ATAIS - Implementation Guide



Advanced Threat Analytics Implementation Services

Prepared for

Customer Name

6/27/2016

Version Draft

Prepared by

**[Update Author in Doc Properties]**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Implementation Guide Summary 1](#_Toc454800137)

[1.1 Objectives 1](#_Toc454800138)

[2 Solution Requirements 2](#_Toc454800139)

[2.1 Sizing Requirements 2](#_Toc454800140)

[2.1.1 ATA Center 2](#_Toc454800141)

[2.1.2 ATA Lightweight Gateway 3](#_Toc454800142)

[2.1.3 ATA Gateway 4](#_Toc454800143)

[2.2 Hardware Requirements 4](#_Toc454800144)

[2.2.1 ATA Center 4](#_Toc454800145)

[2.2.2 ATA Lightweight Gateway 5](#_Toc454800146)

[2.2.3 ATA Gateway 5](#_Toc454800147)

[2.3 Software Requirements 7](#_Toc454800148)

[2.3.1 ATA Center 7](#_Toc454800149)

[2.3.2 ATA Lightweight Gateway 8](#_Toc454800150)

[2.3.3 ATA Gateway 9](#_Toc454800151)

[2.4 Pre-deployment Requirements 10](#_Toc454800152)

[3 Deployment 11](#_Toc454800153)

[3.1 Step 1: Installing the ATA Center 11](#_Toc454800154)

[3.1.1 Validating the Installation of the Center 13](#_Toc454800155)

[3.2 Step 2: Configure ATA Gateway Domain Connectivity Settings 14](#_Toc454800156)

[3.3 Step 3: Download the ATA Gateway Setup Package 15](#_Toc454800157)

[3.4 Step 4: Install the ATA Gateways 16](#_Toc454800158)

[3.4.1 Install the ATA Lightweight Gateway 16](#_Toc454800159)

[3.4.2 Install the ATA Gateway 17](#_Toc454800160)

[3.5 Step 5: Configure the ATA Gateways 19](#_Toc454800161)

[3.5.1 Configure the ATA Lightweight Gateway 19](#_Toc454800162)

[3.5.2 Configure the ATA Gateway 20](#_Toc454800163)

[3.5.3 Validating the ATA Gateway Installation 23](#_Toc454800164)

[3.6 Step 6: Configure Short-Term Lease Subnets 24](#_Toc454800165)

[3.7 Step 7: Configure the Honeytoken User 25](#_Toc454800166)

[3.8 Step 8: Post-Installation Information 25](#_Toc454800167)

[4 Appendix 26](#_Toc454800168)

[4.1 Configure Port Mirroring 26](#_Toc454800169)

[4.1.1 Supported Port Mirroring Options 27](#_Toc454800170)

[4.1.2 Hyper-V Virtual Switch – Windows Server 2012 27](#_Toc454800171)

[4.2 Configuring Security Information and Event Management (SIEM) Integration 28](#_Toc454800172)

[4.2.1 Configuring the ATA Gateway to Listen for and Accept SIEM Events 28](#_Toc454800173)

[4.2.2 Supported SIEM Solutions 29](#_Toc454800174)

[4.3 Configuring Windows Event Forwarding (WEF) 29](#_Toc454800175)

## Table of Tables

[Table 1: Requirements - Center Sizing 2](#_Toc454800176)

[Table 2: Requirements – ATA Lightweight Gateway Sizing 3](#_Toc454800177)

[Table 2: Requirements – ATA Gateway Sizing 4](#_Toc454800178)

[Table 3: Requirements – ATA Center Hardware 4](#_Toc454800179)

[Table 4: Requirements – ATA Lightweight Gateway Hardware 5](#_Toc454800180)

[Table 4: Requirements – ATA Gateway Hardware 6](#_Toc454800181)

[Table 5: Requirements - Center Software 7](#_Toc454800182)

[Table 6: Requirements - Gateway Software 8](#_Toc454800183)

[Table 6: Requirements - Gateway Software 9](#_Toc454800184)

[Table 7: ATA Center - Installation Configuration 11](#_Toc454800185)

[Table 8: ATA Gateway - Domain Connectivity Settings 14](#_Toc454800186)

[Table 9: ATA Lightweight Gateway - Installation Configuration 16](#_Toc454800187)

[Table 9: ATA Gateway - Installation Configuration 18](#_Toc454800188)

[Table 10: ATA Gateway – Post-Installation Configuration 19](#_Toc454800189)

[Table 10: ATA Gateway – Post-Installation Configuration 21](#_Toc454800190)

[Table 11: Port Mirroring Options 27](#_Toc454800191)

## Table of Figures

[Figure 1: ATA Center - Installation Configuration 13](#_Toc454800192)

[Figure 2: ATA Gateway - Domain Connectivity Settings 15](#_Toc454800193)

