exterro®
Data Risk Management

FTK 8.2 SP2

MAC AGENT INSTALLATION 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.

Purpose of the Document

This document provides the step-by-step instructions to guide you through the successful deployment of macOS Agents. These agents are designed to enable seamless data collection functionality within the FTK Web UI.

1 Supported macOS Versions

- Big Sur (macOS 11)
- Monterey (macOS 12)
- Ventura (macOS 13)
- Sonoma (macOS 14)
- Sequoia (macOS 15)

2 Backwards Compatibility

FTK Site Server is enhanced with Backward compatibility, the process of ensuring the older versions (before 8.2 SP2) of Agents (along with the latest) will work without any issues with the latest version of Site Server. The Backward Compatibility process is supported for the 8.1 SP3 (Agent version - 1.0.502) and 8.2 SP1 (Agent version - 1.0.402) versions.

3 Prerequisites

The prerequisites outlined below are specific to macOS Agents only.

- Port Requirements
- Certificate Requirements
- Site Server Installation
- Temporary Location for Agent Data

There are two different types of deployment methods used for macOS agent which are provided below:

- **Deployment Type 1** - For macOS Agents that operate in an isolated network environment and lack direct network visibility and connectivity to the application server.
- **Deployment Type 2** - For macOS Agents that **do not** operate in an isolated environment and has direct network visibility and connectivity to the application server.

3.1 Deployment Type 1

Deployment Type 1 is designed for macOS Agents located outside the organization's internal network, such as remote employee devices or systems in field locations. These agents rely on a reverse proxy (Integrated with the Site Server Managed API) to establish secure and reliable communication with the FTK Web Service over the internet.

Key Features:

- **Flexibility and Reach:** Agents enable FTK to manage endpoints regardless of physical location, supporting remote and distributed workforces.
- **Reverse Proxy Support:** To facilitate communication, a reverse proxy acts as an intermediary, providing a secure path for check-ins and data transfer from devices to the central server.
- **Secure External Connectivity:** With properly configured certificates and HTTPS, these agents ensure encrypted data exchange, maintaining high security standards.
- **Dynamic Configuration:** Designed to adapt to varied and unpredictable network conditions common in remote environments.
- **Use Case:** Essential for organizations with a hybrid workforce or devices operating in remote, external, or untrusted networks.

Considerations:

- Configuration of the reverse proxy is necessary.
- Performance may depend on the quality of the endpoint’s internet connection.
- Live Preview is not supported for macOS Agents (Deployment Type 1).

3.2 Deployment Type 2

Deployment Type 2 is designed to operate within the same local or enterprise network as the FTK Web Service. These agents directly communicate with the FTK Web Service without the need for additional intermediaries (Reverse Proxy via Site Server), making their deployment straightforward and highly efficient for centralized environments.

Key Features:

- **Direct Communication:** On-network agents establish a seamless and direct connection to the FTK Web Service over internal network protocols.
- **High Performance:** They typically experience minimal latency, ensuring faster data transfers and real-time operations like Live Previews and Data Collection.
- **Simplicity of Configuration:** With no need for complex routing or proxy setups, deploying on-network agents is quick and easy.
- **Security Within Controlled Environment:** Communication occurs within a trusted internal network, leveraging existing security policies and firewalls for protection.
- **Use Case:** Ideal for organizations where endpoints and servers reside on the same internal infrastructure, such as within a corporate office or data center.
- **Live Preview:** Allows Live Preview of MacOS Agents within the application.

Considerations:

- Limited to environments where agents can maintain a consistent connection to the internal network.
- Not suitable for endpoints operating outside the corporate infrastructure on remote, external, or untrusted networks.

3.2.1 Ports

The following ports ensure secure and controlled connectivity between macOS Agents and the FTK application. Users must ensure their firewall and network settings allow outbound traffic to these ports to establish a successful connection.

