Table of Contents

Overview .................................................................................................................................................... 5

1 FTK Central Installation Guide .............................................................................................................. 5
   1.1 Prerequisites ................................................................................................................................ 6
      1.1.1 Service Account ..................................................................................................................... 7
      1.1.2 Firewall .................................................................................................................................. 9
      1.1.3 User Access Control ............................................................................................................. 10
      1.1.4 Anti-Virus Software ............................................................................................................. 11
      1.1.5 Microsoft Distributed Transaction Coordinator (MSDTC) ..................................................... 12
   1.2 Microsoft Windows Optimizations For Performance................................................................. 13
      1.2.1 Windows Power Settings ..................................................................................................... 13
      1.2.2 Microsoft Indexing Service ................................................................................................... 14
   1.3 Microsoft SQL Server 2016/2017/2019 ....................................................................................... 15
      1.3.1 To install Microsoft SQL Server ............................................................................................ 15

2 Standard Installation .......................................................................................................................... 18
   2.1 AccessData Forensic Tools Suite 7.5............................................................................................ 18
      2.1.1 To install FTK Central ........................................................................................................... 18
   2.2 Database: DBConfig .................................................................................................................... 24
      2.2.1 To install Database: DBConfig .............................................................................................. 24
   2.3 AppDB ........................................................................................................................................ 26
      2.3.1 To install AppDB .................................................................................................................. 26

3 Component by Component Installation (Advanced) ........................................................................... 28
   3.1 Licensing..................................................................................................................................... 28
      3.1.1 License Manager ................................................................................................................... 28
      3.1.2 CodeMeter .......................................................................................................................... 29
   3.2 .NET 4.7.2 ................................................................................................................................... 30
      3.2.1 To install .NET 4.7.2 ............................................................................................................. 30
3.3 AccessData Forensic Tools .......................................................................................................... 31
3.3.1 To install AccessData Forensic Tools (App/Web/Collections Server) ........................................... 31
3.4 Database: DBConfig .................................................................................................................... 33
3.4.1 To install Database: DBConfig .............................................................................................. 33
3.5 AppDB ........................................................................................................................................ 35
3.5.1 To install AppDB .................................................................................................................. 35
3.6 AccessData Collab ....................................................................................................................... 37
3.6.1 To install AccessData Collab................................................................................................. 37
3.7 AccessData Evidence Processing Engine(s) .................................................................................. 38
3.7.1 To install AccessData Evidence Processing Engine ........................................................... 38
3.8 AccessData Distributed Processing Manager .............................................................................. 39
3.8.1 To install AccessData Distributed Processing Manager ........................................................ 39
3.9 Site Server(s) ................................................................................................................................ 40
3.9.1 Dependencies and PostgreSQL ............................................................................................ 41
3.9.2 Installing Site Server(s) ........................................................................................................ 42
3.10 Agent(s)...................................................................................................................................... 43
3.10.1 Agent Push Requirements ................................................................................................... 43
3.10.2 Manually Installing Agents (Windows) ................................................................................. 45
3.10.3 Manually Uninstalling Agents (Windows) ............................................................................. 48
3.10.4 Installing Agents with a script (Windows) ............................................................................ 49
3.10.5 Manually Installing Agents (Unix/Linux) ............................................................................... 50
3.10.6 Manually Uninstalling Agents (Unix/Linux) .......................................................................... 52
3.10.7 Manually Stopping Agents (Unix/Linux) ............................................................................... 53
3.11 AI Server ..................................................................................................................................... 54
3.11.1 Installing the AI Server ......................................................................................................... 54
3.12 KFF Server ................................................................................................................................... 55
3.12.1 Installing the KFF Server ...................................................................................................... 55
4 Configuration ..................................................................................................................................... 56
4.1.1 Virtual CodeMeter (VCM) Activation Guide ......................................................................... 56
4.2 Site Server(s) ........................................................................................................................................58
  4.2.1 Configuring the Site Server(s) .......................................................................................................58
4.3 Distributed Processing Manager ........................................................................................................59
  4.3.1 Configuring Distributed Processing Engine(s) ...........................................................................59
  4.3.2 Configuring Distributed Processing Engines: Certificates ..........................................................60
4.4 Agent(s) ..............................................................................................................................................61
  4.4.1 Configuring Execname Values (Windows) ...................................................................................61
  4.4.2 Configuring Servicename Values (Values) ..................................................................................62
  4.4.3 Controlling Consumption of the CPU (Windows): Throttling .....................................................63
  4.4.4 About Using Certificates .............................................................................................................64
  4.4.5 Certificate Verification Checklist ................................................................................................65
4.5 Enable SSL/HTTPS In FTK-Central ....................................................................................................66
  4.5.1 Configuring SSL/HTTPS .............................................................................................................66
4.6 Enable NATO Specific Features/Jobs ....................................................................................................67
  4.6.1 Enabling NATO Jobs ...................................................................................................................67
Overview

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 Legal GRC 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 FTK Central Installation Guide

This document discusses the process of installing a new FTK Central environment. This process attempts to avoid any mid-install reboots when possible.
1.1 Prerequisites

1. Install all current Windows updates.
2. Disable any antivirus/malware scanning software.
3. A physical or virtual dongle with a license.
4. Confirm a supported Windows Server version has been installed and fully patched.
   - Windows Server 2019 (Preferred)
   - Windows Server 2016 (Preferred)
   - Windows 10
5. Confirm a supported Microsoft SQL Server version has been installed.
   - Microsoft SQL 2019 (Preferred)
   - Microsoft SQL 2017 (Preferred)
   - Microsoft SQL 2016
6. Confirm there is a domain-level service account with local Administrator permissions to all backend servers. Additionally, with the inclusion of “sysadmin” permissions in MSSQL.
7. Confirm a HTML5-compatible browser is installed on Web/App/Collection servers as well as any machines being used to access FTK Central.
   - Edge Chromium
   - Google Chrome
   - Mozilla Firefox

Notes:
- FTK Central currently does not have the ability to have a stand-alone Web Server or Work Manager Collections Server. The majority of backend work is now combined into a single App/Web/Collections Server.
- Processing Servers and Site Servers can still be allocated to additional machines as desired.
1.1.1 Service Account

