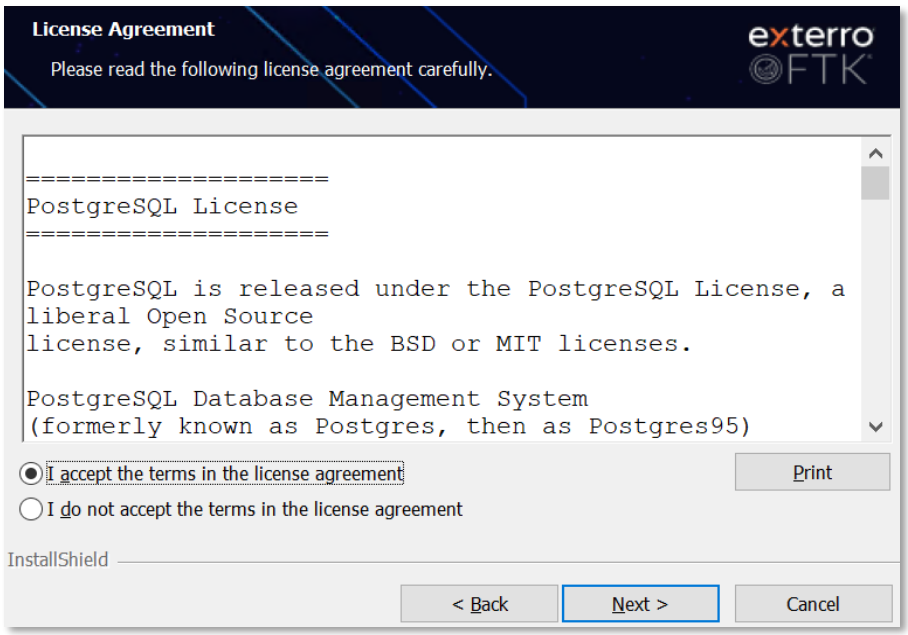
5. Click **Yes** to proceed with upgrading the Site Server to the latest version.
6. Click **Install** to upgrade PostgreSQL 14.17.



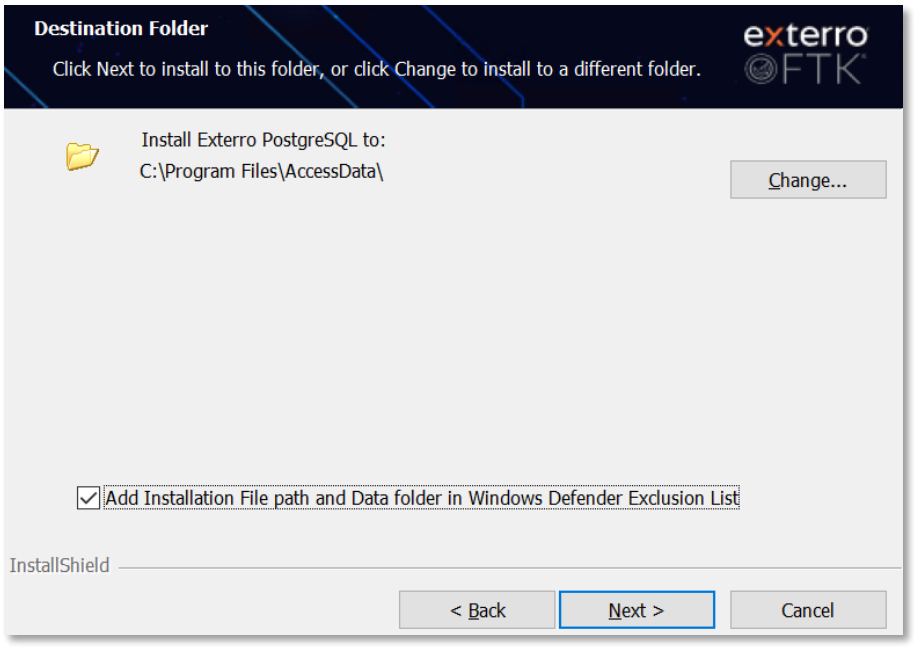
- The following Welcome screen is displayed.



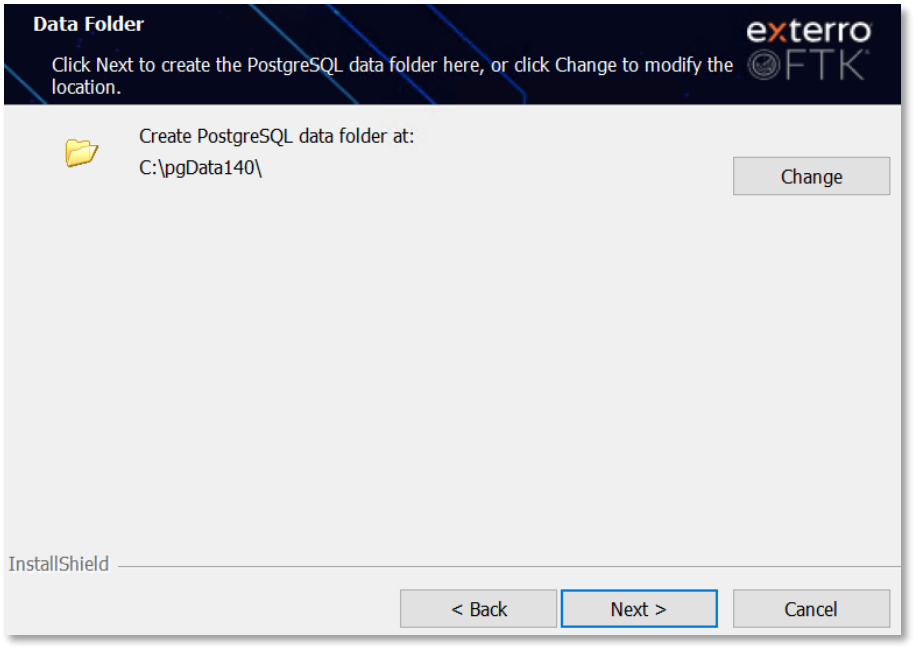
7. Click **Next**.
8. Accept the End User License Agreement (EULA) and click **Next**.



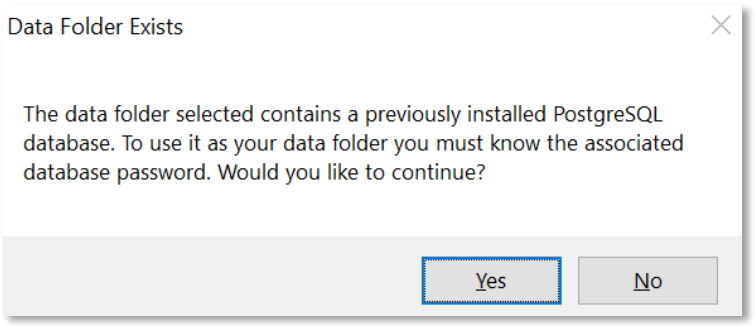
9. Choose the desired **Installation Directory** and click **Next**.