Functionality	Port	Deployment Type
Agent Check-In	443 Can be customized when configuring the Site Server.	Deployment Type 1
Agent Jobs	4446 Can be customized when configuring the FTK Web Service.	Deployment Type 1 and Deployment Type 2
Agent Live Preview	3999 Cannot be customized.	Deployment Type 2

3.2.2 Certificates

Purpose

The FTK Web Service certificate is essential for establishing secure, encrypted communication between the application server and macOS Agents during collections and Agent check-ins. The certificate is presented to macOS agents configured to communicate with the FTK Web Service directly (Deployment Type 2) as well as any macOS Agents communicating through the Reverse Proxy - Site Server (Deployment Type 1).

A default certificate is provided, however if a custom certificate is required, ensure the following is reviewed:

Configuration File Location:

The certificate configuration parameters are found in ADG.WeblabSelfHost.exe.config. This file is found in the FTK application installation directory.

Location: *C:\Program Files\AccessData\Forensic Tools\<Version>\bin\ADG.WeblabSelfHost.exe.config*

Configuration Properties:

Private Certificate	
Configuration Properties	**Description**
certificateFileName	Specifies the full path to the PFX certificate file used by the FTK Web Service.
certificatePassword	The password relating to the certificate provided for certificateFileName. This password will be automatically encrypted after restarting the FTK Web Service.
certificateThumbprint	An optional configuration. Instead of specifying a certificate file, you can reference a certificate from the system store using its unique thumbprint.
Certificate Properties	
• A PFX certificate must be configured to enable secure HTTPS connections. • Common Name (CN): Ensure this matches the FQDN or alias of the FTK Web Service host. • Certificate Authority (CA): Ensure it is signed by a trusted CA to ensure validity. • Must be trusted by all FTK Web UI clients (Deployment Type 2).	
Validation Settings	
• validateCertificate configuration key can be found in the agentinstall.config during macOS Agent installations. • This is set to false by default. If set to true, a custom certificate must be provided.	

3.2.3 macOS Agent Validation Certificates

Purpose:

These certificates enable secure communication between the FTK Web Service and macOS agents. The FTK Web Service presents the private certificate (agentCertificateFileName) to macOS Agents for authentication. A public certificate (clientCertificatePath), derived from this (agentCertificateFileName) certificate, must be distributed to macOS Agents for authentication.

The macOS agent hosts its local API over HTTPS, ensuring only the FTK Web Service and it's related UI are the only clients that can access the Agent API.

A default certificate is provided, however if a custom certificate is required, ensure the following is reviewed:

3.2.3.1 Private Certificate

Configuration File Location:

The certificate configuration parameters are found in ADG.WeblabSelfHost.exe.config. This file is found in the FTK application installation directory.

Location: *C:\Program Files\AccessData\Forensic Tools\<Version>\bin\ADG.WeblabSelfHost.exe.config*

Configuration Properties:

Private Certificate	
Configuration Properties	**Description**
agentCertificateFileName	Specifies the full path to the PFX certificate file used by the FTK Web Service.
agentCertificatePassword	The password relating to the certificate provided for agentCertificateFileName. This password will be automatically encrypted after restarting the FTK Web Service.
agentCertificateThumbprint	An optional configuration. Instead of specifying a certificate file, you can reference a certificate from the system store using its unique thumbprint.
Certificate Properties	

- A PFX certificate must be configured to enable secure HTTPS connections.
- Common Name (CN): Ensure this matches the FQDN of the FTK Web Service host.
- A public certificate should be derived from this PFX in .CER (DER) format, and explicitly mentioned in the **agentinstall.config** > clientCertificatePath during macOS Agent installation in addition to setting the **validateCertificate** configuration to true.

3.2.3.2 Public Certificate

Configuration File Location

The certificate configuration parameters are found in the agentinstall.config. This file is located in the root directory of the unzipped agent installer packages and should be copied along with the agent installer during installation.

Location: *C:\Program Files\AccessData\Forensic Tools\<version>\bin\Agent\MAC*

Configuration Properties:

Private Certificate	
Configuration Properties	**Description**
clientCertificatePath	Specifies the full path to the public certificate used by the macOS Agent.
Certificate Properties	

- A CER certificate must be configured to enable secure HTTPS connections.
- Common Name (CN): Ensure this matches the FQDN of the agent.