- FTK Central requires the use of a single, preferably dedicated, Windows account to operate properly. This account is the “Service Account”.
- In a multi-server installation environment, a domain-level (Active Directory) Service Account is required.
- AccessData will only support Workgroup authentication in single-server installation environments. In either case, the Service Account must be a local administrator on each of the servers hosting components with both “Logon as Service” and “Interactive Logon” system permissions.
- AccessData recommends configuring the password of the Service Account to never expire and to not allow modification. Changing the password of the Service Account after installation will require the reinstallation of some components.
- The SQL Instance hosting the SQL Database component must have the Service Account added to the Logins and provided sysadmin rights.
1.1.1.1 To create the service account in Active Directory

Steps:

1. Login to the Active Directory Server as an Administrator.
2. Open the Active Directory Users and Computers object.
3. In the Active Directory User and Computers dialog, navigate to the Users object.
4. Right-click Users.
5. At the menu, choose New >User.
6. In the New Object - User dialog, create the FTK Central Service account.
7. For example, name the service account Summation Service with the User logon name of FTKService.
8. Click Next.
9. At the next dialog, make sure that the password has been entered correctly, and that both User cannot change password and Password never expires are checked.
10. Click Next at the next dialog.
11. Click Finish.
12. Log out and log in as the service account.
1.1.2 Firewall

- Disable the Firewall or create custom exception rules.

1.1.2.1 To turn off the Firewall

Steps:

1. Run the following command from the Windows Command Prompt with Admin rights to disable the firewall completely on Microsoft Windows Server 2016 and Microsoft Windows Server 2019:

   ```
   <Drive>:\> netsh advfirewall set allprofiles state off
   ```

   **Note:** Ensure this change is evaluated by your Domain Administrator before execution.
1.1.3 User Access Control

1.1.3.1 To turn off Access Control

Steps:


```
<Drive>:\> %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
```

Note: This modification requires a reboot to take effect.
1.1.4 Anti-Virus Software

AccessData recommends that any anti-virus or anti-malware software on any server hosting components of the FTK Central are configured to disable on-access scanning of the directories or drives containing case files, database files, or temp/log files. Additionally, *should any full scans be scheduled, they should be monitored to ensure they are not interfering with the overall performance of the solution.* For Microsoft SQL Information, see [here](#).
1.1.5 Microsoft Distributed Transaction Coordinator (MSDTC)

AccessData strongly recommends that the following Microsoft Distributed Transaction Coordinator settings are changed.

Steps:

1. On all servers involved in your environment, enable the following Security settings in your Local DTC Properties.
2. Click Start → Administrative Tools → Component Services → Computers → My Computer → Distributed Transaction Coordinator → Local DTC.

Note: Several issues will arise (including a failure when creating cases) if MSDTC has not been configured properly.
1.2 Microsoft Windows Optimizations For Performance

This section will discuss the methods to improve performance for FTK Central and its components. Using Windows Optimizations can improve the performance.

1.2.1 Windows Power Settings

Steps:

1. Run the following command from the Windows Command Prompt with Admin rights to set the power plan to “High Performance” on Microsoft Windows Server 2016 and Microsoft Windows Server 2019:

   `<Drive>:\> powercfg /s scheme_min`

1.2.2 Microsoft Indexing Service

Steps:

1. Run the following commands from the Windows Command Prompt with Admin rights to disable the Windows Indexing Service on Microsoft Windows Server 2016 and Microsoft Windows Server 2019:

   `<Drive>:\> dism /online /Disable-Feature /FeatureName:Indexing-Service-Package
   `<Drive>:\> sc config WSearch start= disabled

1.3 Microsoft SQL Server 2016/2017/2019

Microsoft SQL Server is required for project creation and storage.

**Supported versions:** 2016, 2017 and 2019.

1.3.1 To install Microsoft SQL Server

**Notes:** Incompatibility:
- 32-bit and Express versions of MSSQL are not supported for collaboration or larger installations.

**Licensing:**
- Both "Standard" or "Enterprise" editions can be used.
- MSSQL licensing should be done based on CPU Core count rather than by User count (CAL).

**Steps:**

1. Run the SQL Server Installation Setup executable and wait for the **SQL Server Installation Center** window to appear.
2. Choose the **Installation** tab and click **New SQL Server stand-alone installation or add features to an existing installation**.
3. Enter your product key and click **Next**.
4. Accept the License Terms, and click **Next**.
5. When prompted, allow the installer to check for updates.
6. On the **Feature Selection** page, check **Database Engine Services** and click **Next**. You can also modify the directories, if desired.
7. On the **Instance Configuration** page, select either **Default Instance** or **Named Instance** and click **Next**.

**Note:** If using a Named Instance, be sure to remember the name.
8. On the **Server Configuration** page, open the **Collation** tab and ensure the Database Engine is set to **SQL_Latin1_General_CP1_CI-AS** and click **Next**. You may also change the Service Accounts, if desired.

9. On the **Database Engine Configuration** page, under the **Server Configuration** tab, select **Mixed Mode**, enter a password for the SQL system administrator (SA) account, add the domain "service account" as an administrator, and click **Next**. You can also modify the Data Directories, if desired.

   **Note:** Mixed Mode allows our product’s internal SQL users to function. It will also create the "sa" account, which can be disabled but not deleted during AccessData product installation.

10. At the **Ready to Install** page, confirm everything is correct and click **Install**.

11. Wait for the installation to complete and then close **Setup**.

12. Open **SQL Server Configuration Manager**.

13. In the left pane, expand **SQL Server Network Configuration**.

14. Select the **Protocols** entry for your newly installed SQL instance.
15. In the right pane, right-click **Named Pipes** and click **Enable**.

16. In the left pane, select **SQL Server Services**.

17. In the right pane, right-click the **SQL Server** service for your newly installed SQL instance and click **Restart**.

⚠️ **Warning:** Do not install SQL Reporting Service. If you have questions about this, please contact AccessData Support.
2 Standard Installation

The Installation section will take you through the installation of all components using the installer.

Note: All installations must be executed as the Service Account.

Warning: Paths may differ depending upon installation directories being used (e.g. ISO v Extracted Install folder).

Additionally, you may be prompted to install dependencies and frameworks. Ensure they are installed for a successful installation.

It is advisable to ensure all Windows Updates have been completed prior to installing the application. It is recommended to disable any automatic updates.

If any part of the installation prompts to reboot the computer, you must reboot and start over from step 1 to ensure all components are installed.

2.1 AccessData Forensic Tools Suite 7.5

2.1.1 To install FTK Central

Steps:

1. Download the latest version of FTK Central from https://accessdata.com/product-download
2. Insert or Mount the FTK Central installation media and launch the autorun.
   - Alternatively run AccessData_Forensic_Tools_Suite_(64-bit).exe from the root of the installation media.
3. At the AccessData Forensic Tools Suite Installer Welcome dialog, click **Next**.