[Figure 3: ATA Lightweight Gateway - Installation Configuration 17](#_Toc454800194)

[Figure 3: ATA Gateway - Installation Configuration 19](#_Toc454800195)

[Figure 4: ATA Lightweight Gateway – Post-Installation Configuration 20](#_Toc454800196)

[Figure 4: ATA Gateway – Post-Installation Configuration 22](#_Toc454800197)

[Figure 5: Performance Monitor - Adding Counters 24](#_Toc454800198)

[Figure 6: ATA Detection Configuration 25](#_Toc454800199)

**Spell/grammar check is turned ON within all Services Delivery Method (SDM) Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click on File
2. Click on the Options on the left
3. Click on Proofing
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl H to open the Find and Replace box
2. Make sure your cursor is in the ‘Find what’ box.
3. Click on the More button at the bottom left
4. Click on the Format Button at the bottom left and select Style
5. Scroll down, locate select the “Visible Guidance”
6. Make sure the ‘Replace with’ box is empty:
7. Click ‘Replace All”
8. If not empty - click on the format button in the lower left hand corner. Scroll down and chose ‘(no style)’then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

1. Implementation Guide Summary

This document provides installation information for the implementation of Microsoft Advanced Threat Analytics (ATA). This document also complements the Operations Guide delivered as part of this engagement.

* 1. Objectives

This document covers the following topics to complete a successful deployment of ATA for Customer Name.

* The requirements for the both the ATA Center and the ATA Gateways as discussed during the Envisioning phase.
* The deployment of ATA based on the agreed configuration in the Solutions Design Document and results of the testing and Stabilization phase.
* The configuration of event collection.
* The configuration of port mirroring within Microsoft Hyper-V, if required.

1. Solution Requirements

The following section outlines the requirements discussed during the envisioning phase of this engagement and its agreed configuration recorded in the Solutions Design document.

* 1. Sizing Requirements
     1. ATA Center

The following information provides recommended guidelines for how to size the ATA Center system. This information is dependent on the amount of network traffic your domain controllers generate (traffic to and from) and the amount of relevant data (suspicious activities) that ATA detects and stores within its database. The following table provides general sizing guidelines that help to design the size needed for the ATA Center.

The ATA Center requires a recommended minimum of 30 days of data for learning normal user behaviors and capturing behavioral analytics. The required disk space for the ATA database for each domain controller is defined in the following table based on Customer Name’s specific domain controller statistics.

This methodology will be used to determine the overall compute needs for your ATA Center. This information will be documented in section 2.4.1 of this document.”

More detail on ATA sizing can be found in the TechNet article “[ATA Capacity Planning](https://technet.microsoft.com/en-us/library/mt429323.aspx).”

Table 1: Requirements - Center Sizing

| Packets Per Second\* | CPU (cores\*\*) | Memory (GB) | Database Storage per Day (GB) | Database Storage Per Month (GB) | IOPS\*\*\* |
| --- | --- | --- | --- | --- | --- |
| 1,000 | 2 | 32 | 0.3 | 9 | 30 (100) |
| 10,000 | 4 | 48 | 3 | 90 | 200 (300) |
| 40,000 | 8 | 64 | 12 | 360 | 500 (1,000) |
| 100,000 | 12 | 96 | 30 | 900 | 1,000 (1,500) |
| 400,000 | 40 | 128 | 120 | 1,800 | 2,000 (2,500) |

\* Total daily average number of packets per second from the all domain controllers being monitored by all ATA Gateways

\*\* This includes physical cores, not hyperthreaded cores.

\*\*\* Average numbers (peak numbers)

**Notes:**

The ATA Center can handle an aggregated maximum of 400,000 frames per second (FPS) from all the monitored domain controllers.

The amounts of storage dictated here are net values, you should always account for future growth and to make sure that the disk the database resides on has at least 20% of available space.

If your free space reaches a minimum of either 20% or 100 GB, the oldest collection of data will be deleted. This will continue to occur until either only two days of data or either 5% or 50 GB of available space remains, at which point data collection will stop working.

The storage latency for read and write activities should be below 10 ms.

The ratio between read and write activities is approximately 1:3 below 100,000 packets per second and 1:6 above 100,000 packets per second.

* + 1. ATA Lightweight Gateway

An ATA Lightweight Gateway is installed directly on the domain controller and monitors its traffic directly. It is recommended that you use an ATA Lightweight Gateway rather than an ATA Gateway whenever possible, as long as your domain controllers comply with the sizing table listed below. An ATA Lightweight Gateway can support the monitoring of one domain controller.

The following table provides some high-level suggestions regarding how to size domain controllers based on the amount of traffic being sent and received. More information about ATA sizing can be found in the TechNet article “[ATA Capacity Planning](https://technet.microsoft.com/en-us/library/mt429323.aspx).”