Certificate File Placement:

During installation the public key file (.cer) is copied to the following macOS Agent location automatically:

- **Default Location:** /Library/ExterroEnterpriseMacAgent/<Agent Version>

The macOS Agent will check both locations for a certificate, if either is empty, it will check the other before proceeding.

3.2.4 Site Server Managed API Certificate (Deployment Type 1)

Purpose:

Site Servers act as a reverse proxy for agent check-ins using the Managed API. The PFX certificate secures the HTTPS connection between the macOS Agent and the Site Server. The FTK Site Server presents this private certificate to macOS Agents for authentication. macOS Agents will validate the presence of a CA-signed certificate during Check-Ins.

Private Certificate	
Configuration Properties within Site Server UI	Description
Certificate Path	Specifies the full path to the PFX certificate file used by the Site Server Managed API.
Certificate Password	The password relating to the certificate provided in the Certificate Path. This password will be automatically encrypted after restarting the Site Server.
HTTPS Port	The port which will be used by the Site Server Managed API to listen on for any macOS Agent communication. By default this port is 443.
Reverse Proxy (Mac Agents Only)	This option will enable/disable the reverse proxy for agents to communicate to. Exterro advises Deployment Type 1 to keep this option selected.
FTKC FQDN/IP	The FTK Web Service URL followed by the MangedAgentApiPort used for macOS Agents. This field is activated upon checking the Reverse Proxy (Mac Agents Only) option. *<FTK Central application URL>:<managed API Port>*
Certificate Properties	

- A **PFX certificate** must be configured to enable secure HTTPS connections.
- **Common Name (CN):** Ensure this matches the FQDN of the Site Server host.
- **Certificate Authority (CA):** Ensure it is signed by a trusted CA to ensure validity.
- This certificate must be trusted by all macOS Agents (Deployment Type 1).

Validation Settings

- validateCertificate configuration key can be found in the agentinstall.config during macOS Agent installations.
- This is set to false by default. If set to true, this certificate must be trusted by the macOS Agent.

Configuration Location

The certificate parameters should be configured in the **Agent Check-In Settings** tab within the Site Server Configuration pop-up. Refer to the Site Server Configuration section.

3.2.5 Summary of Certificates

Certificate	Type	Purpose	Configuration Location	Server/Client
FTK Web Service Certificate - certificateFileName	PFX - PKCS#12	Secures communication between the server, clients accessing the FTK Web UI, macOS agents connecting to the service, and Site Servers acting as Reverse Proxies for macOS Agent collections.	ADG.WeblabSelfHost.exe.config file on the FTK Web Service host Public certificate (.CER - DER) should be derived from this PFX and added to all macOS Agent Keychains if a reverse proxy is not in use and validateCertificate is set to true	Server
Agent Validation Certificate - agentCertificateFileName	PFX - PKCS#12	Authenticates and secures communication between the FTK Web Service and macOS Agents.	ADG.WeblabSelfHost.exe.config file on the FTK Web Service host	Server
Agent Validation Certificate - ClientCertificatePath	CER - X.509 DER		agentinstall.config file on macOS Agents	Client
Site Server Managed API Certificate (Deployment Type 1)	PFX - PKCS#12	Secures HTTPS communication between macOS Agents and the Site Servers Managed API.	Agent Check-In configuration tab within the Site Server Config UI. Public certificate (.CER - DER) should be derived from this PFX and added to all macOS Agent Keychains if a reverse proxy is in use and validateCertificate is set to true.	Server

3.3 Host Entries (Deployment Type 2 Only)

For Deployment Type 2, the below provided steps should be performed to establish a connection between Mac Agent and FTK Central application:

In Mac agent:

1. Open the Terminal
2. Execute the below command

```
sudo nano/etc/hosts
```

3. Provide the Agent IP, in case of off network pass public IP and URL

```
<FTKC application IP address><space><URL>
```

In FTK Central server:

1. Navigate to the below location:

```
C:\Windows\System32\drivers\etc\hosts
```

2.Provide the mac agent IP address and URL in the below format:

```
<MAC IP address><Tab><hostname of the MAC machine>
```