4. Review and accept the License Terms, and click **Next**.

5. Click **Install FTK Central**.
6. Select the program features applicable to your environment.
   - Select **Distributed Processing Manager** only if you will be utilizing Distributed Processing Engines.

7. Click **Install**.

8. Once complete, the **Evidence Processing Engine 10.25** will begin installing.

9. Review and accept the License Terms, and click **Next**.
10. Select an **installation path**.
   - If you are planning on utilizing a distributed environment with a **Distributed Processing Manager**, ensure you check “Install as distributed processing engine”.

11. Click **Next**.

12. Select a path for both the **Processing Temporary** folder as well as the **Processing State** folder.
   - It is recommended that the **Processing Temporary** folder is stored on a separate drive.

13. Click **Install**.

14. Once complete, (if selected) the **Distributed Processing Manager 10.25** will begin installing.

15. Click **Next**.

16. Review and accept the License Terms, and click **Next**.
17. Select a path for both the **Installation** folder as well as the **Processing State** folder.

18. Enter the **Service Account** credentials and **Domain**
   - If you are using a local non-domain account then leave the **Domain** field empty.

19. Click **Install**.

20. Click **Finish**.

21. Once complete, **Collab** will begin installing.

22. Click **Next**.

23. Review and accept the License Terms, and click **Next**.

24. Enter the **Service Account** credentials and **Domain**
   - If you are using a local non-domain account then check “**Use Local System account for service**”.

25. Click **Next**.

26. Click **Install**.

27. Once complete, **AccessData Forensic Tools 7.5** will begin installing.

28. Select a **Language** and click **OK**.

29. Click **Next**.

30. Review and accept the License Terms, and click **Next**.

31. Select an **installation path**.
32. Set the Database Computer/IP and Exterro Server Computer/IP.

33. Click Next.

34. Enter the Service Account credentials and Domain
   - If you are using a local non-domain account then check “Use Local System account for service”.

35. Click Next.

36. Click Install.

37. Click Finish.
2.2 Database: DBConfig

This section discusses the installation of DBConfig, it must be installed to allow FTK Central to function completely.

2.2.1 To install Database: DBConfig

Steps:

1. Navigate to ("<Drive>:\Program Files\AccessData\Forensic Tools\7.5\bin\DBConfig.exe").
2. Run the DBConfig executable as an Administrator.
3. Click Add Configuration.
4. Complete the following entries:
   - **Database Type** – MSSQL
   - **Server Name: Port** – Database location in the format host:port (Port is only required when using a non-default port).
   - **Create Database** – True/Check.
   - **Authentication Mode** – Mode to Authenticate, Windows Authentication preferably.
• **System User** – When using Database Authentication, this is the database user to use when authenticating.

• **System Password** – When using Database Authentication, this is the database password to use when authenticating.

• **Application Admin** – The desired username for your first FTK Central administrator.

• **Admin Password** – The desired password your first FTK Central administrator.

5. Click **Create**.

   **Note:** Once the database has been created, confirm the **Default** box has been checked next to the entry of your new database.

6. Close the **AccessData Database Configuration Tool** window and reboot your system.
2.3 AppDB

This section discusses the installation of AppDBs, it must be installed to use Off-Network and Cloud Data connectors.

2.3.1 To install AppDB

Steps:

1. Navigate to ("<Drive>:\Program Files\AccessData\Forensic Tools\7.5\bin\AccessData_eDiscovery_Database_Setup.exe").
2. Run the AccessData eDiscovery Database Setup executable as an Administrator.

Note: You may be prompted to install additional runtime libraries, click Install.

3. Click Next.
4. Review and accept the License Agreement and click Next.
5. At the Database Server dialog, enter the connect string and credentials for your MSSQL database used with FTK Central and click Next.
6. Click Install.
7. Click Finish.

Warning: By default, the application will use the SQL instance pointed to in dbconfig.
If MSSQL is using a named instance and/or on a different machine than FTK Central, do the following:

i. Navigate to ("<Drive>:\Program Files\AccessData\Forensic Tools\7.5\bin\ADG.WeblabSelfHost.exe.Config").
ii. Open the config file in a text editor.
iii. Under the **ConnectionString** section, modify the “Infrastructure” and “eDiscovery” keys, replacing the word “localhost” with your MSSQL connection string.

iv. Save the file.

```xml
<add name="Infrastructure" connectionString="Data Source=\SQL02\Initial
Catalog=Infrastructure;Integrated
Security=SSPI;MultipleActiveResultSets=True;App=EntityFramework"
    providerName="System.Data.SqlClient" />
<add name="eDiscovery" connectionString="data
source=\SQL02\initial
    catalog=eDiscovery;Integrated
Security=SSPI;MultipleActiveResultSets=True;App=EntityFramework"
    providerName="System.Data.SqlClient" />
```

v. Restart **AccessData Quin-C Self Host Service** service.
3 Component by Component Installation (Advanced)

The Installation section will take you through the installation of all components without using the installer.

Note: All installations must be executed as the Service Account.

Warning: Paths may differ depending upon installation directories being used (e.g. ISO v Extracted Install folder).

3.1 Licensing

3.1.1 License Manager
The License Manager is required for AD License Manager to recognize installed licenses.

3.1.1.1 To install the License Manager
Steps:

1. Navigate to: ("\<Version>\ALL_Suite\x64\{6F8C49D6-8EDC-4F06-9348-2E6EC0798963}\LicenseManager_Install.exe ").
2. Run the License Manager Install 3.5.0 executable as an Administrator.
3. Click Next.
4. Review and accept the License Terms, and click Next.
5. Select the installation folder for the License Manager.
6. Click Next.
7. Click Install.
8. Click Finish.
3.1.2 CodeMeter

CodeMeter is required to authenticate the licenses tied to a machine.

3.1.2.1 To install CodeMeter

Steps:

1. Navigate to: (“\<Version>\ALL_Suite\x64\{F5F91CCC-5315-49F7-8849-AE1673C65222}\CodeMeterRuntime64.msi”).
2. Run the CodeMeter executable as an Administrator.
3. The CodeMeter Runtime Kit Setup Wizard will appear, click Next.
4. Review and accept the License Agreement, click Next.
5. Fill in the Username and Organization fields and click Next.
6. Review the Custom Setup dialog and click Next.
7. Click Install.
8. Once the installation is complete, click Finish.