Table 2: Requirements – ATA Lightweight Gateway Sizing

| Packets Per Second\* | CPU (cores\*\*) | Memory (GB) |
| --- | --- | --- |
| 1,000 | 2 | 6 |
| 5,000 | 6 | 16 |
| 10,000 | 10 | 24 |

**\*** Total busy-hour average number of packets per second from the domain controllers that are being monitored by the specific ATA Lightweight Gateway

**\*\*** Hyperthreading must be disabled.

* + 1. ATA Gateway

An ATA gateway can support the monitoring of multiple domain controllers, depending on the amount of network traffic of the domain controllers being monitored. The following table provides some high-level suggestions regarding how to size your ATA gateway based on the amount of network traffic being sent and received. More information about ATA sizing can be found in the TechNet article “[ATA Capacity Planning](https://docs.microsoft.com/en-us/advanced-threat-analytics/plan-design/ata-capacity-planning).”

Table 2: Requirements – ATA Gateway Sizing

| Packets Per Second\* | CPU (cores\*\*) | Memory (GB)\*\*\* |
| --- | --- | --- |
| 1,000 | 1 | 6 |
| 5,000 | 2 | 10 |
| 10,000 | 3 | 12 |
| 20,000 | 6 | 24 |
| 50,000 | 16 | 48 |

**\*** Total busy-hour average number of packets per second from the domain controllers that are being monitored by the specific ATA Gateway. In addition, the total amount of domain controller port-mirrored traffic cannot exceed the capacity of the capture NIC on the ATA Gateway.

**\*\*** Total amount of non-hyper threaded cores that this domain controller has installed. While hyper-threading is acceptable for the ATA Lightweight Gateway, when planning for capacity, you should count actual cores and not hyperthreaded cores.

**\*\*\*** Total amount of memory that this domain controller has installed

* 1. Hardware Requirements
     1. ATA Center

The number of domain controllers that Customer Name are monitoring and the load on each of the domain controllers dictates the hardware requirements.

The following table outlines the base hardware requirements for the Center.

Table 3: Requirements – ATA Center Hardware

| Component | Center Hardware Requirements |
| --- | --- |
| Processor | Refer to sizing requirements |
| Memory | Refer to sizing requirements |
| Available disk space  Database storage | Refer to sizing requirements |
| Network | Communication between the ATA Center and the ATA Gateways is encrypted using the Secure Sockets Layer (SSL) on port 443. Additionally, the ATA Management console runs on Microsoft Internet Information Services (IIS) and security is enhanced using SSL on port 443. **Two IP addresses** are required. The ATA Center service will bind port 443 to the first IP address and IIS will bind port 443 to the second IP address. Also see the network ports requirements in the following table.  **Note:** Make sure there is a stable and effective network connection between the Center and the Gateway. See Gateway requirements for memory.  **Note:** Short-term lease subnets   * Identify the subnets in which IP addresses are reassigned between devices within a very short period of time (seconds or minutes). ATA reduces the cache lifetime for the IP addresses in these subnets to accommodate the fast reassignment between devices. Virtual private network (VPN) or wireless networks are common examples of short-term lease subnets. |
| Virtualization | Installation of the ATA Center as a virtual machine (VM) is supported. |
| BIOS | The ATA database requires that Customer Name DISABLE non-uniform memory access (NUMA) in the BIOS. Your system might refer to NUMA as Node Interleaving, in which case you will have to ENABLE Node Interleaving. |

* + 1. ATA Lightweight Gateway

An ATA Lightweight Gateway will support and monitor only the domain controller it is installed on.

Table 4: Requirements – ATA Lightweight Gateway Hardware

| Domain Controller Name | Packets per Second | CPU (Cores) | Memory (GB) |
| --- | --- | --- | --- |
| DCName | X,xxx | # CPU Cores | Installed Memory |

* + 1. ATA Gateway

An ATA gateway can support the monitoring of multiple domain controllers, depending on the amount of network traffic of the domain controllers being monitored.