10. Select the **Data Directory** and click **Next**.

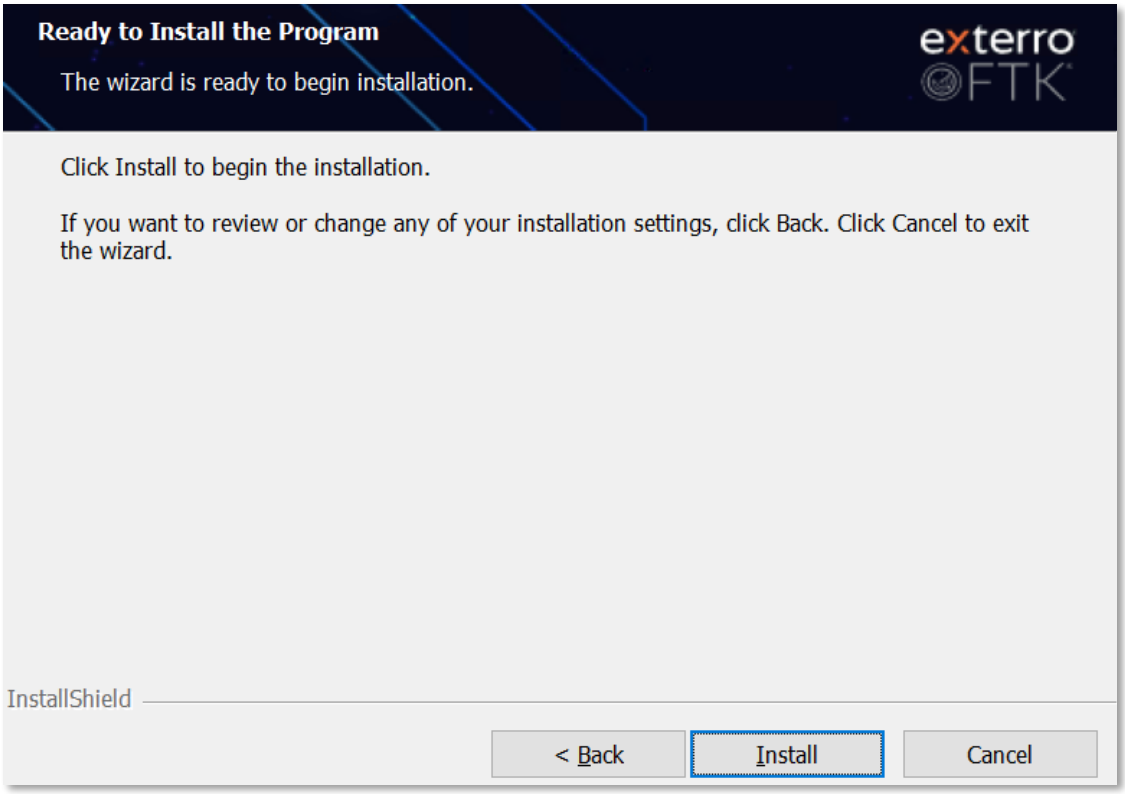


- The following pop-up is displayed.



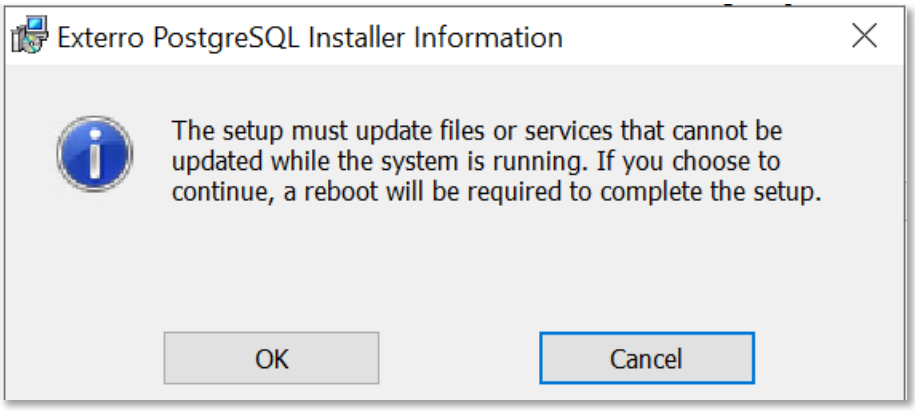
11. Click **Yes**.

- The following installation page is displayed.

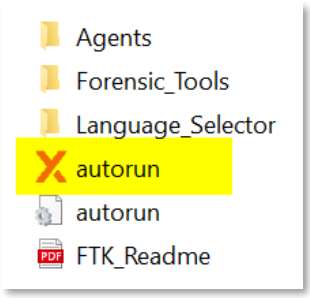


12. Click **Install**.

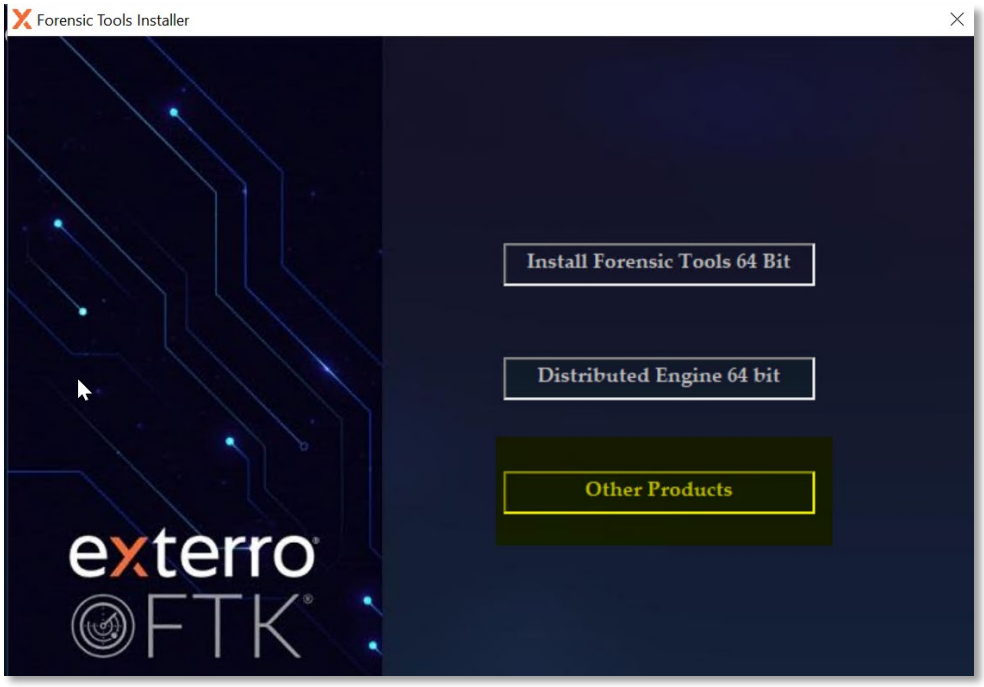
- The following pop-up is displayed.



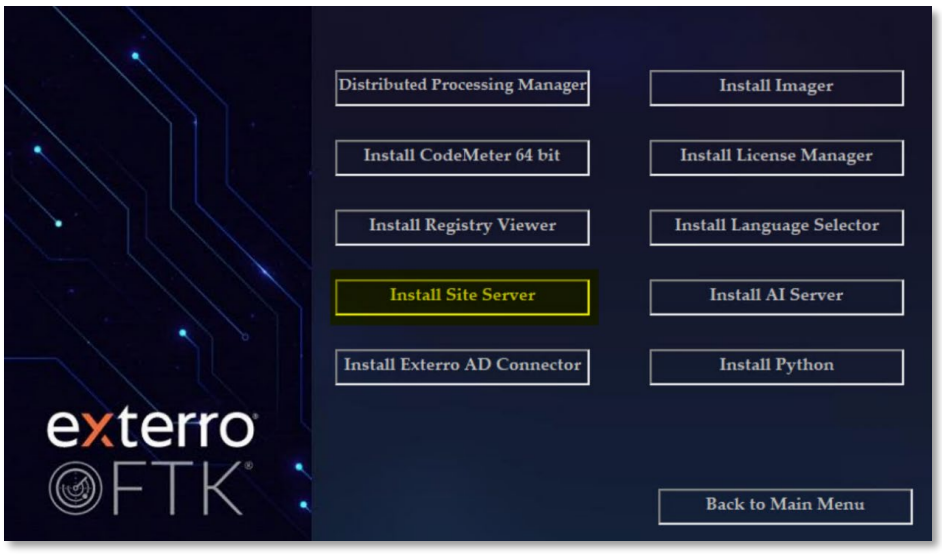
13. Monitor the installation progress and click **Ok**.
14. Once the installation is complete, click **Finish**.
15. After clicking on 'Finish', the installer will automatically close. You can now proceed with the Site Server installation by running the **autorun.exe** application.