3.4 macOS Agent Location

The following location stores macOS Agent installers for both ARM/Intel processors:

```
C:\Program Files\AccessData\Forensic Tools\<Version>\bin\Agent\MAC
```

- **For Mac with an Apple Silicon processor** - ARM version of the agent installer
    - **Installer name:** ExterroEnterpriseMacAgent-installer-arm64-(Agent_version)
- **For Mac with an Intel processor** - X64 version of the agent installer
    - **Installer name:** ExterroEnterpriseMacAgent-installer-x64-(Agent_version)

3.5 Temporary Location

The following path is required on the server hosting the FTK Web Service. This folder will serve as the upload location for any data transferred by a given macOS Agent. This is the default path required for macOS Agent collections; **however, this can be customized based on an organization's requirements.**

```
C:\temp\managed_agent_uploads
```

- This folder should be accessible by the Service Account used during installation of FTK and its related components.
    - The Service Account should have full read/write permissions available.

3.6 Site Server (Deployment Type 1 Only)

3.6.1 Site Server

To enable communication between macOS Agents and the FTK Web Service, a Site Server must be deployed. This server acts as an intermediary, ensuring that direct communication between external agents and the FTK Web Service is avoided.

While this deployment deviates from traditional site server configurations, it leverages the Managed Site Server API specifically for check-ins and reverse proxy functionality. This solution is designed to operate seamlessly with minimal setup required, providing an efficient and secure communication pathway.

The FQDN/IP of the system should be added as the value for the **ServerBaseUris** configuration in the macOS Agent configuration file (agentinstall.config).

Note: The Site Server Managed API will run and start automatically regardless of the Site Server type being used.

3.6.2 Site Server Installation

The following steps should be followed if an environment does not have an existing site server available for use with the macOS Agent:

1. Download the latest Site Server available here.
2. Extract the Site Server ZIP file.
3. Open and run the **Exterro_Site_Server.exe** file as an Administrator.
4. Click **Next** on the Welcome page.
5. Read and **Accept** the License Agreement.
6. Click **Next**.
7. Select the Installation Location and click **Next**.
   Default: *C:\Program Files\AccessData\*
8. Select the **Specific User Account** and enter the **User Credentials** used for installing all FTK Components.
   - The credentials required are typically those of the Service Account used during the installation of FTK and its associated components. This account must be a member of the local administrators' group to ensure proper permissions. Use of the "Local System" account is recommended only if all components, including case and evidence storage, are hosted on a single machine.
9. Click **Next**.
10. Click **Install**.
11. Once the installation has completed, perform the following steps:
    a. Check Open Site Server Config.
    b. Click Finish once the installation is complete.
    c. Follow the steps in the Site Server Configuration section.

4 Configuring FTK Web Service Settings

The following steps should be followed once the prerequisites are completed:

1. Open the Windows Services and stop the Exterro Self Host Service.
2. Open the below provided file in a text editor *(**Example:** Notepad++):*

```
C:\Program Files\AccessData\ForensicTools\8.1\bin\ADG.WeblabSelfHost.exe.config
```

3. Change the value of the certificateFileName setting to the full file path of the PFX file.

Example:

```
<add key="certificateFileName" value="C:\Program Files\AccessData\Certificates\myCertificateui.pfx" />
```

Note: The certificateFileName (.PFX) must be in the same directory as **ADG.WebLabSelfhost.exe** otherwise a full path must be provided.

4. Change the value of the certificatePassword setting to the password entered when creating the PFX certificate.

Example:

```
<add key="certificatePassword" value="myPassword" />
```

Note: The password string should be provided in clear text, it will then be encrypted when the Exterro Self Host Service is restarted.

5. (Optional) Change the value of the **ManagedAgentApiPort** setting to the port for use with Mac agents; the FTK Web Service presents the (certificateFileName) certificate on the specified port.

Component	Inbound Port Required
FTK Web Server	4446

6. (Optional) Change the value of the **agentCertificateFileName** setting to the full file path of the PFX file if a custom certificate is required in a deployment.

