exterro®
Data Risk Management

FTK 8.3 MANAGED SITE SERVER OVERVIEW GUIDE

JULY 2026

Table of Contents

About Exterro 3

1 Exterro Managed Site Server 3

1.1 What is Exterro Managed Site Server? 3

1.2 Technological Outline 4

1.2.1 PFX Certificate 4

1.2.2 Default Port Usage 5

1.3 Minimum Hardware Requirements 7

1.4 Benchmark Results (Check-ins) 7

1.4.1 Benchmark (HTTPS Check-in Triggered using Script) 8

1.5 Installation and Configuration Options 9

1.5.1 Configuring the Site Server to Use a PFX Certificate 11

1.6 Installation Script for Off-Network Agents 14

1.6.1 Agent Installation Parameters 15

1.7 Site Server Log Information 16

Contact Exterro 17

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.

- **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	8 Core	16 GB 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	

1.4.1 Benchmark (HTTPS Check-in Triggered using Script)

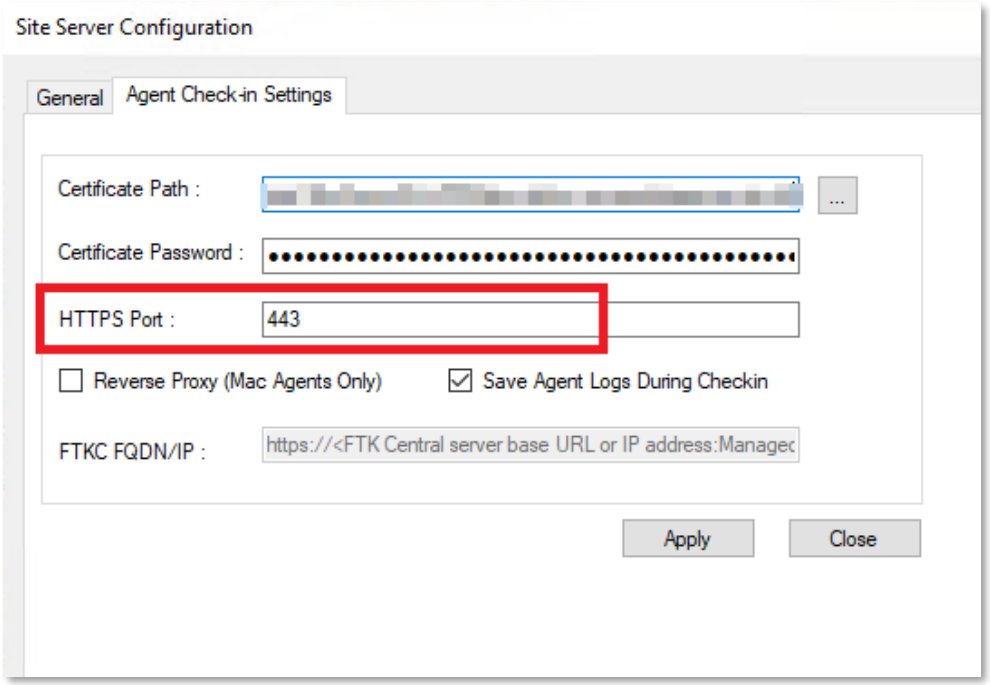
Exterro conducted tests within a controlled environment using the corresponding hardware specifications, we observed 100,000 successful check-ins by Agents to the Managed Site Server triggered via script.