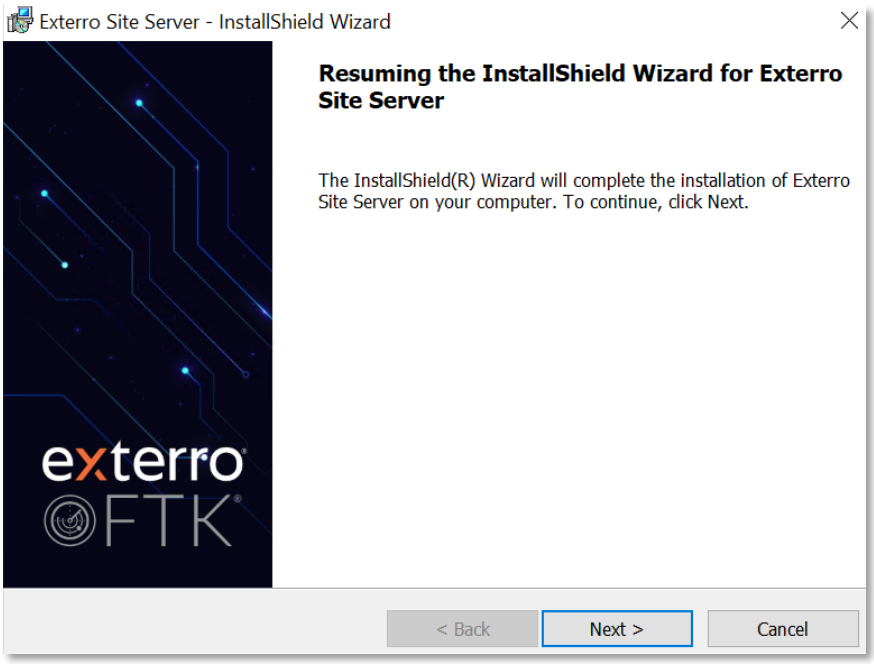
- The Forensic Tools Installer page is displayed.



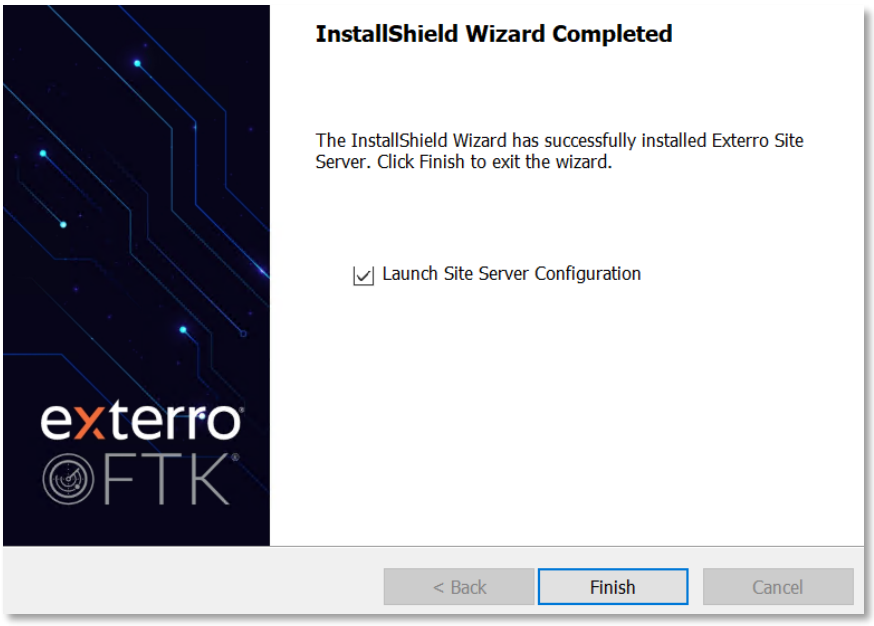
16. Select **Other Products**.
17. Select the **Install Site Server** product.



- The following installation page is displayed.

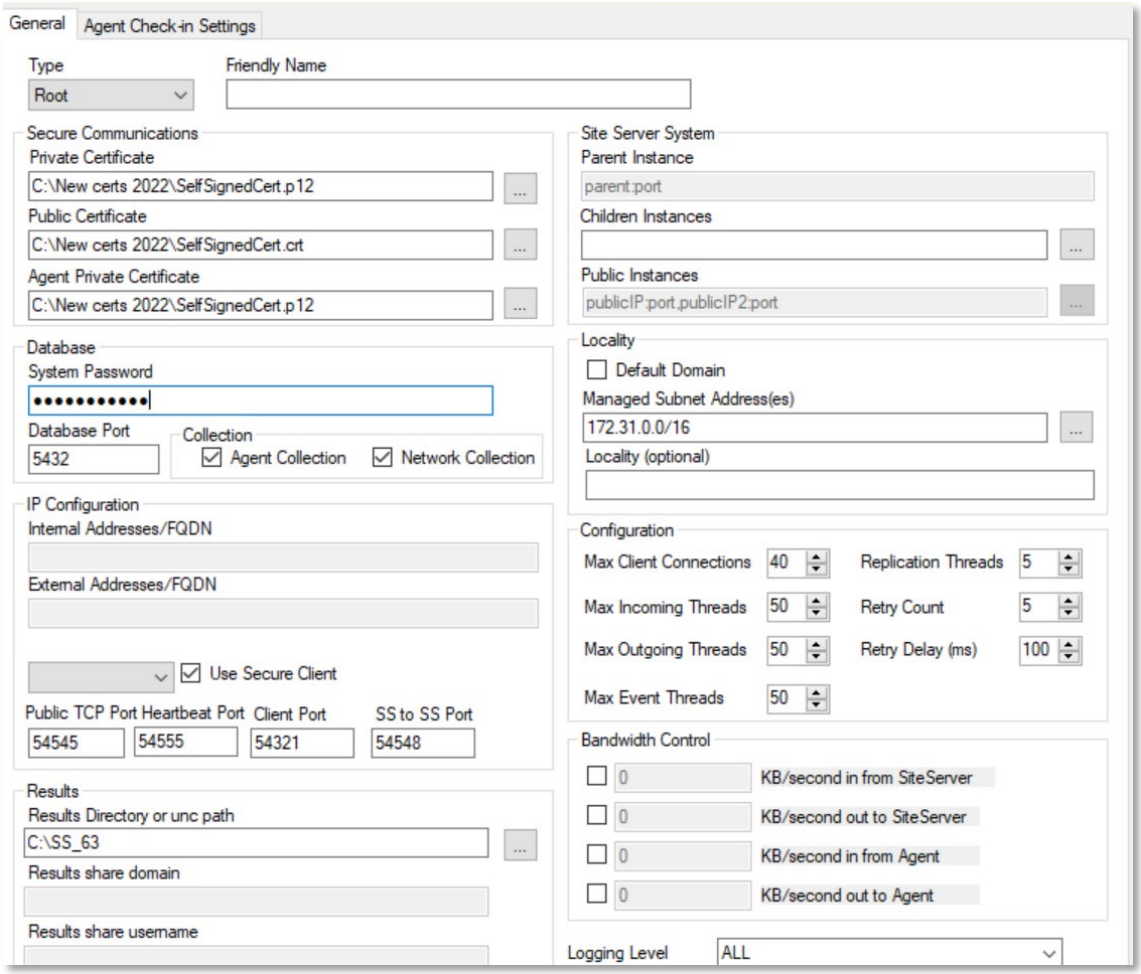


18. Click **Next**.
19. Select the **Launch Site Server Configuration** checkbox.



20. Click **Finish**.

- The 'Site Server Configuration' page is displayed.