Note: A default certificate is provided and configured for both the FTK Web Service and macOS Agent. Should a custom certificate be provided in the agentCertificateFileName configuration; the agentinstall.config > ClientCertificateFileName must have a path to a public certificate explicitly mentioned (derived from the agentCertificateFileName).

Example:

```
<add key="certificateFileName" value="C:\Program Files\AccessData\Certificates\myCertificateui.pfx" />
```

Note: The agentCertificateFileName (.PFX) must be in the same directory as **ADG.WebLabSelfhost.exe** otherwise a full path must be provided.

7. (Optional) Change the value of the **agentCertificatePassword** setting to the password entered when creating the PFX certificate.

Example:

```
<add key="agentCertificatePassword" value="myPassword" />
```

Note: The password string should be provided in clear text, it will then be encrypted when the **Exterro Self Host Service** is restarted.

8. Change the value of the **ManagedAgentUploadFolder** setting to the location where you would like the agent to store temporary upload files during collections.

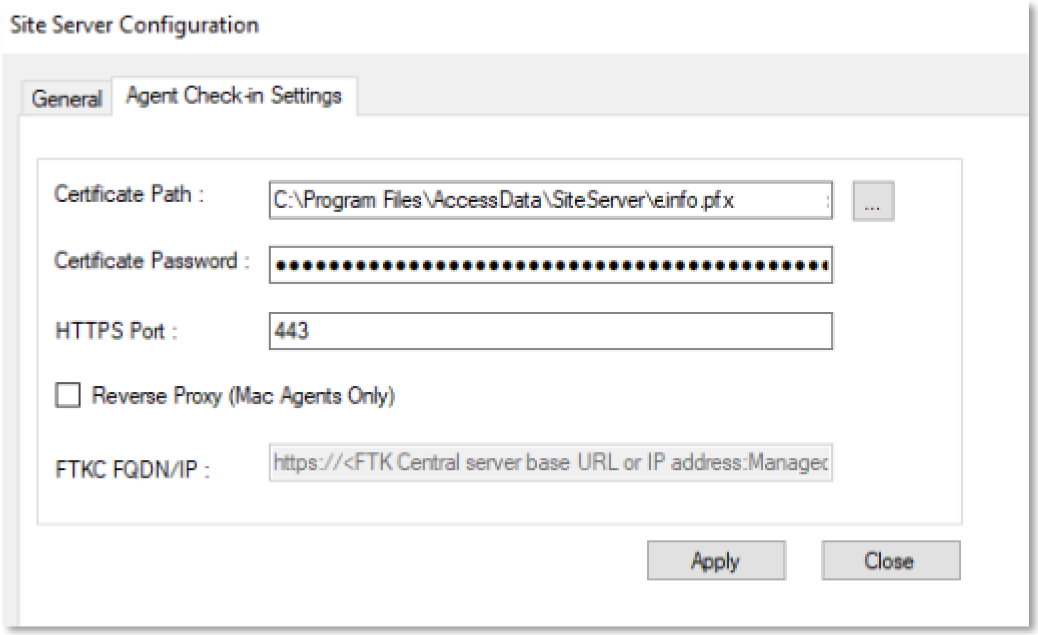
Notes:

- Ensure the directory specified in the **ManagedAgentUploadFolder** setting exists in the temp folder. The upload directory can be a file share or drive path.
- The default value for this configuration is **C:\temp\managed_agent_uploads**.

9. Restart the **Exterro Self Host Service.**

5 Configuring FTK Site Server Settings (Deployment Type 1 Only)

The following steps should be followed once a Site Server has been successfully installed. The following steps will ensure minimal configurations are made to enable macOS Agent connectivity.



Site Server Configuration

Certificate Path : C:\Program Files\AccessData\SiteServer\einfo.pfx

Certificate Password : ●●●

HTTPS Port : 443

□ Reverse Proxy (Mac Agents Only)

FTKC FQDN/IP : https://<FTK Central server base URL or IP address:Managec

1. Open the **Configure Site Server** application as an Administrator.
2. Select the **Agent Check-in Settings** tab.
3. Browser and select a Certificate within the **Certificate Path**. Refer to Site Server (Reverse Proxy - Server) section for more information.
4. Provide the **Certificate Password.**

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

5. Provide the value for HTTPS Port.
   - 443 is the default port used; however, users can customize this as required.
   - This port determines where agents can check-in through.