**Note:** During installation, reboot if prompted before continuing with the installation of other components.
3.2 .NET 4.7.2

.NET 4.7.2 framework is a dependency required for FTK Central and its components to run appropriately.

3.2.1 To install .NET 4.7.2

Steps:

1. Navigate to (“\<Version>\ALL_Suite\x64\{BFDD2D86-12F9-41AE-9D8A-260A59C66C71}\ISSetupPrerequisites\{BFF4A593-74C5-482F-9771-7495035EBBB0}\NDP472-KB4054530-x86-x64-AllOS-ENU.exe”).
2. Run the .NET 4.7.2 executable as an Administrator.
3. Review and accept the License Agreement, click Install.
4. Once the installation is complete, click Finish.

Note: During installation, reboot if prompted before continuing with the installation of other components.
3.3 AccessData Forensic Tools

This section discusses the installation of AccessData Forensic Tools, which includes but is not limited to FTK Central

3.3.1 To install AccessData Forensic Tools (App/Web/Collections Server)

Steps:

1. Navigate to ("\<Version>\ALL_Suite\x64\{BFDD2D86-12F9-41AE-9D8A-260A59C66C71}\AccessData_Forensic_Tools.exe").
2. Run the AccessData Forensic Tools executable as an Administrator.
3. Accept the License Agreement and click Next.
4. Click Install FTK Central.

⚠️ Warning: Default installations should only be done in a single-box, single-drive environment.

5. Check Forensic Tools and uncheck any other components and click Install.
6. Select the Language for installation and click OK.
   - It is advisable to select the same language which the Operating System is actively using. In most cases, English will be the best choice for user experience.

   Note: You may be prompted to install additional Microsoft Visual C++ runtime libraries, click Install.

7. Click Next.
8. Review and accept the License Agreement and click Next.
9. At the Configuration dialog, select the desired installation folder, database host and Quin-C host and click Next.
10. At the User Credentials dialog, enter the credentials for an account to run the Quin-C service.

**Warning:** This account should be a member of the local administrator’s 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.

11. Click **Next**.
12. Click **Install**.
13. Click **Finish**.
3.4 **Database: DBConfig**

This section discusses the installation of DBConfig, it must be installed to allow FTK Central to function completely.

3.4.1 **To install Database: DBConfig**

**Steps:**

7. Navigate to ("<Drive>:\Program Files\AccessData\Forensic Tools\7.5\bin\DBConfig.exe").

8. **Run the DBConfig executable as an Administrator.**

![DBConfig Configuration Tool](image)

9. Click **Add Configuration**.

10. Complete the following entries:
    - **Database Type** – MSSQL
    - **Server Name: Port** – Database location in the format host:port (Port is only required when using a non-default port).
    - **Create Database** – True/Check.
    - **Authentication Mode** – Mode to Authenticate, Windows Authentication preferably.
• **System User** – When using Database Authentication, this is the database user to use when authenticating.

• **System Password** – When using Database Authentication, this is the database password to use when authenticating.

• **Application Admin** – The desired username for your first FTK Central administrator.

• **Admin Password** – The desired password your first FTK Central administrator.

11. Click **Create**.

**Note:** Once the database has been created, confirm the **Default** box has been checked next to the entry of your new database.

12. Close the **AccessData Database Configuration Tool** window and reboot your system.
3.5 AppDB

This section discusses the installation of AppDBs, it must be installed to use Off-Network and Cloud Data connectors.

3.5.1 To install AppDB

Steps:

8. Navigate to ("<Drive>:\Program Files\AccessData\Forensic Tools\7.5\bin\AccessData_eDiscovery_Database_Setup.exe").
9. Run the AccessData eDiscovery Database Setup executable as an Administrator.

Note: You may be prompted to install additional runtime libraries, click Install.

10. Click Next.
11. Review and accept the License Agreement and click Next.
12. At the Database Server dialog, enter the connect string and credentials for your MSSQL database used with FTK Central and click Next.
13. Click Install.
14. Click Finish.

Warning: By default, the application will use the SQL instance pointed to in dbconfig. If MSSQL is using a named instance and/or on a different machine than FTK Central, do the following:

vi. Navigate to ("<Drive>:\Program Files\AccessData\Forensic Tools\7.5\bin\ADG.WeblabSelfHost.exe.Config").

vii. Open the config file in a text editor.
viii. Under the `ConnectionString` section, modify the “Infrastructure” and “eDiscovery” keys, replacing the word “localhost” with your MSSQL connection string.

ix. Save the file.

```xml
  <add name="Infrastructure" connectionString="Data Source=SQL01;Initial Catalog=Infrastructure;Integrated Security=SSPI;MultipleActiveResultSets=True;App=EntityFramework"
       providerName="System.Data.SqlClient" />
  <add name="eDiscovery" connectionString="Data Source=SQL02;Initial Catalog=eDiscovery;Integrated Security=SSPI;MultipleActiveResultSets=True;App=EntityFramework"
       providerName="System.Data.SqlClient" />
```

x. Restart **AccessData Quin-C Self Host Service** service.
3.6 AccessData Collab

This section discusses the installation of AccessData Collab, it must be installed to allow FTK Central to function completely.

3.6.1 To install AccessData Collab

Steps:

1. Navigate to ("\<Version>\ALL_Suite\x64\{C44A37E3-939F-445C-9EA9-65CE5BAD3657\}\AccessData_Collab_(64-bit).exe").

2. Run the AccessData Collab (64-bit) executable as an Administrator.

3. Click Next.

4. Uncheck “Use Local System account for service”.

5. Enter the Username, Domain and Password for the service account.

   Warning: 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.

6. Click Next.

7. Click Install.

8. Click Finish.
3.7 AccessData Evidence Processing Engine(s)

This section discusses the installation of AccessData Evidence Processing Engine (distributed processing engine), it must be installed to allow FTK Central to function completely.

3.7.1 To install AccessData Evidence Processing Engine

Steps:

1. Navigate to ("\<Version>\ALL_Suite\x64\DPM_10.25.0_203\Engine\x64\{1F0B9032-5C06-4032-91AB-BB51EF44E34C}\AccessData_Evidence_Processing_Engine_(64-bit).exe").
2. Run the AccessData Evidence Processing Engine (64 bit) executable as an Administrator.
3. Click Next.
4. Review and accept the License Agreement and click Next.
5. Select the install path for the distributed processing engine.
6. Check “Install as distributed processing engine”.
7. Click Next.
8. Select the Processing Temporary folder.