Note: All existing configured values will be retained during the upgrade. If necessary, you can modify them according to your requirements.

21. Enter the PostgreSQL **System Password**.
22. Reselect the desired **Results folder** using the file explorer (…).
    - **Alternatively,** add/delete a trailing backslash \ at the end of the path.
23. Once all the required configurations are reviewed and updated, click **Apply**.
    - The service will need to restart, and any ongoing jobs may need to be restarted.
24. Click **OK**.
    - It is recommended to reboot the system once the installation is completed.

1.9.1 Fresh Install on a New Site Server with PostgreSQL 14.17

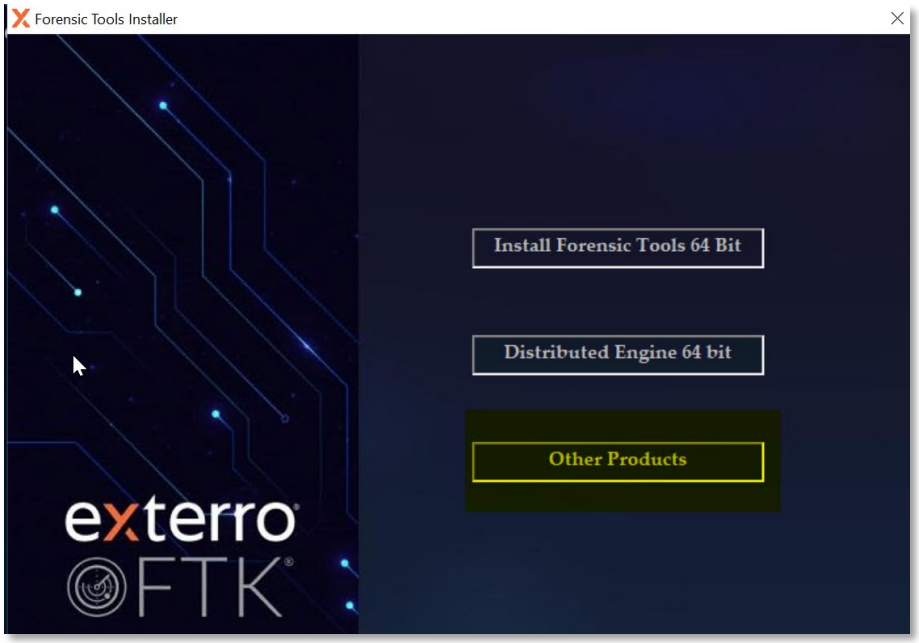
Steps:

1. Download the latest 8.2 Site Server installer from the ***Exterro Product Downloads*** page.

   (or)

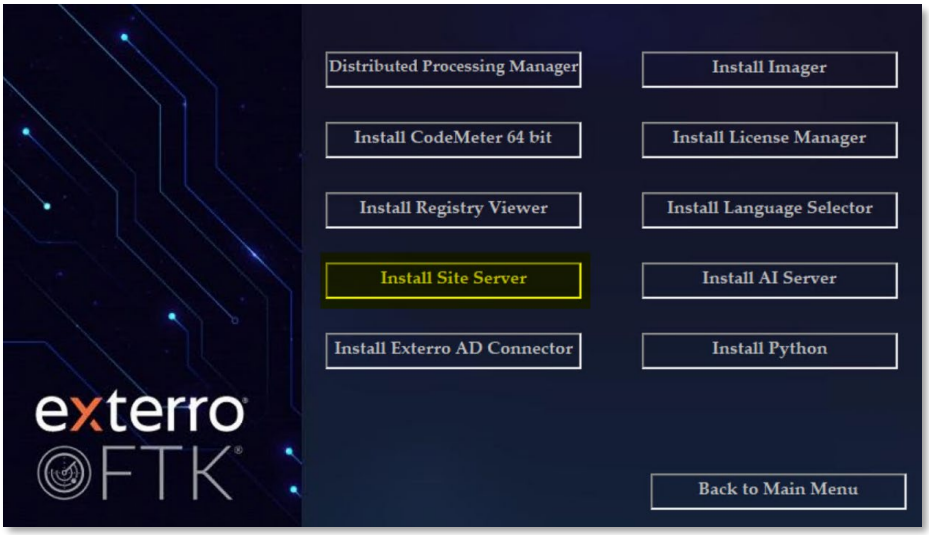
   Download the ISO and run the **Autorun.exe** application.

   - The following Product Installs page is displayed.



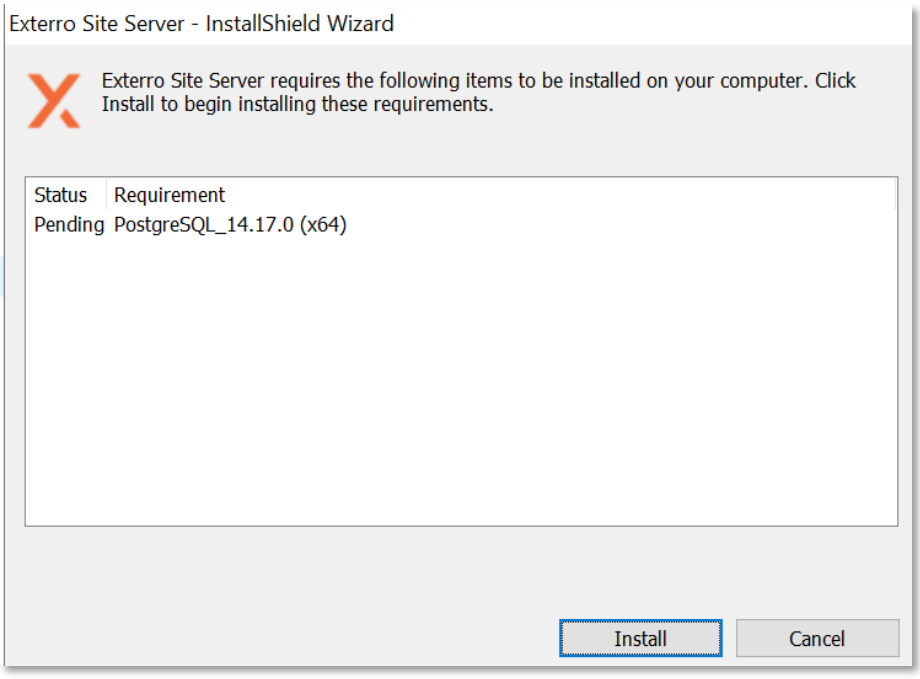
2. Select **Other Products**.

- The following list of product install page is displayed.