Table 4: Requirements – ATA Gateway Hardware

| Component | Gateway Hardware Requirements |
| --- | --- |
| Processor | Refer to sizing requirements |
| Memory | Refer to sizing requirements  **Note:** The ATA Gateway uses its memory to buffer captured data and sends it to the Center. This is at a default setting of 1,000,000 entities and is configurable. Depending on the load of domain controller connected to the Gateway, this can generate a tremendous amount of data.  **Caution note:** If communication between the Center and the Gateway is disrupted, the Gateway will cache in memory. 1,000,000 entities can take up to 5 GB of memory. Once this limit is reached, it will stop collecting network traffic until communication is restored with the Center. This can be hours or minutes depending on the domain controller load. |
| Available disk space | Refer to sizing requirements |
| Network | The gateway requires two or more network adapters.  **Management adapter**: Will be used for communications on the company network. This adapter should be configured with the following:   * Static IP address including default gateway. * Preferred and alternate Domain Name System (DNS) servers. * “DNS suffix for this connection” should be the DNS name of the monitored domain.   **Capture adapter**: Will be used to capture traffic to and from the domain controllers.   * Configure port mirroring for the capture adapter as the destination of the domain controller network traffic. * Configure a static non-routable IP address for your environment with no default gateway and no DNS server addresses. For example, 1.1.1.1 /8. * This will make sure that the capture network adapter captures the maximum amount of traffic and that the management network adapter is used to send and receive the required network traffic.   **Note:** Short-term lease subnets  Identify the subnets in which IP addresses are reassigned between devices within a very short period of time (seconds or minutes). ATA reduces the cache lifetime for the IP addresses in these subnets to accommodate the fast reassignment between devices. VPN or wireless networks are common examples of short-term lease subnets. |
| Virtualization | Installation of the ATA Gateway as a VM is supported when the monitored domain controllers are also running as VMs on the same virtualization host.  **Important Note:** Do not install KB 3047154 on a virtualization host. This might cause port mirroring to stop working properly. |

* 1. Software Requirements
     1. ATA Center

This section provides the software requirements for the ATA Center.

Table 5: Requirements - Center Software

| Component | Center Software Requirements |
| --- | --- |
| Certificates | ATA Center requires certificates for the following services:   * IIS – web server certificate * ATA Center service – server authentication certificate |
| Operating system | Windows Server 2012 R2 Standard or Datacenter Editions  The ATA Center **CANNOT** be installed on a domain controller. |
| Domain or workgroup membership | The ATA Center can be installed on a server that is a member of a domain or workgroup.  It is highly recommended to distribute in a workgroup configuration. |
| User account | **Local administrator (non-domain joined)**  **Standard user account (domain joined):** Added to local administrator, ATA Administrators |
| Components | The following components are installed and configured during the installation of ATA Center:   * IIS * MongoDB * ATA Center service and ATA Management IIS site * Custom Performance Monitor data collection set * X.509 certificate will be recommended and issued by an internal public key infrastructure. Self-signed is only recommended for testing purposes. |
| Browser support | Access to the ATA Management console is through a browser. The following browsers are supported:   * Internet Explorer version 10 * Google Chrome 40 * Minimum screen width resolution of 1700 pixels |
| Microsoft updates | Make sure that Microsoft updates have been installed on the server.  Install [KB 2934520](https://support.microsoft.com/en-us/kb/2934520) as a prerequisite. |

* + 1. ATA Lightweight Gateway

This section provides the software requirements for the ATA Lightweight Gateway.

Table 6: Requirements - Gateway Software

| Component | ATA Lightweight Gateway Software Requirements |
| --- | --- |
| Certificates | ATA Lightweight Gateway requires certificates for the following services:   * A certificate supporting **Server Authentication** is required to be installed in the computer store of the ATA Gateway in the local computer store. This certificate must be trusted by the ATA Center. |
| Operating System | The ATA Lightweight Gateway supports installation on a domain controller running Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2.  The domain controller can be a read-only domain controller (RODC).  The domain controller cannot be running Server Core. |
| User Accounts | **Standard service account**: Used to query Active Directory for indexing and object or entity cataloguing. (Domain connectivity)  **Honeytoken account**: Use a security identifier (SID) (optional): A honeytoken account is a user who has no network activities. This account will be configured as the ATA honeytoken user. To configure the honeytoken user you will need the SID of the user account, not the username.  **Optional:** The standard service account should have read-only permissions on the Deleted Objects container. This will allow ATA to detect bulk deletion of objects in the domain. For information about configuring read-only permissions on the Deleted Objects container, see the **Changing permissions on a deleted object container** section in the [View or Set Permissions on a Directory Object](https://technet.microsoft.com/library/cc816824(v=ws.10).aspx) topic. |
| Components | The following components are installed and configured during the installation of ATA Gateway:   * ATA Lightweight Gateway service * Microsoft Visual C++ 2013 Redistributable * Custom Performance Monitor data collection set |
| Microsoft updates | Run Windows Update and make sure **Important** updates have been installed. |
| Network sniffers | Do not install Message Analyzer, Wireshark, or other network capture software on the ATA Lightweight Gateway. If you need to capture network traffic, install and use Microsoft Network Monitor 3.4. |

* + 1. ATA Gateway

This section provides the software requirements for the ATA Gateway.