**Note:** It's recommended to put the Processing Temporary Folder on its own drive.

9. Enter the Username, Domain and Password for the service account.

**Warning:** This account must 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.

10. Click Next.
11. Click Install.
12. Click Finish.
3.8 AccessData Distributed Processing Manager

This section discusses the installation of AccessData Distributed Processing Manager it must be installed to allow FTK Central to function completely.

3.8.1 To install AccessData Distributed Processing Manager

Steps:

1. Navigate to, ("\<Version>\ALL_Suite\x64\{FE937E9C-3BC9-4D26-90C3-A4549E86FB32}\AccessData_Distributed_Processing_Manager_(64-bit).exe").
2. Run the AccessData Distributed Processing Manager (64-bit) executable as an Administrator.
3. Click Next.
4. Review and accept the License Agreement and click Next.
5. Select the install path for the Distributed Processing Manager.
6. Select the Processing State Folder.

Note: It's recommended to put the Processing State Folder on its own drive.

7. Click Next.
8. Enter the Username, Domain and Password for the service account.

Warning: This account must to be a member of the local administrator’s 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.

9. Click Next.
10. Click Install.
11. Click Finish.
3.9 Site Server(s)

This section discusses the installation of the Site Server it must be installed to allow FTK Central to function completely.

Note: If the DMZ machine is only running PostgreSQL and the Public Site Server, this machine can be off-domain and Public Site Server can be run by the "Local System" account.
3.9.1 Dependencies and PostgreSQL

3.9.1.1 To install dependencies and PostgreSQL

Steps:

1. Install .NET 4.7.2 (`"\<Version>\ALL_Suite\x64\{BFDD2D86-12F9-41AE-9D8A-260A59C66C71}\ISSetupPrerequisites\{BFF4A593-74C5-482F-9771-7495035EBBB0}\NDP472-KB4054530-x86-x64-AllOS-ENU.exe"`) and reboot if prompted.
3. Download and install Microsoft Visual C++ 2015-2019 Redistributable x64 and reboot if prompted.
4. Navigate to (`"\<Version>\ALL_Suite\x64\{C32BC7B7-3086-44FD-8A90-9EC47966B4B7}\PostgreSQLSetup_x64.exe"`).
5. Run the PostgreSQLSetup x64 executable as an Administrator.
6. Click Next.
7. Review and accept the License Agreement and click Next.
8. Select the installation path for PostgreSQL.
9. Click Next.
10. Select the PostgreSQL data folder.

**Note:** It's recommended to put the Data Folder on its own drive.

11. Enter the port.
12. Click Next.
13. Create a PostgreSQL database administrator password.
14. Click Next.
15. Click Install.
16. Click Finish.
3.9.2 Installing Site Server(s)

3.9.2.1 To install Site Server(s)

Steps:

1. Navigate to (“\<Version>\ALL_Suite\x64\installer\AccessData_Site_Server.exe”).
2. Run the AccessData Site Server executable as an Administrator.
3. Click Next.
4. Review and accept the License Agreement and click Next.
5. At the Destination Folder Dialog, select the desired installation folder and click Next.
6. At the User Credentials dialog, enter the credentials for an account to run the Site Server service, and click Next.

    **Warning:** This account should be a member of the local administrator’s 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.

7. Click Install.
8. Once the install is complete, check “Launch Site Server Configuration”.
9. Click Finish.
3.10 Agent(s)

This section discusses the installation of the Agent it must be installed to allow FTK Central to run collections.

3.10.1 Agent Push Requirements

3.10.1.1 Requirements

**AD Enterprise/Lab/FTK Central:**

- Verify the Agent and Modules paths under Tools > Configure Agent Push.
- Verify the Certificate paths in Enterprise Configuration.
- Verify the Agent certificates have not expired.
- Verify the Examiner machine can ping the target node.
- Verify the Windows account credentials specified when pushing the Agent have full Administrator permissions to the target Node (verify this by attempting to browse to \<TargetNode>\admin$)
- Ensure the Examiner machine is on the same domain as the target Node.
- Verify you are specifying the target by machine name or IP, not UNC path.
- Verify the Site Server is online via the Site Server Console.
- Verify the Agent and Modules folders have been created in the Site Server Results Directory.
- Verify the Certificate paths in Site Server Configuration.
- Verify the Agent certificates have not expired.
- Verify the target node IP is included in the "Manage Subnet Address" CIDR blocks in Site Server Configuration.
- Verify the Site Server machine can ping the target node.
- Verify you are specifying the target by machine name or IP, not UNC path.
Target Node:

- Verify the target doesn't already have an existing Agent installed.
- Verify TCP ports 135, 445, and 3999 are open (also open UDP 137 if using machine name instead of IP and 54555 if using Agent periodic check-in with eDiscovery).
- Verify SSL traffic is allowed over port 3999.
- Disable Antivirus/malware scanning software on target Node.
- Disable "Simple File Sharing" on the target Node.
- Verify the Windows %TEMP% and/or %TMP% locations are not full on the target Node.
- Delete any old copies of "AccessData Agent.msi" sitting in the target's %TEMP% and/or %TMP% locations.
- See if the Agent can even be installed manually.

Post Usage:

- 135 - Windows Messenger Service, used by WMI during Agent push
- 137 - Windows Naming Service, used to resolve machine names
- 445 - SMB File Sharing, used by WMI during Agent push
- 3999 - Agent communication port
- 54555 - Agent check-in port
3.10.2 Manually Installing Agents (Windows)

3.10.2.1 To install an Agent(s) manually

Prerequisites:

- Disable all firewalls.
- Enable network discovery and file sharing.

Steps:

1. Copy your Agent installer MSI "AccessData Agent (64-bit).msi"
   - Located in "<Drive>:\Program Files\AccessData\SiteServer\Agent\x64") to the extracted "Agent Installer" folder.