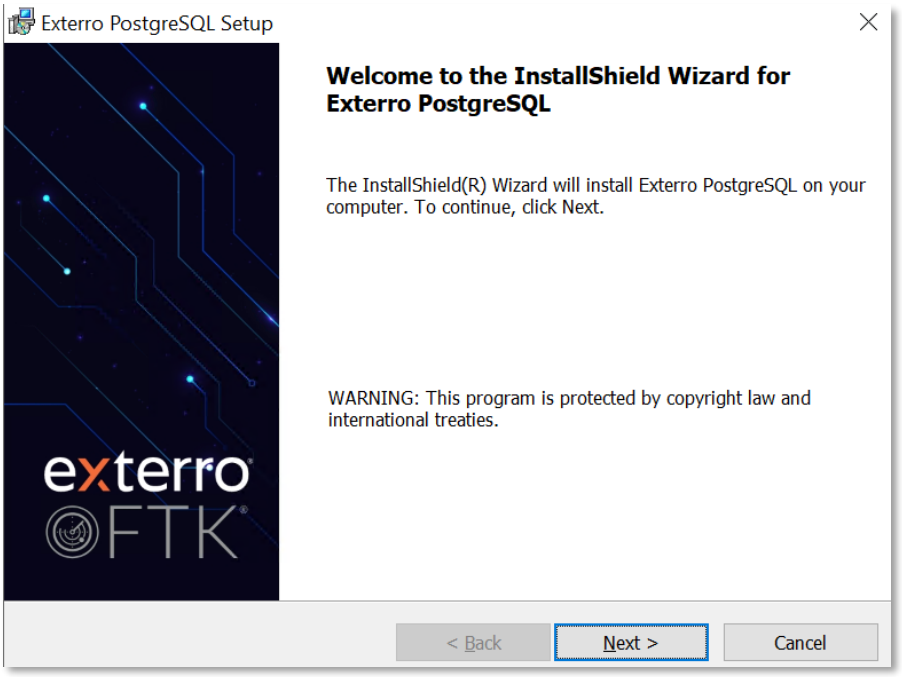
3. Select the **Install Site Server** product.

- The following installer page is displayed.



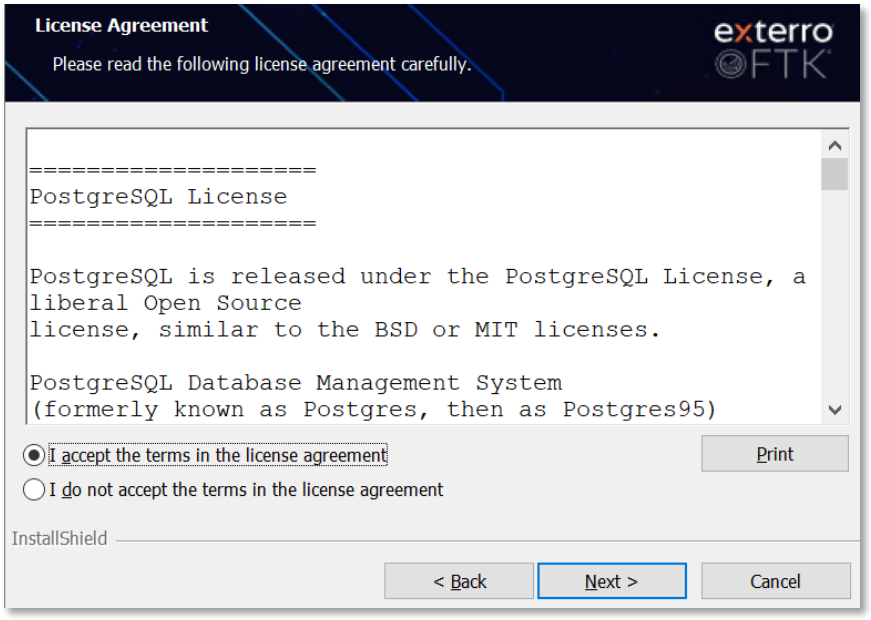
4. Click **Install**.

- The following Welcome Page is displayed.



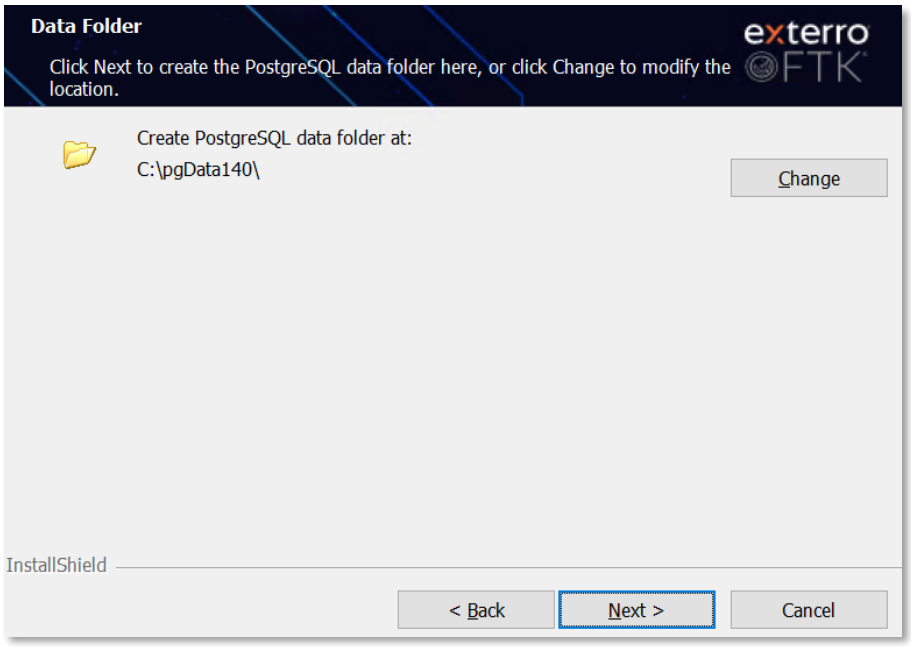
5. Click **Next**.

- The following License Agreement page is displayed.



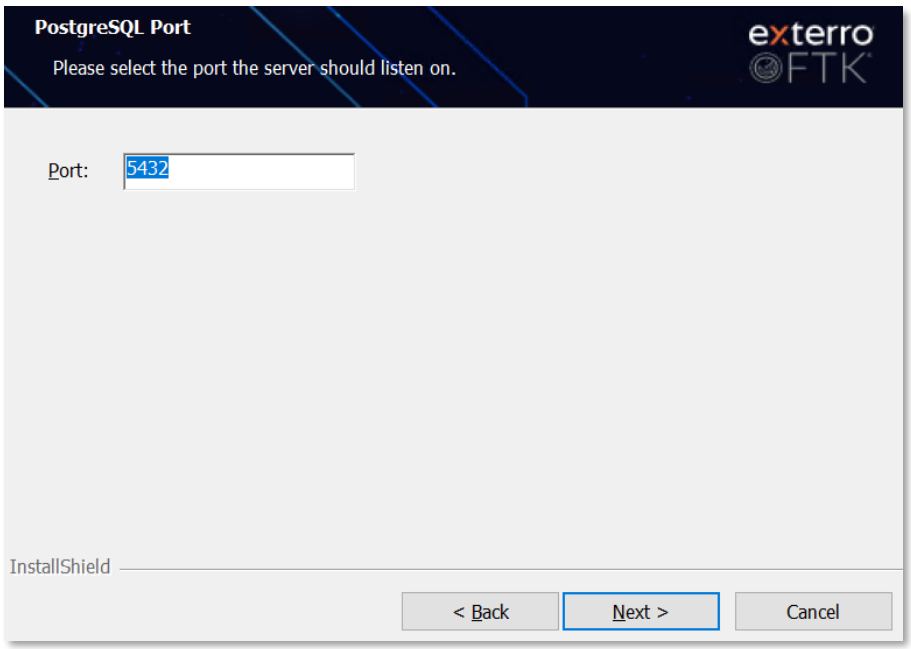
6. Read and accept the terms and click **Next**.

   - The following page is displayed (to select the PostgreSQL Data directory).