6. Check the **Reverse Proxy (Mac Agents Only)** option.
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. The Managed Agent API Port relates to the FTK Web Service Configuration key: **ManagedAgentApiPort.** By default, this port is set to 4446.

8. Click **Apply** to save the configurations made in the **Agent Check-in Settings** section.
   - Upon clicking Apply, the Exterro Site Server Managed API will be restarted.

6 Installing the macOS Agent

6.1 Locating the Agent Installer

To locate the agent installer:

1. Navigate to the below location in the FTK Central server:

   C:\Program Files\AccessData\Forensic Tools\<Version>\bin\Agent\MAC

2. Copy any one of the following agent installers into the Mac machine (based on the Mac machine in which the installation should be performed):
   - **For Mac with an Apple Silicon processor** - ARM version of the agent installer
     - **Installer name:** ExterroEnterpriseMacAgent-installer-arm64-(Agent_version)
   - **For Mac with an Intel processor** - X64 version of the agent installer
     - **Installer name:** ExterroEnterpriseMacAgent-installer-x64-(Agent_version)

3. (Optional) Copy the custom public .CER certificate which will be used for the Mac Agent into the Mac machine (based on the Mac machine in which the installation should be performed).

   Note: This public certificate should be derived from the custom .PFX certificate configured in the ADG.weblabselfhost.exe.config > agentCertificateFileName configuration. If these certificates do not match, macOS Agents will have communication issues.

   Warning: During installation ensure both the .CER certificate and agent installer are stored in the same location of the Mac machine.

4. Locate the **ExterroEnterpriseMacAgent.zip.**
5. Move the required ZIP file (x64 or arm64) into the agent.
6. Extract the zip file in the agent to obtain the **agentinstall.config** and **ExterroEnterpriseMacAgent**(x64/arm64.pkg)

6.2 Configuring the Agent Installation Parameters

Note: Ensure the **Exterro Site Server Managed API** service is running in your machine before performing the below steps**.**

To configure the agent installation parameters:

1. Open the **agentinstall.config** in a text editor.
2. Update the **ServerBaseUris** value to the server and port of your server separated with a colon (:).

Syntax for Single Server:

```
<servername_or_public_ip>:<port number>
```

Example:

ServerBaseUris=ftkc.example.com:443

Syntax for Multiple Servers:

```
<servername_or_public_ip>:<port number>,<servername_or_public_ip>:<port number>
```

Example:

ServerBaseUris=ftkc.example.com:443,172.31.15.195:4446

Note: The **<servername_or_public_ip>** should be replaced with the value of:

- The fully qualified domain name (FQDN) or IP of the Site Server (Deployment Type 1)
- The fully qualified domain name (FQDN) or IP of the FTK Web Service (Deployment Type 2)

The **<port number>** should be replaced with the value of:

- HTTPS Port configuration present in the Site Server (Deployment Type 1)
- ManagedAgentApiPort configuration present in the ADG.WeblabSelfHost.exe.config (Deployment Type 2)

3. (Optional) Update the ClientCertificatePath value to the public certificate derived from the PFX configured for the agentCertificateFileName if a custom certificate has been configured.

Agentinstall.config - Common Configurations - Reference

Warning: The configuration file contains many configurations, some of which are not recommended to be edited. The following configurations listed are common configurations.