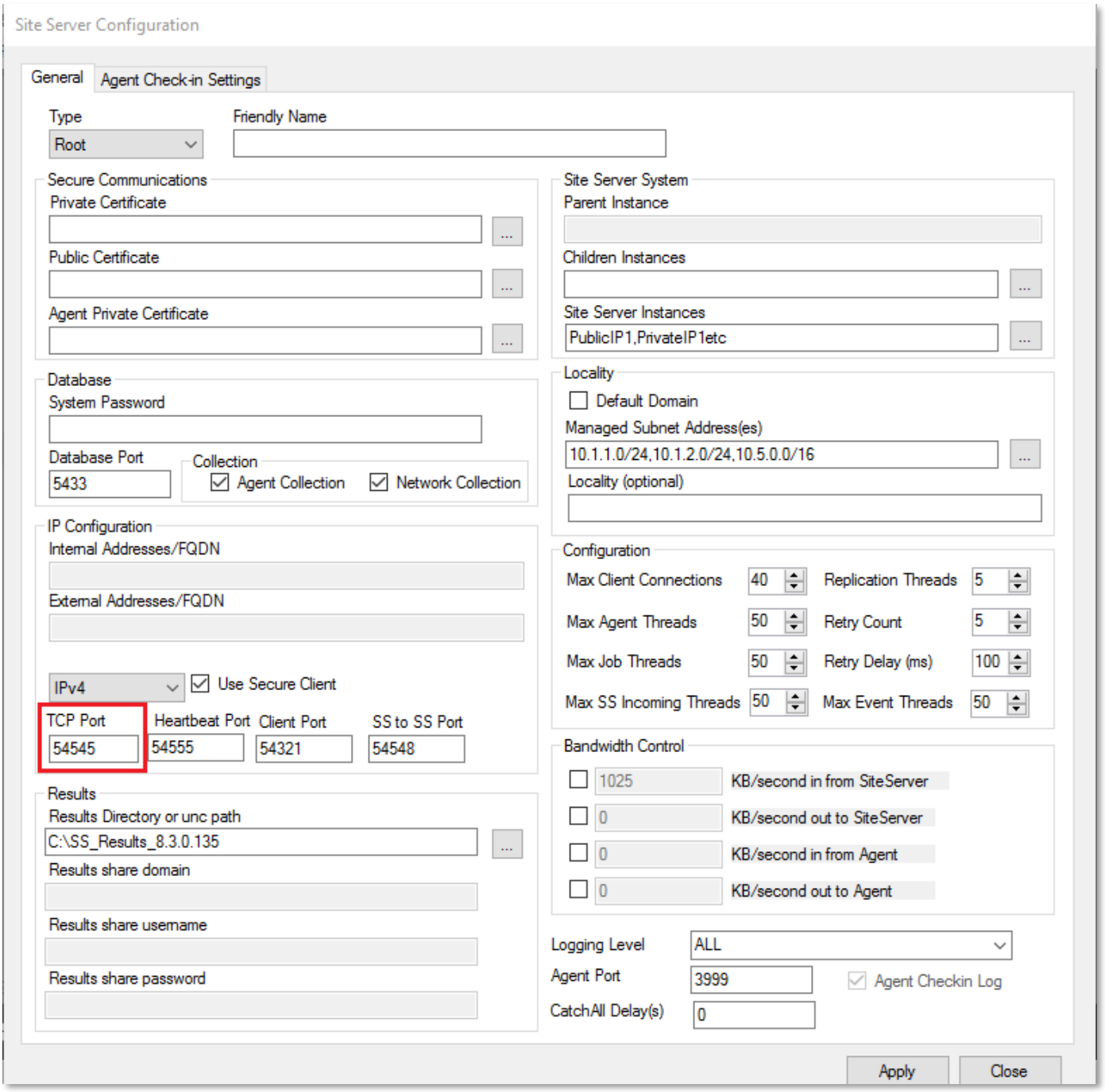
Hardware Utilized for Benchmarking	Agent Count	Time to Complete Last Check-in in the database (in mins)	Average Check-ins per minute
Processor: 8 Core RAM: 16 GB	10.000	1 minute 24 seconds	10,000 to 15,000
	50,000	3 minutes 20 seconds	
	100,000	10 minutes	

1.5 Installation and 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 'Site Server Instances' field.
- 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 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.

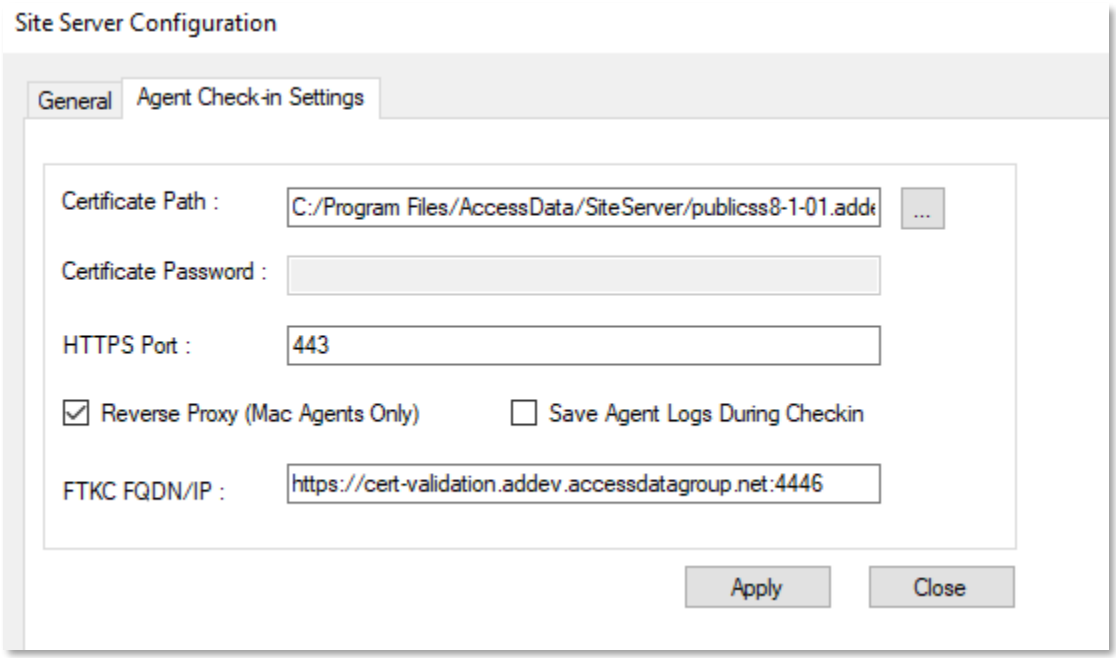
Important Note: The following fields should be configured for the corresponding Agents:

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

Agent Type	Fields to be configured
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.**

Notes:

- The Certificate Password field is greyed out and does not display the configured password. The field remains disabled until the Certificate Path is updated.
- Passwords must be provided in plain text, which will be encrypted automatically when the Site Server service is restarted.

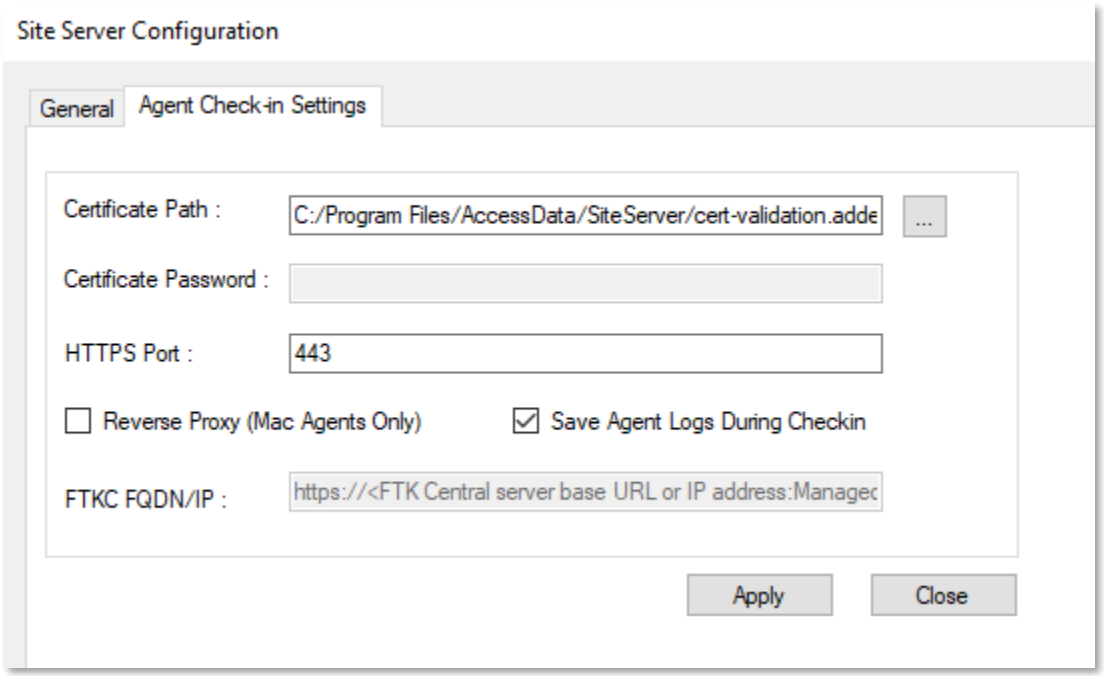
5. The value for **HTTPS Port** is updated as **443** by default. However, you can change it based on your preference.

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 agent API Port>

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



8. Enable the **Save Agent Logs During Checkin** option to automatically upload agent log files to the Site Server during each check-in.

Note: Only the latest 2000 lines are updated during each check-in.

9. Check the **Save Agents Logs During Checkin** to save the agent logs in the below location every time a check-in happens:
   [Result Directory or UNC Path]\AgentLogs\<AgentGUID>
10. 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:

- By default, port 443 is designated for all HTTPS check-ins. To use a different port, you must specify the HTTPSPORT 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.

Tip: To check if an agent can check-in to your site server (for 8.2 SP2 and later versions), execute the below URL:

```
https://<network load balancer or public site server DNS>:<managed site server port number>/publicagent/test
```

The configured site server is reachable for check-ins only if the 'ok' response is displayed.

1.6.1 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.*
SSLIST	”PUB1SS,PUB2SS,DNS1,DNS2,NLB1,NLB2”	-	Yes	Consists of the entire list of Private or Public Site Servers (DNS or Network Load Balancers or IP) without any port numbers .

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 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*** **[Result Directory or UNC Path]\AgentLogs\<AgentGUID>**	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.** The last 2000 lines of Agent logs will be stored in this location every time a check-in happens.

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