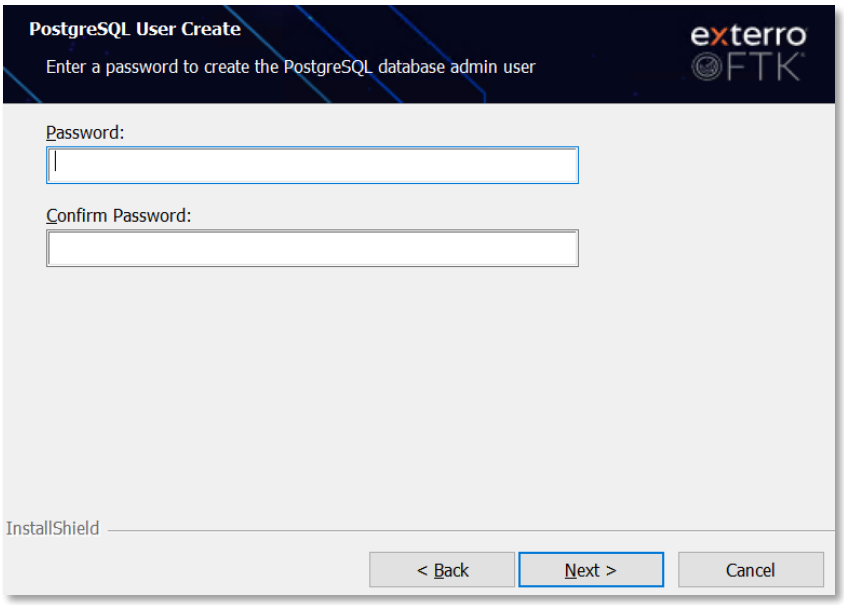
7. Select the PostgreSQL Data directory and click **Next**.

   - The following page is displayed.



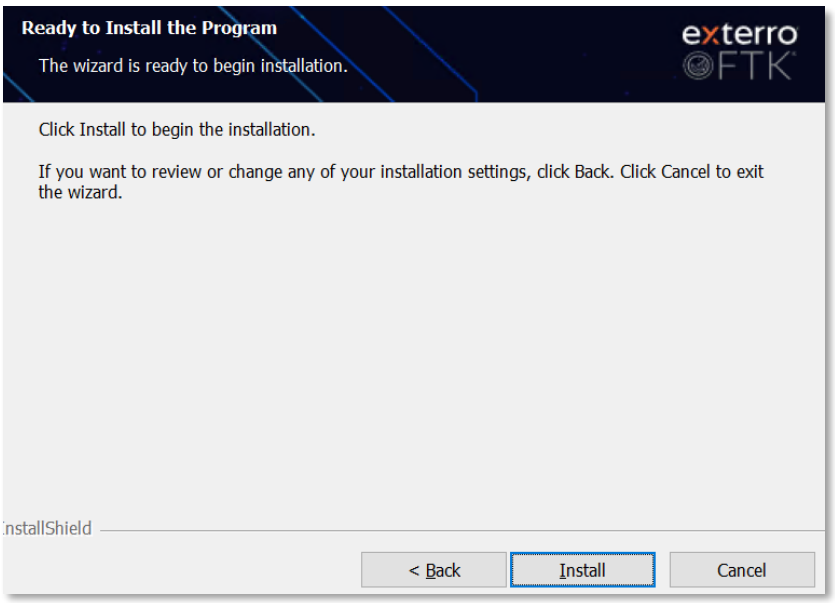
8. Select the Port and click **Next**.

   - The following page is displayed.



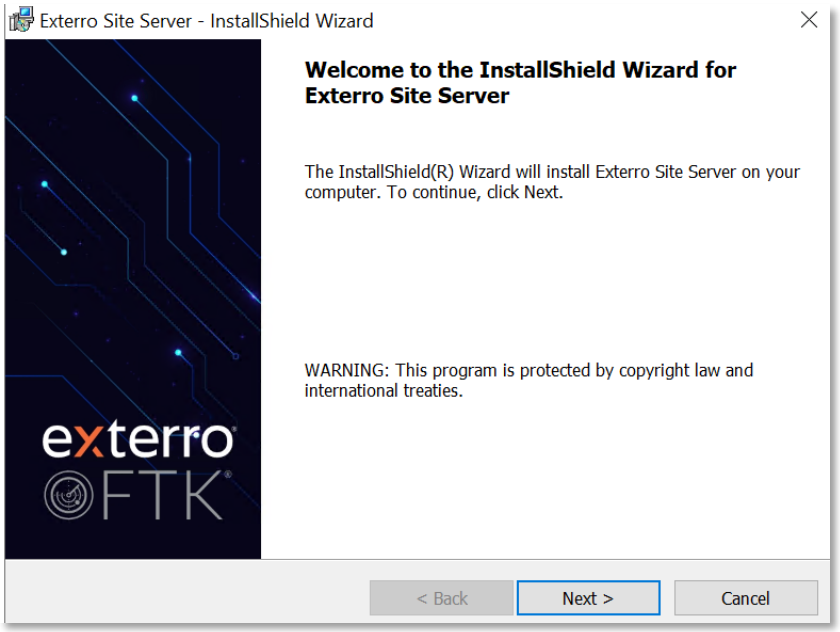
9. Provide the PostgreSQL database Admin **Password** and click **Next**.

   - The following installation page is displayed.

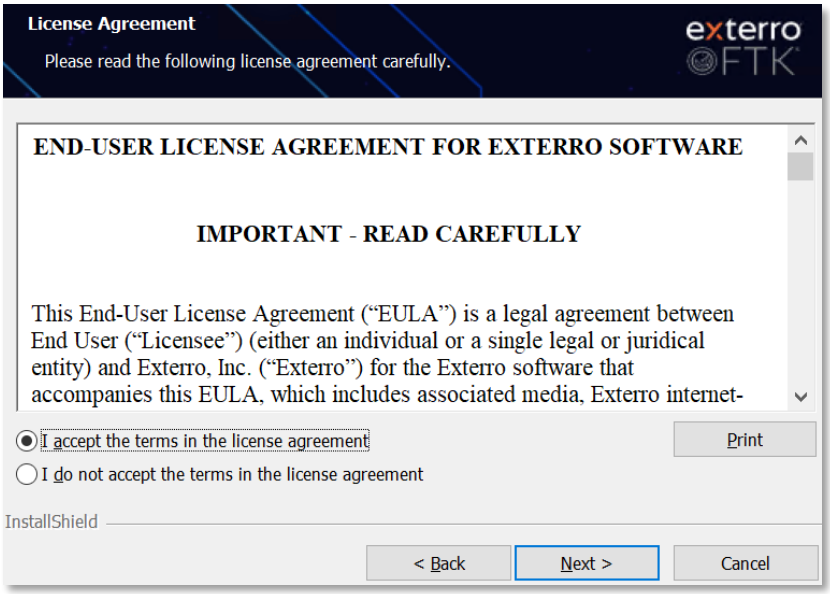


10. Click **Install**.

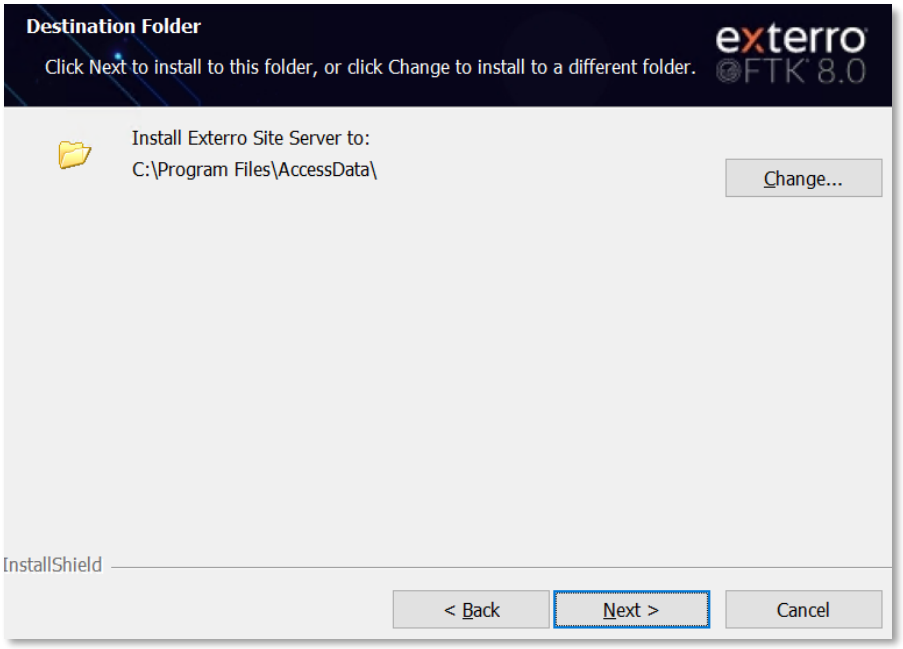
- The following Welcome Page is displayed.