Configuration	Default Value	Description
ServerPollIntervalSeconds	1800	Time interval for agent check-in. This value should be provided in seconds. ***Example:*** *1800 = 30 Minutes* ***Note:*** *The minimum value recommended to set for this configuration is 300.*
ServerBaseUris	FTKC dns/Server name	Server to which the agent has to be connected with, followed by the port. **Example Deployment Type 1:** exampleserver.com:[HTTPS PORT - Site Server] **Example Deployment Type 2:** exampleserver.com:[ManagedAgentApiPort - FTK Web Service] ***Note:*** *You can add multiple URLs (belonging to the same server) separated with commas (,).* **Example:** ServerBaseUris=ftkc.example.com:443,172.31.15.195:4446

Configuration	Default Value	Description
		In this case, the first address is publicly accessible, and the IP address is internal only. This allows users to use an agent in hybrid environments, where they are roaming across public/private networks.
validateCertificate	false	Set to false by default. The certificate presented by the FTK Web Service (Deployment Type 2) or Site Server (Deployment Type 1) will not be validated by the macOS Agent. If validateCertificate is set to true, the agent would expect a trusted certificate to be presented to the macOS Agent during collections and check-ins.
ClientCertificatePath	-	Client certificate path is the public certificate used to initiate trust with the FTK Web Service, allowing Live Preview. A certificate should be explicitly mentioned if a custom certificate has been provided for the agentCertificateFileName configuration in the ADG.weblabselfhost.exe.config file.
CollectionFailedFileCount	0	The maximum number of failed files allowed during the collection process. If the number of files exceeds this value, the collection will fail.

Note: The configurations above can be accessed and updated after the installation from the following appsettings.json file in the below location:

```
/Library/ExterroEnterprise/(agent version)/appsettings.json
```

After making the changes/updates to the file, the Agent should be restarted by executing the below command in the terminal:

```
sudo adagent restart
```

6.3 Installing the agent

Prerequisites:

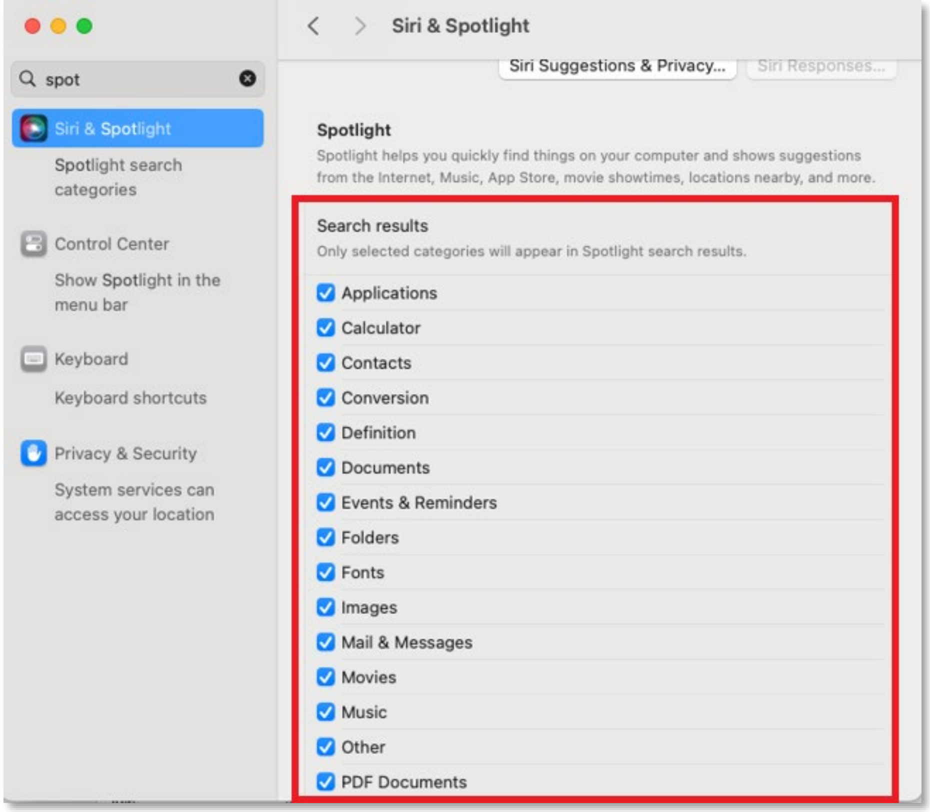
Spotlight Indexing must be enabled to perform Searching/Filtered Collections on MacOS Agents. Failure to enable Spotlight indexing will result in 0 search result hits.