Table 6: Requirements - Gateway Software

| Component | ATA Gateway Software Requirements |
| --- | --- |
| Certificates | ATA Gateway requires certificates for the following services:   * A certificate supporting **Server Authentication** is required to be installed in the computer store of the ATA Gateway in the local computer store. This certificate must be trusted by the ATA Center. |
| Operating system | Windows Server 2012 R2 Standard or Datacenter Editions |
| Domain/workgroup membership | The ATA Gateway can be installed on a server that is a member of a domain or workgroup.  Distributing in a workgroup configuration is highly recommended. |
| User accounts | **Local administrator (non-domain joined)**  **Standard user account (domain joined)**: Added to local administrator, ATA Administrators  **Standard service account**: Used to query Active Directory for indexing and object or entity cataloguing. (Domain connectivity)  **Honeytoken account**: Use a security identifier (SID) (optional) – A honeytoken account is a user who has no network activities. This account will be configured as the ATA honeytoken user. To configure the honeytoken user you will need the SID of the user account, not the username.  **Optional:** The standard service account should have read-only permissions on the Deleted Objects container. This will allow ATA to detect bulk deletion of objects in the domain. For information about configuring read-only permissions on the Deleted Objects container, see the **Changing permissions on a deleted object container** section in the [View or Set Permissions on a Directory Object](https://technet.microsoft.com/library/cc816824(v=ws.10).aspx) topic. |
| Components | The following components are installed and configured during the installation of ATA Gateway:   * KB 3047154 (Do not install KB 3047154 on a virtualization host. This might cause port mirroring to stop working properly.) * ATA Gateway service * Microsoft Visual C++ 2013 Redistributable * Custom Performance Monitor data collection set |
| Microsoft updates | Run Windows Update and make sure **Important** updates have been installed. Before installing ATA Gateway confirm that the following update has been installed, [KB 2919355](https://support.microsoft.com/en-us/kb/2919355/). If the update is not installed, install the update before installing the ATA Gateway service.  Install [KB 2934520](https://support.microsoft.com/en-us/kb/2934520) as a prerequisite. |
| Network sniffers | Do not install Message Analyzer, Wireshark, or other network capture software on the ATA Gateway. If you need to capture network traffic, install and use Microsoft Network Monitor 3.4. |

* 1. Pre-deployment Requirements

1. According to the previous software requirements section, validate that knowledge base article [KB 2934520](https://support.microsoft.com/en-us/kb/2934520) is installed on the ATA Center server and on the ATA Gateway servers before beginning installation. Otherwise the ATA installation will install this update and will require a restart in the middle of the ATA installation.
2. On the ATA Gateway, make sure that [KB 2919355](http://support.microsoft.com/kb/2919355/) has been installed. Run the following PowerShell cmdlet to check if the hotfix is installed: Get-HotFix -Id kb2919355.
3. See the appendix of this document for additional information on configuring port mirroring. The deployment section of this document assumes that port mirroring has been configured and is operational.
4. To validate port mirroring, see the ATAIS-Operations Guide as part of this engagement.
5. Deployment

The following section outlines the installation steps followed to distribute ATA within Customer Name.

* 1. Step 1: Installing the ATA Center

After you have verified that the server meets the requirements, the administrator can proceed with the installation of the ATA Center.

1. Log on to the Center server with a user who is a member of the local administrators group.
2. From an elevated command prompt, run Microsoft ATA Center Setup.EXE and follow the setup wizard.
3. On the **Welcome** page, select your language and click **Next**.
4. Read the End User License Agreement and if you accept the terms, click **Next**.
5. On the **Center Configuration** page, enter the following information based on the Solutions Design Document.

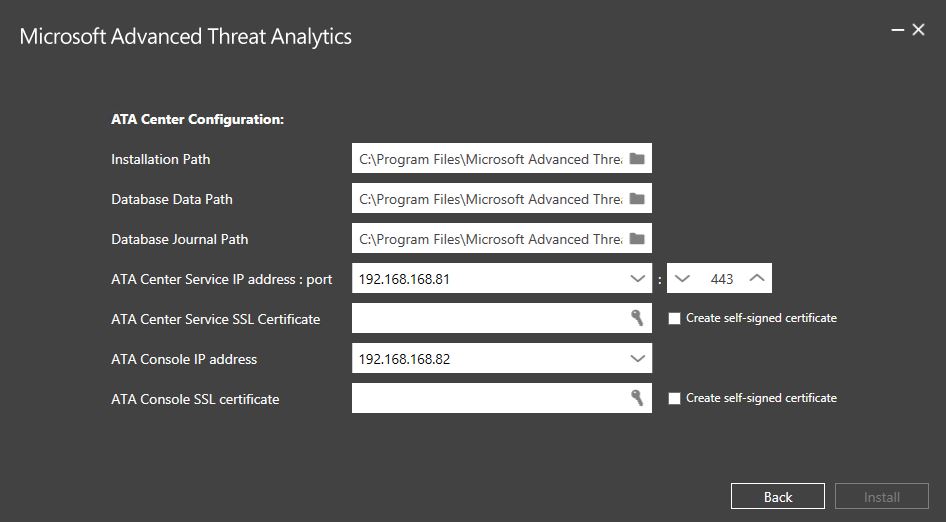
**Instructions:** Update the following table to record the customer specific installation configuration. This will include certificate information, network ports, or default install locations if they are modified discussed during the design phase. Remove the highlights if default is not changed.