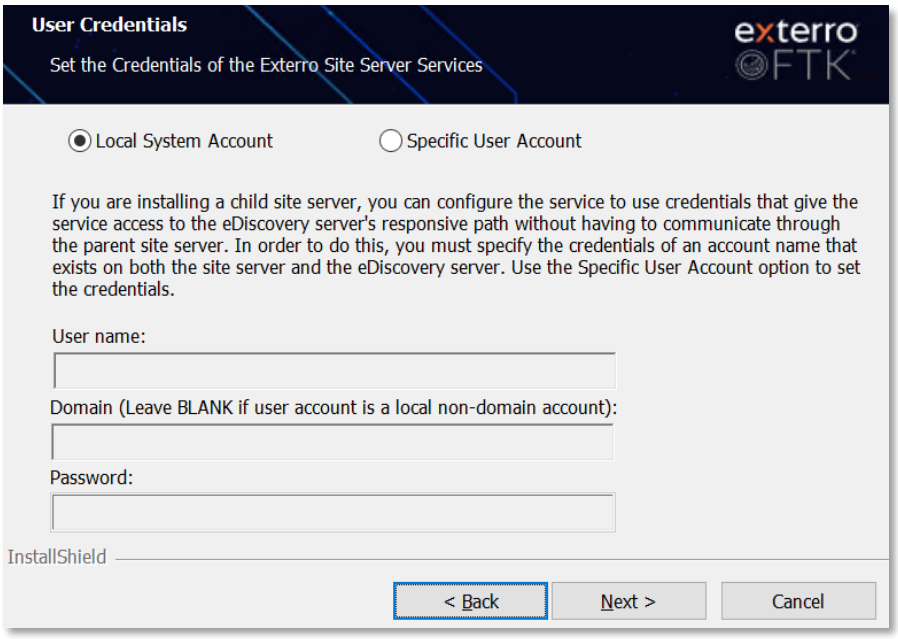
11. Click **Next**.
12. Review and accept the **EULA** and click **Next**.



13. Select the installation directory and click **Next**.



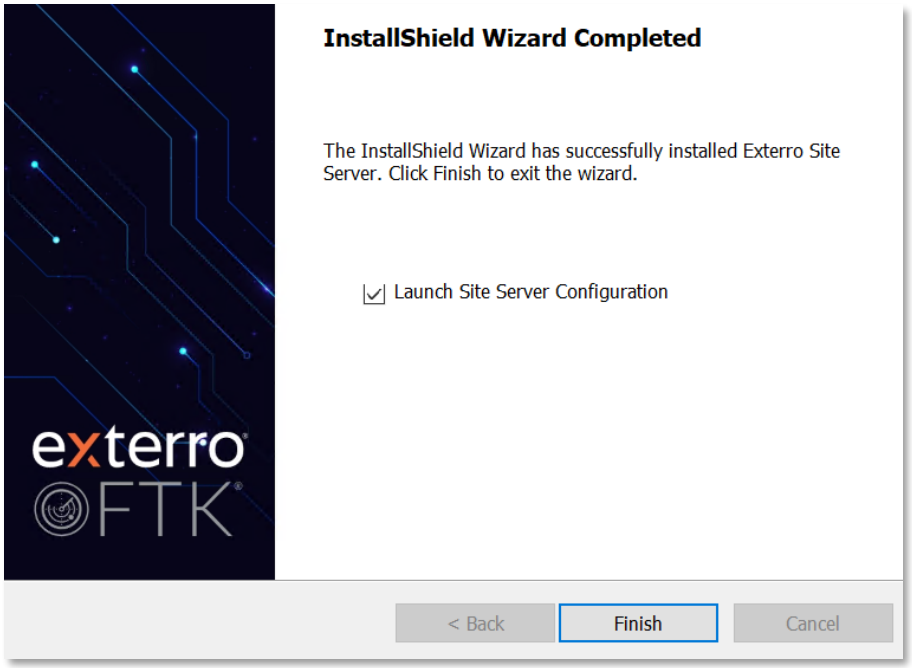
- The following User Credentials page is displayed.



14. At the **User Credentials** dialog, select **Specific User Account** and enter the credentials for an account to run the Exterro service (This account should be a member of the local administrators group, and be a domain-level account in a multi-box environment. The **Local System Account** should only be used if all components, as well as case and evidence storage, will be on one single machine.)

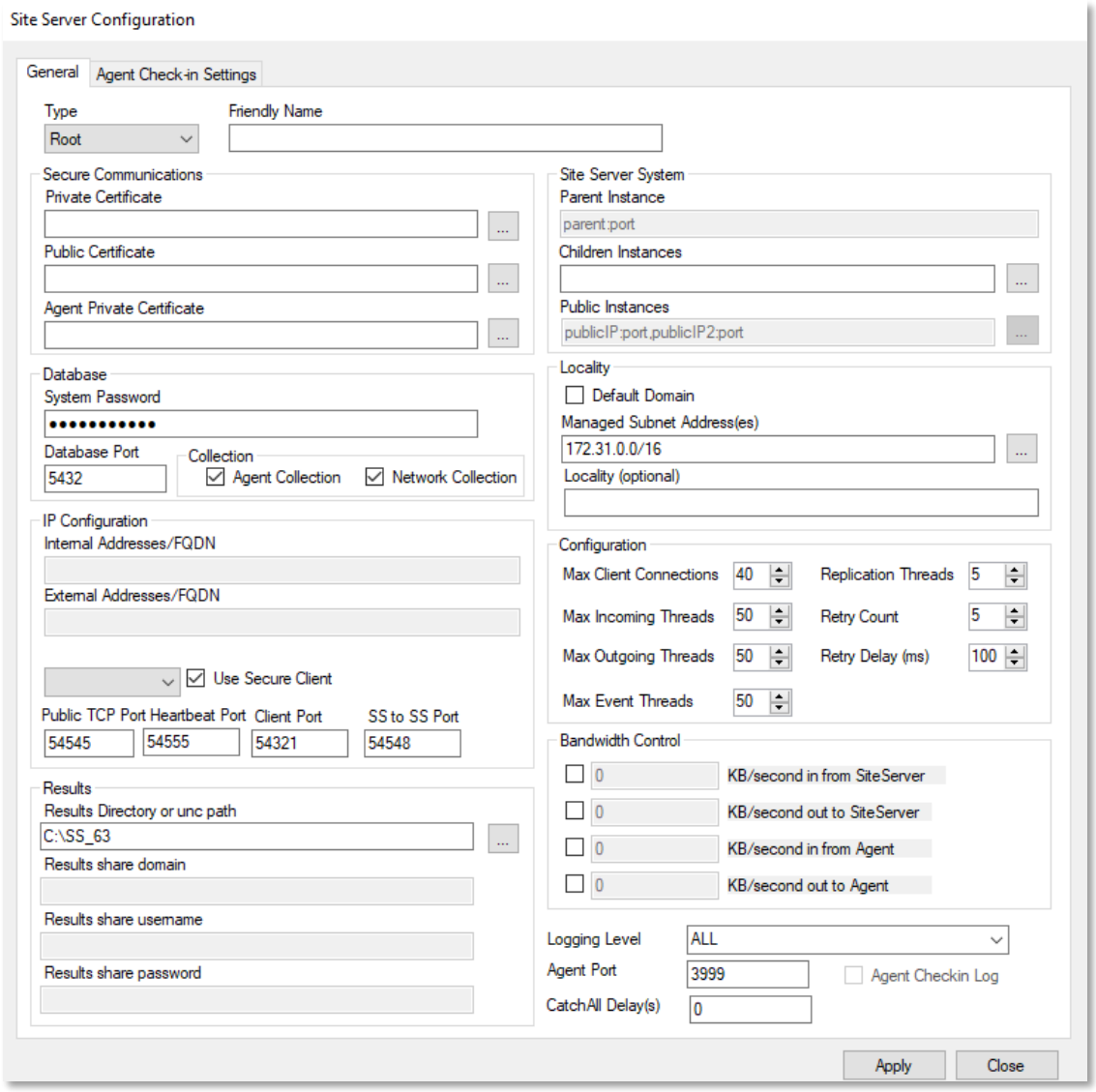
15. Click **Next**.
16. Click **Install**.