2. Copy your Agent public certificate to the local machine.

3. Open Command Prompt as an Administrator.

4. Formulate and run the installation command, according to the following:

   msiexec /i "<full_path_to_agent>" CER="<full_path_to_certificate>" {additional parameters}
   ALLUSERS=2

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Default Value</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CER=</td>
<td>&lt;PATH&gt;</td>
<td>N/A</td>
<td>Yes</td>
<td>Full path to the public certificate. Path must be enclosed in quotes if it contains spaces. Acceptable certificate formats are P7B, P7C, DER, CER, and CRT.</td>
</tr>
<tr>
<td>INSTALLDIR=</td>
<td>&lt;PATH&gt;</td>
<td>C:\Program Files\AccessData\Agent</td>
<td>No</td>
<td>Specifies a desired path to install the agent. Path must be enclosed in quotes if it contains spaces. If not specified, the default value is assumed.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Default Value</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>---------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PORT=</td>
<td>&lt;PORT&gt;</td>
<td>3999</td>
<td>No</td>
<td>The port that the agent will be listening on. If not specified, the default value is assumed.</td>
</tr>
<tr>
<td>STORESIZE=</td>
<td>&lt;NUMBER&gt;</td>
<td>268435456</td>
<td>No</td>
<td>Specifies the agent temporary data storage size. If not specified, the default value is assumed.</td>
</tr>
<tr>
<td>SYSTEMSIZE=</td>
<td>&lt;NUMBER&gt;</td>
<td>16777216</td>
<td>No</td>
<td>Specifies the agent configuration files storage size. If not specified, the default value is assumed.</td>
</tr>
<tr>
<td>TRANSIENT=</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>LIFETIME=</td>
<td>&lt;NUMBER&gt;</td>
<td>0</td>
<td>No</td>
<td>Specifies the amount of time that a transient agent will exist before self-destructing. A negative value is used to denote minutes (eg. -30 denotes 30 minutes), and a positive value is used to denote days (eg. 30 denotes 30 days). Requires use of TRANSIENT=1.</td>
</tr>
<tr>
<td>FOLDER_STORAGE=</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>SERVICELESS=</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Default Value</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------</td>
<td>---------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MAME=</td>
<td><a href="">HOSTNAME:PORT</a> Or <a href="">IP:PORT</a></td>
<td>N/A</td>
<td>No</td>
<td>Hostname or IP address and port of the Site Server that the agent should check-in with. Default Site Server port is 54545. If using v6.x or newer heartbeat port is by default 54555. This should only be used with a product that uses Site Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Retry Interval:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Connect every 30 mins.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Retry 3 times.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Wait 30 Seconds between retries.</td>
</tr>
<tr>
<td>PUBSS=</td>
<td><a href="">IP:PORT</a></td>
<td>N/A</td>
<td>No</td>
<td>IP address and port of the Public Site Server that the agent should check-in with. Default Site Server port is 54545. This should only be used with a product that uses Site Server.</td>
</tr>
<tr>
<td>PUBSS_DELAY=</td>
<td>&lt;NUMBER&gt;</td>
<td>N/A</td>
<td>No</td>
<td>The delay cycle, in seconds, between connections to the Public Site Server. This will reset to the value sent from the SiteServer upon successful connection.</td>
</tr>
</tbody>
</table>
3.10.3 Manually Uninstalling Agents (Windows)

3.10.3.1 To uninstall an Agent(s) manually

**Warning:** The version of the agent being copied must be the same version as the installed agent. Failing to match versions will result in failed removals.

**Steps:**

1. **Copy** the Agent installer to the local machine.
2. Open Command Prompt as an **Administrator**.
3. Formulate and run the uninstallation command, according to the following:
   