Table 7: ATA Center - Installation Configuration

| Field | Description | Comments |
| --- | --- | --- |
| Installation path | This is the location where the ATA Center will be installed. By default, this is %programfiles%\Microsoft Advanced Threat Analytics\Center | Leave the default value |
| Database data path | This is the location where the MongoDB database files will be located. By default, this is %programfiles%\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\data | Change the location to a place where you have room to grow based on your sizing.   |  | | --- | | System_CAPS_noteNote | | In production environments the administrator should use a drive that has enough space based on capacity planning.  For large deployments the database should be on a separate physical disk; this is to enhance performance. | |
| Database journal path | This is the location where the database journal files will be located. By default, this is %programfiles%\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\data\journal | For large deployments, the database journal should be on a separate physical disk from the database and the system drive. Change the location to a place where you have room for your database journal. |
| ATA Center Service IP address: Port | This is the IP address that the ATA Center service will listen on for communication from the ATA Gateways.  Default port: 443 | Click the down arrow to select the IP address to be used by the ATA Center service.  The IP address and port of the ATA Center service cannot be the same as the IP address and port of the ATA Console. Make sure to change the port of the ATA Console. |
| ATA Center Service SSL certificate | This is the certificate that will be used by the ATA Center service. | Click the key icon to select a certificate installed or check the self-signed certificate when distributing in a lab environment. |
| ATA Console IP address | This is the IP address that will be used by IIS for the ATA Console. | Click the down arrow to select the IP address used by the ATA Console.   |  | | --- | | System_CAPS_noteNote | | Make a note of this IP address to make it easier to access the ATA Console from the ATA Gateway. | |
| ATA Console SSL certificate | This is the certificate to be used by IIS. | Click the key icon to select a certificate installed or check the self-signed certificate when distributing in a lab environment. |

See the following example:

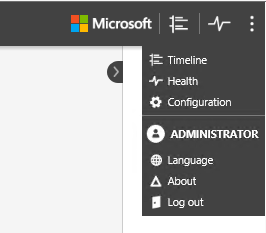
Figure 1: ATA Center - Installation Configuration



1. Click **Install** to install ATA and its components and create the connection between the ATA Center and the ATA Console.
2. When the installation completes, click **Launch** to connect to the ATA Console.
   * 1. Validating the Installation of the Center
3. Verify that the Microsoft ATA Center service is running by activating Services.msc on the **Windows Start Icon** and select **Run**.
4. On the desktop click the Microsoft ATA shortcut to connect to the ATA Console. Log on with the same user credentials that you used to install the ATA Center. The first time you log on to the ATA Console you will be brought automatically to the **Domain connectivity settings** page to continue the configuration and the deployment of the ATA Gateways.
5. Review the error file in the **Microsoft.Tri.Center-Errors.log** file which can be found in the following default location: %programfiles%\Microsoft Advanced Threat Analytics\Center\Logs.
   1. Step 2: Configure ATA Gateway Domain Connectivity Settings

The settings in the domain connectivity settings section apply to the ATA Gateways managed by the ATA Center.

1. Open the ATA Console and log on.
2. The first time you log on to the ATA Console after the ATA Center has been installed, you will automatically be taken to the ATA Gateways configuration page. If you need to modify the settings afterwards, click the Settings icon and select **Configuration**.