    - The following installation page is displayed.



17. Select the 'Launch Site Server Configuration' checkbox and click **Finish**.

- The 'Site Server Configuration' page is displayed.



18. Enter the PostgreSQL **System Password**.

Note: Refer to the KB Article for instructions on configuring the Site Server.

19. Once all the required configurations are made, click **Apply**.
    - The service will need to restart, and any ongoing jobs may need to be restarted.
20. Click **OK**.
    - It is recommended that the system be rebooted once the installation is completed.

1.10 Agent Out of Band

Note: You are recommended to obtain the latest CAB file for the FTK Suite 8.2 SP2 from the Exterro team and place it in the locations below:

Program Files\AD\SiteServer\Agent
Storage\Agent

1.10.1 Agent Installation and Configuration

- **Installation Arguments**:
  - During agent installation, specific arguments are stored in the agent.ini file.
  - The key used to store these installation arguments is InstalledArgs.

1.10.2 Managed Agent Flow

- **Initial Call and Version Check:**
  - The Managed Agent makes a call to the public site server via the API endpoint - PublicAgent/CheckInAgentUpdate.
  - The response from this call contains the current agent version stored in the Site Server's storage path.
- **Version Comparison:**
  - On the Managed Agent side, the version received from the site server is compared to that of the currently installed agent on the client machine.
  - If the installed version matches the public site server version, no action is required.
  - If a newer version is available, the agent will initiate an update process.
- **CAB File:**
  - If the CAB file:
    - **Contains Public Certificate -** The certificate should be updated to the agent
    - **Does not contain the Public Certificate -** The public certificate existing on the agent will be retained

Notes:

- *When an agent has an ongoing job or a job waiting while a version check occurs, the **agent version update happens only on Agent Check-in**.*
- *The **.cab file** is stored in the **site server directory**:*
- *C:\Program Files\AD\SiteServer\Agent*
- *If the updated **.cab file** is present in the **root site server**, it **does not automatically transfer** to all child site servers.*
- *If only one site server has the updated **.cab file**, the **Agent Version does not get updated**.*
- ***All site servers synchronize** with the latest **.cab file** when available.*
- *The .cab file should be signed by Exterro. Otherwise, the updates will not occur automatically.*
- *If you want to change the communication certificates, you should share the certificates along with installation parameters with the Exterro team. Based on this information, the Exterro team will create and share the package with you.*

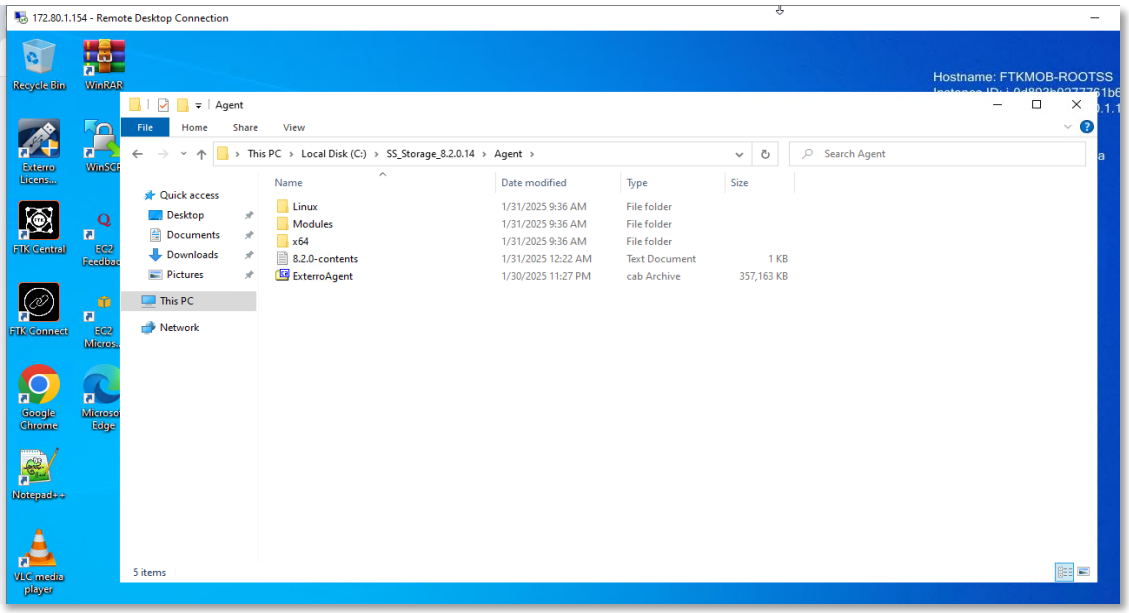
- **Downloading Update:**
  - If an update is needed, the update package (in the form of a .cab file) located in the public site server's storage path is downloaded to a temporary location on the client machine.
- **Backup of Installed Agent:**
  - Once the .cab file is downloaded, the current agent version is backed up in the temporary location before performing the update.
- **Agent Update Process:**
  - After the backup is complete, the .cab file is extracted.
  - If an .msi (Microsoft Installer) file is present within the extracted .cab file, the agent update is performed using the .msi installation package.
  - While updating the Agent using a CAB file, the update will only be made using HTTPS check-in and not TCP check-in.

1.10.3 Error Handling & Edge Cases

- **No Update Available:**
  - If the installed agent version matches the version on the site server, the process terminates without an update.
- **Update Process Failures:**
  - If the .cab file download fails or the .msi installation encounters issues, appropriate error messages are logged, and the agent update process is aborted.
- **Backup Failures:**
  - In case of backup failure, the update is halted to prevent data loss. Logs are generated for troubleshooting.

1.10.4 Log & Monitoring

- **Log Details:**
  - Logs related to the agent's installation, version checks, updates, and backups are stored on the client machine. These logs help troubleshoot and monitor the health of the Managed Agent.
- **Monitoring:**
  - Site administrators can monitor the agent's update status and errors through the Site Server interface.



Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization's internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:

Exterro, Inc.

2175 NW Raleigh St., Suite 110

Portland, OR 97210.

Telephone: 503-501-5100

Toll Free: 1-877-EXTERRO (1-877-398-3776)

Fax: 1-866-408-7310

General E-mail:info@exterro.com

Website: www.exterro.com