   ```msiexec /x "<full_path_to_agent_msi>" NUKE=1```

   **Note:** The above MSIXEC command can be used in conjunction with an Agent MSI in SCCM (or similar) to uninstall Agents en masse.
3.10.4 Installing Agents with a script (Windows)

3.10.4.1 To install an Agent(s) with a script

Steps:

1. Download [Windows Agent Installation Package Template.zip](#).
2. Extract the contents off the ZIP file.
3. Copy your Agent installer MSI "[AccessData Agent (64-bit).msi](#)"
   - Located in "<Drive>:\Program Files\AccessData\SiteServer\Agent\x64") to the extracted "Agent Installer" folder.
4. Copy your Agent public certificate to the extracted "Public Certificate" folder.
5. Edit the extracted "Install Windows Agent.bat" in a text editor and update the "certname", "MAMA'", and "PUBSS" variables.
3.10.5 Manually Installing Agents (Unix/Linux)

### 3.10.5.1 To install an Agent(s) manually

**Prerequisites:**
- Allow incoming communication on port 3999.

**Steps:**

1. **Locate** the Agent installer SH script.
   - Typically located in “<Drive>:\Program Files\AccessData\SiteServer\Agent\core”.
2. **Locate** the public certificate to be used by your Agents.
3. Copy the SH script and public certificate to the target machine.
4. **Open** Terminal, and run the following command to give the SH script execute permissions.
   ```
   chmod +x <full_path_to_sh_script>
   ```
5. **Run** the following command to install the Agent.
   ```
   sudo <full_path_to_sh_script> <full_path_to_certificate> {parameters}
   ```
6. **Start** the Agent with the following command:
   ```
   sudo /etc/init.d/agentcored start
   ```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Default Value</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-installpath</td>
<td>&lt;PATH&gt;</td>
<td>/usr/AccessData/agent</td>
<td>No</td>
<td>Specifies a desired path to install the agent. Path must be enclosed in quotes if it contains spaces. If not specified, the default value is assumed.</td>
</tr>
<tr>
<td>-lifetime</td>
<td>&lt;NUMBER&gt;</td>
<td>0</td>
<td>No</td>
<td>Specifies the amount of time that a transient agent will exist before self-destructing. A</td>
</tr>
</tbody>
</table>
### Installation Guide

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Default Value</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-port</td>
<td>&lt;PORT&gt;</td>
<td>3999</td>
<td>No</td>
<td>The port that the agent will be listening on. If not specified, the default value is assumed.</td>
</tr>
<tr>
<td>-connections</td>
<td>&lt;NUMBER&gt;</td>
<td>10</td>
<td>No</td>
<td>Specifies the number of concurrent connections allowed to the agent. If not specified, the default value is assumed.</td>
</tr>
<tr>
<td>-size</td>
<td>&lt;NUMBER&gt;</td>
<td>16777216</td>
<td>No</td>
<td>Specifies the agent configuration files storage size. If not specified, the default value is assumed.</td>
</tr>
<tr>
<td>-datasize</td>
<td>&lt;NUMBER&gt;</td>
<td>268435456</td>
<td>No</td>
<td>Specifies the agent temporary data storage size. If not specified, the default value is assumed.</td>
</tr>
</tbody>
</table>

- A negative value is used to denote minutes (e.g., -30 denotes 30 minutes), and a positive value is used to denote days (e.g., 30 denotes 30 days). 0 indicates that the agent will not self-destruct. If not specified, the default value is assumed.
3.10.6 Manually Uninstalling Agents (Unix/Linux)

3.10.6.1 To uninstall an Agent(s) manually

Steps:

1. **Open** Terminal and stop the Agent with the following command.

   ```bash
   sudo /etc/init.d/agentcored stop
   ```

2. Navigate (cd) to the Agent installation directory (typically /usr/AccessData/agent).

3. **Run** the following command.

   ```bash
   sudo ./installer.sh -remove
   ```

4. **Delete** the Agent installation directory.

5. **Reboot** the machine.
3.10.7 Manually Stopping Agents (Unix/Linux)

3.10.7.1 To stop an Agent(s) manually

The Linux Agent service is started automatically on system startup, but can be stopped, started, and restarted anytime manually by executing commands pertaining to stop, starting and restarting (as root).

- /etc/init.d/agentcored stop
- /etc/init.d/agentcored start
- /etc/init.d/agentcored restart
3.11 AI Server

This section discusses the installation of the AI Server, as it must be installed to allow Image Recognition features to function appropriately.

3.11.1 Installing the AI Server

Steps:

1. Navigate to (“\<Version>\ALL_Suite\x64\Optional-AI-{08B9F350C54B}\AccessData_AI_Server_x64.exe”).
2. Run the AccessData AI Server x64 as an Administrator.
3. Click Next.
4. Review and accept the License Agreement and click Next.
5. Select the installation path for the AI Server.
6. Check “Install for GPU use” if the server has a CUDA enabled graphics card.
7. Click Next.
8. Enter the Username, Domain and Password for the service account.

**Warning:** 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.

9. Click Next.
10. Click Finish.
3.12 KFF Server

This section discusses the installation of the KFF Server, as it must be installed to compare the file hash values of known files against the files in your project.

3.12.1 Installing the KFF Server

- Find the Installation of the KFF Server and configuration [here](#) or the 7.5 Enterprise manual from page 328.
4 Configuration

The configuration section will take you through the configuration of the App/Web/Collections Server.

4.1.1 Virtual CodeMeter (VCM) Activation Guide

4.1.1.1 To install a VCM

Note: If your forensic PC is offline, you will need access to a PC that is online and also has CodeMeter and License Manager installed.

Warning: Once activated, a VCM is tied to the machine where it was activated and cannot be moved.

Steps:

Online Activation
1. Disconnect all dongles
2. Open License Manager
3. At the error reporting "No Security Device Found!", click OK
4. Select "Create A Local Virtual CMStick" and click OK
5. Enter your VCM activation code and click OK
6. Click OK when the update completes.

Offline Activation
On the Offline machine follow the below steps:

1. Disconnect all dongles.
2. Open License Manager.
3. At the error reporting "No Security Device Found!", click OK
4. Select "Create Empty Virtual CMStick (Offline)" and click OK
5. Save the resulting WIBUCMRAC file.
6. Transfer the WIBUCMRAC file to the online PC.
On the Online machine follow the steps below:

1. Disconnect all dongles.
2. Open License Manager.
3. At the error reporting "No Security Device Found!", click OK.
4. Select "Create Activation File (Offline)" and click OK.
5. Enter your VCM activation code and click OK.
6. Browse to the WIBUCMRAC file and click Open.
7. Save the resulting WIBUCMRAU file.
8. Click OK when the update completes.
9. Transfer the WIBUCMRAU file back to the offline PC.

Again, on the Offline PC follow the below steps:

1. Disconnect all dongles
2. Open License Manager
3. At the error reporting "No Security Device Found!", click OK.
4. Select "Activate Virtual CMStick (Offline)" and click OK.
5. Browse to the WIBUCMRAU file and click Open.
4.2 Site Server(s)

4.2.1 Configuring the Site Server(s)

4.2.1.1 To configure the Site Server:

Steps:

1. In the Site Server Configuration, do the following:
   - **Type**: Root.
   - **Friendly Name**: Desired name to identify the Site Server.
   - **Private Certificate**: Your Agent Private Certificate.
   - **Public Certificate**: Your Agent Public Certificate.
   - **System Password**: Your PostgreSQL password.
   - **Database Port**: Your PostgreSQL port (Default: 5432).
   - **Results Directory**: Desired Site Server temporary storage path.
   - **Children Instances**: Blank.
   - **Managed Subnet Address(es)**: CIDR range(s) that you would like Site Server to be able to collect from.

2. Click Apply for the Site Server service to restart.

3. Click OK and Close.
4.3 Distributed Processing Manager

4.3.1 Configuring Distributed Processing Engine(s)

4.3.1.1 To configure the AccessData Distributed Processing Manager

Steps:

1. Navigate to "(<Drive>:\Program Files\AccessData\Distributed Processing Manager\10.25\ProcessingManagerConfig.exe)".

2. Run the ProcessingManagerConfig executable as an Administrator.