***Note:** The Spotlight indexing is enabled by default. However, you are recommended to check and ensure if the option is enabled.*

You can follow the below steps to enable Spotlight Indexing if it is disabled:

To enable spotlight indexing:

1. Navigate to the System Settings in your machine.
2. Search for ‘Spotlight’.
3. Select all the Spotlight categories displayed in the right pane.



spot
Siri & Spotlight
Spotlight search categories
Control Center
Show Spotlight in the menu bar
Keyboard
Keyboard shortcuts
Privacy & Security
System services can access your location
Siri & Spotlight
Siri Suggestions & Privacy...
Siri Responses...

Spotlight

Spotlight helps you quickly find things on your computer and shows suggestions from the Internet, Music, App Store, movie showtimes, locations nearby, and more.

Search results

Only selected categories will appear in Spotlight search results.

☑ Applications
☑ Calculator
☑ Contacts
☑ Conversion
☑ Definition
☑ Documents
☑ Events & Reminders
☑ Folders
☑ Fonts
☑ Images
☑ Mail & Messages
☑ Movies
☑ Music
☑ Other
☑ PDF Documents

To install the agent:

Warnings:

- During installation ensure both the .CER certificate and agent installer are present in the same location of the Mac machine if using custom certificates.
- If you want to use custom certificates instead of the default ones, you should change the value of ‘validateCertificate property’ to ‘True’ in the agentinstall.config file.

1. Double click on the package installer file to install the agent.

Installer file name:

ExterroEnterpriseMacAgent-installer-arm64-(Agent_version)/ExterroEnterpriseMacAgent-installer-x64-(Agent_version)

Note: During the installation, you will be prompted multiple times (may vary on differing macOS version) to allow permission intended to perform the following actions:

- To access the agentinstall.config file
- To access the client certificate file
- To move the Mac agent package to the trash

You are recommended to click on **Allow** for all prompts, they are mandatory for the installation process.

6.4 Ensuring Full Disk Access for the agent

To ensure Full Disk access for the agent:

1. Navigate to the System Preferences > Privacy and Security in the Mac.
2. Select Full Disk Access from the list of settings.
3. Ensure that the following options have been granted with the full disk access:

Application	Purpose
/Library/ExterroEnterpriseMacAgent>/ADG.ManagedAgentSvc	Required for full disk collections. **Note:** *This application's permissions* should be enabled *upon upgrading the Mac Agent version for the FTK 8.2 SP1 and lower versions.*

7 macOS Agent Log Locations

System	Logs Location
Agent	~/Library/ExterroEnterpriseMacAgent/Logs
FTK Web Server	%PUBLIC%\Documents\AccessData\AccessDataLogs\adgselfhost.txt
Site Server (Site Server Managed API)	C:\Users\Public\Documents\AccessData\AccessDataLogs\SiteServerManagedHostLog.txt
Site Server (Reverse Proxy)	C:\Users\Public\Documents\AccessData\AccessDataLogs\MacReverseProxyHostLog.txt

8 Uninstalling the macOS Agent

Agents can be uninstalled using the command below:

```
sudo bash /Library/ExterroEnterpriseMacAgent/uninstall.sh
```

Note: *While upgrading the Agents of FTK 8.2 SP2 and later versions, the older versions of the Agents will be automatically uninstalled.*

9 Stop/Restart the macOS Agent

Agents can be started/restarted using the command below:

```
sudo adagent restart
```

Agents can be stopped using the command below:

```
sudo adagent stop
```

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

The United States export control laws and regulations, including the Export Administration Regulations of the U.S. Department of Commerce, and other applicable laws and regulations apply to this documentation which prohibits the export or re-export of content, products, services, and technology to certain countries and persons. You agree to comply with all export laws, regulations and restrictions of the United States and any foreign agency or authority and assume sole responsibility for any such unauthorized exportation.

You may not use this documentation if you are a competitor of Exterro, Inc, except with Exterro Inc’s prior written consent. In addition, you may not use the documentation for purposes of evaluating its functionality, or for any other competitive purposes.

If you have any questions, please contact Customer Support by email at support@exterro.com.