3. For each of the machines running the Distributed Processing Engine, do the following:
   a. In the Computer name/IP field, enter the name/IP of the machine.
   b. Click Add.

4. After all desired processing engines have been added, click Save.

5. Click Close.
4.3.2 Configuring Distributed Processing Engines: Certificates

4.3.2.1 To configure the AccessData Distributed Processing Manager

Steps:

1. Obtain a certificate to use for SSL, issued to the App/Web/Collections server by a valid CA authority, in PFX format.
2. Copy the PFX to ("<Drive>:\Program Files\AccessData\Certificates").
3. Open "<Drive>:\Program Files\AccessData\Forensic Tools\7.5\bin\ADG.WeblabSelfHost.exe.Config" in a text editor.
4. Under the appSettings section, do the following:
   i. Change the value of the "certificateFileName" key to the full path of the exported PFX.
   ii. Change the value of the "certificatePassword" key to the password to the exported PFX.
   iii. Change the value of the "CertificatePath" key to the full path to the Agent private certificate.
   iv. Change the value of the "PushCert" key to the full path to the Agent public certificate.
   v. Change the value of the "TrustedCertificatePath" key to the full path to the adata.p7b (typically "<Drive>:\Program Files\AccessData\Forensic Tools\7.5\bin\Agent\modules\adata.p7b").
   vi. Change the value of the "ModulesPath" key to the full path to the Windows 64-bit modules folder (typically "<Drive>:\Program Files\AccessData\Forensic Tools\7.5\bin\Agent\modules\Windows\x64").
   vii. Change the value of the "SiteServerHost" key to the IP or hostname of the Root Site Server.
5. Save and close the file.
6. Restart the "AccessData Quin-C Self Host Service" service.
4.4 Agent(s)

4.4.1 Configuring Execname Values (Windows)

4.4.1.1 To configure Execname Value:

Steps:

1. Run Orca.EXE.
2. Click File > Open.
3. Browse to the folder containing the “AccessData Agent.msi” or “AccessData Agent (64-bit).msi” file and open the file.

\<Drive>:\Program Files\AccessData\SiteServer\Agent\x64\n
4. In the Tables list, select File...
5. In the FileName column, double-click “u4jwdc7h.exe|agentcore.exe”.
   - Enter the filename to use for the agent core executable.
6. Press Enter.
7. Click File > Save.
4.4.2 Configuring Servicename Values (Values)

4.4.2.1 To configure Servicename Value

Steps:

1. Run Orca.EXE.
2. Click File > Open.
3. Browse to the folder containing the “AccessData Agent.msi” or “AccessData Agent (64-bit).msi” file and open the file. The default path is:

   <Drive>:\Program Files\AccessData\SiteServer\Agent\x64\n
4. In the Tables list, select “ServiceControl”.
5. In the Name column, double-click “AgentService”.
   - Enter the name to use for the AgentService and press Enter.

   Note: Use the same value in steps 5, 7 and 8.

6. In the Tables list, select “ServiceInstall”.
7. In the Name column, double-click “AgentService”.
   - Enter the name to use for the AgentService (use the same value entered in step 5a) and press Enter.
8. In the DisplayName column, double-click “AgentService”.
   - Enter the name to use for the AgentService (use the same value entered in steps 5a and 7a) and press Enter.
9. Click File > Save.
10. Click File > Close.
4.4.3 Controlling Consumption of the CPU (Windows): Throttling

4.4.3.1 To control CPU Consumption

Steps:

1. In the Registry Editor, expand the HKEY_LOCAL_MACHINE hive and locate the
   HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared folder.
2. Add a new DWORD (32-bit) value to the Shared folder.
   (HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared\throttling)
3. The data value of the DWORD should be the maximum percentage of the CPU allowed to be used by
   the module. For example, if you want the maximum percentage of the CPU used to be 25 percent,
   modify the DWORD data value and enter 25 in the Edit DWORD dialog. The value should be from 0-
   100. If the data value is left at 0, the CPU will not be throttled when the agent is started.
4. In the Edit DWORD dialog, select the Decimal radio button and click OK.
5. After applying the registry key changes, restart the agent service.
4.4.4 About Using Certificates

4.4.4.1 Using Certificates:

<table>
<thead>
<tr>
<th>Component</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents</td>
<td>• Agents only use a Public Cert. It must be provided at install time.</td>
</tr>
</tbody>
</table>
| Site Server | • SiteServer certs are configured using the SiteServer Config tool (SS_Config.exe).  
• SiteServer uses its Private Cert to communicate with agents.  
• SiteServer uses its Public Cert to communicate with Clients (if Use Secure Client is selected) and to communicate with other SiteServer instances. |
| Client    | • Client programs use a Private Cert to communicate with a SiteServer instance. For the eDiscovery Work Manager, the path to the Private Cert must be entered into its config file. |
4.4.5 Certificate Verification Checklist

4.4.5.1 Verification Checklist

- Print out the human-readable contents of Public and Private certs using OpenSSL.
- You may also be able to verify some items by just double-clicking to view them in Windows. This works fine for CER and P7B; unfortunately, with PFX it wants to do an import, so you may not want to do that.
- For the Public Cert (P7B): Verify that it contains the Root CA cert in there.
- It may have up to 3 certs in here (root CA, intermediate, and leaf). For each one, you are looking for the "CN=" part of the Subject to tell which cert it is.
- Also, verify that this file is in binary format by opening with notepad and noticing that it looks like "<randomchars>". If you see a "-----BEGIN CERTIFICATE-----" in the P7B, then it was exported incorrectly and will not work with our products.
- For the Private Cert (PFX or PEM): Convert to PEM following instructions in my doc.
- Verify that it contains the correct public cert with the common name (look for CN= on Subject line) you chose. This cert doesn't need to have the full chain of certs; usually just the one cert.
- Also, run the command to print out the private key to verify the PEM contains a private key. Once you plug in the PEM (or PFX) into SiteServer, it will automatically convert it to an ADP12. Always use ADP12 in SS Config tool and in the WM config file.
- For the Cert to use while pushing agents (CER): This should be a CER file containing the Root CA (a P7B is also ok, but no need to be a P7B since only one cert in here). Use openssl to print it out in human-readable format and verify it contains just the Root CA cert.
4.5 Enable SSL/HTTPS In FTK-Central

4.5.1 Configuring SSL/HTTPS

Prerequisite:
Certificate archive, in password-protected PFX format, whose "Issued To" name either matches the base URL of the Quin-C website or has a domain wildcard.

Note: The password cannot contain certain characters, such as quotes, for it to work in the XML config file.

4.5.1.1 To configure SSL/HTTPS

Steps:

1. **Copy your PFX file** into the FTK-Central bin folder (typically "<Drive>:\Program Files\AccessData\Forensic Tools\<version>\bin\").
2. From the bin folder, open `ADG.WeblabSelfHost.exe.config` in a text editor.
3. Find and change the value of the `certificateFileName` key to the full path to your PFX file.
   
   ```xml
   <add key="certificateFileName" value="<Drive>\Program Files\AccessData\Forensic Tools\7.5\bin\myCertificate.pfx" />
   ```

4. Find and change the value of the `certificatePassword` key to the password for your PFX file.

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

5. Find and change the value of the `JobMasterLink` key to use https and port 443.

   ```xml
   <add key="JobMasterLink" value="https://localhost:443/" />
   ```

6. **Restart** the AccessData Quin-C Self Host Service service.
4.6 Enable NATO Specific Features/Jobs

4.6.1 Enabling NATO Jobs

4.6.1.1 To configure NATO Jobs

Steps:

1. Navigate to ("<Drive>:\Program Files\AccessData\Forensic Tools\<Version>\bin\").
2. From the bin folder, open ADG.WeblabSelfHost.exe.config in a text editor.
3. Add the EnableAgentScanJobs key to the config file.

   <add key="EnableAgentScanJobs" value="true"/>

4. Restart the AccessData Quin-C Self Host Service service.