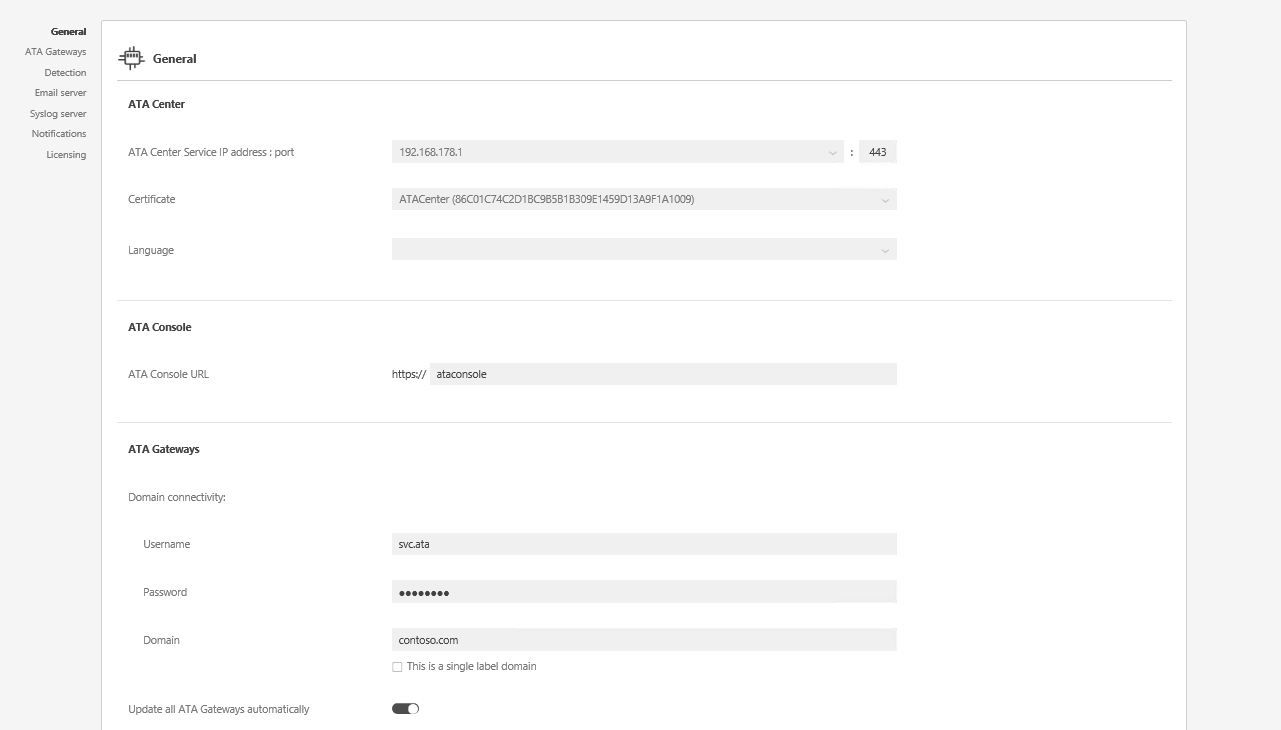
On the **Gateways** page, click on **Domain connectivity settings**, enter the following information and click **Save**.

Table 8: ATA Gateway - Domain Connectivity Settings

| Field | Comments |
| --- | --- |
| Username (required) | Enter the read-only username discussed during the solutions design. |
| Password (required) | Enter the password for the read-only user.   |  | | --- | | System_CAPS_note**Note** | | Make sure this password is correct. If you save the wrong password, the ATA Service will stop running on the ATA Gateway servers. | |
| Domain (required) | Enter the domain for the read-only user, for example, **contoso.com**.   |  | | --- | | System_CAPS_note**Note** | | It is important that you enter the complete fully qualified domain name (FQDN) of the domain where the user is located. For example, if the user’s account is in domain corp.contoso.com, you need to enter corp.contoso.com not contoso.com | |

See the following example:

Figure 2: ATA Gateway - Domain Connectivity Settings



* 1. Step 3: Download the ATA Gateway Setup Package

After configuring the domain connectivity settings, the administrator can download the ATA Gateway setup package.

1. Log on to the Gateway server.
2. On the ATA Gateway machine, open a browser and enter the IP address you configured in the ATA Center for the ATA Console. When the ATA Console opens, click on the settings icon and select **Configuration**.
3. In the **ATA Gateways** tab, click **Download ATA Gateway Setup**.
4. Save the package locally.

The .zip file includes the following:

* ATA Gateway installer
* Configuration setting file with the required information to connect to the ATA Center
  1. Step 4: Install the ATA Gateways
     1. Install the ATA Lightweight Gateway

The ATA Lightweight Gateway is installed directly on the domain controller it will be monitoring. Perform these steps on a domain controller.

1. Extract the files from the .zip file.
2. From an elevated command prompt, run Microsoft ATA Gateway Setup.exe and follow the setup wizard.
3. On the **Welcome** page, select your language and click **Next**.
4. In the Deployment type wizard, only the ATA Lightweight Gateway option is displayed, click **Next**.
5. Under **ATA Gateway Configuration**, enter the following information based on your environment:

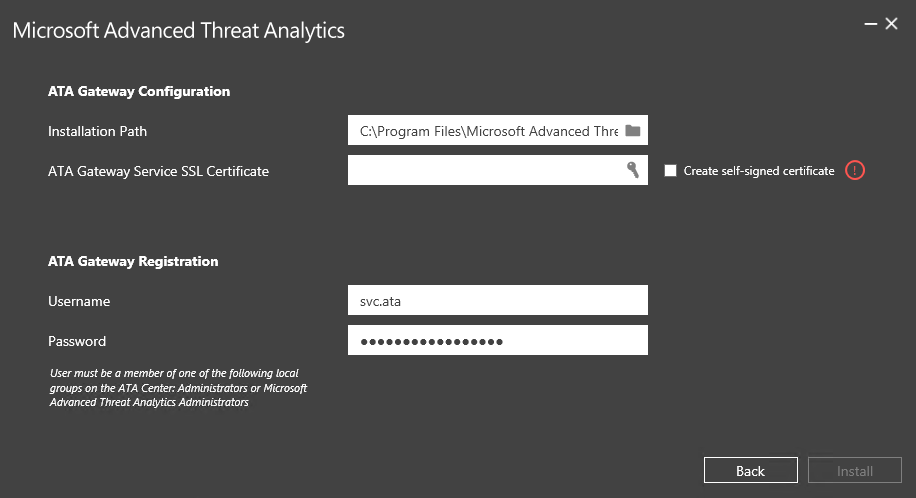
**Instructions:** Update the following table to record the customer specific installation configuration. This will include certificate information and default install locations if they are modified discussed during the design phase. Remove the highlights if default is not changed.

Table 9: ATA Lightweight Gateway - Installation Configuration

| Field | Description | Comments |
| --- | --- | --- |
| Installation path | This is the location where the ATA Gateway will be installed. By default this is %programfiles%\Microsoft Advanced Threat Analytics\Gateway | Leave the default value. |
| ATA Gateway Service SSL certificate | This is the certificate that will be used by the ATA Gateway. | Use a self-signed certificate for lab environments only. |
| ATA Gateway registration | Enter the username and password of the ATA administrator. | For the ATA Gateway to register with the ATA Center, enter the username and password of the user who installed the ATA Center. This user must be a member of one of the following local groups on the ATA Center.   * Administrators * ATA administrators  |  | | --- | | System_CAPS_note**Note** | | These credentials are used only for registration and are not stored in ATA. | |

See the following example:

Figure 3: ATA Lightweight Gateway - Installation Configuration



1. After the installation completes, click **Finish.**
2. From another machine, open your browser and log on to the ATA Console.
   * 1. Install the ATA Gateway

Before installing the ATA Gateway, validate that port mirroring is properly configured and that the ATA Gateway can see traffic to and from the domain controllers that will be monitored by each ATA Gateway. See the Operations Guide document as part of this engagement to verify port mirroring.

1. Extract the files from the .zip file.
2. From an elevated command prompt, run Microsoft ATA Gateway Setup.exe and follow the setup wizard.
3. On the **Welcome** page, select your language and click **Next**.
4. Under **ATA Gateway Configuration**, enter the following information based on your environment:

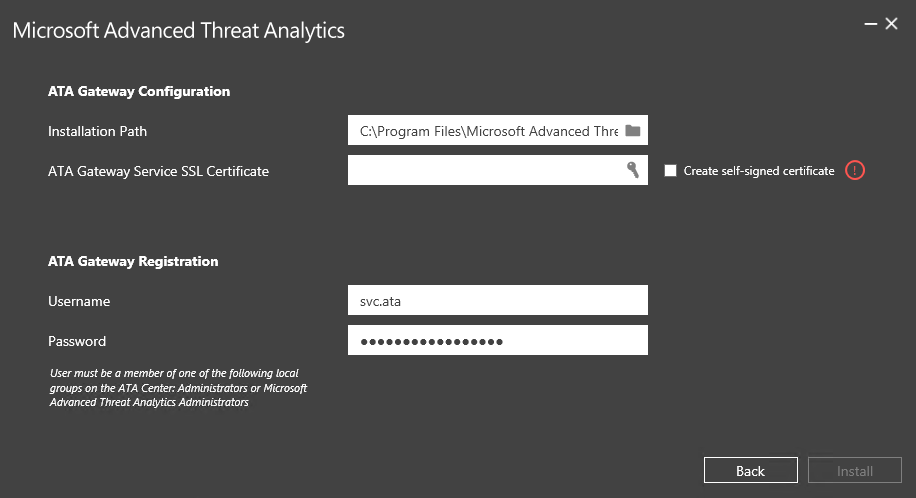
**Instructions:** Update the following table to record the customer specific installation configuration. This will include certificate information and default install locations if they are modified discussed during the design phase. Remove the highlights if default is not changed.

Table 9: ATA Gateway - Installation Configuration

| Field | Description | Comments |
| --- | --- | --- |
| Installation path | This is the location where the ATA Gateway will be installed. By default, this is %programfiles%\Microsoft Advanced Threat Analytics\Gateway | Leave the default value. |
| ATA Gateway Service SSL certificate | This is the certificate that will be used by the ATA Gateway. | Use a self-signed certificate for lab environments only. |
| ATA Gateway registration | Enter the username and password of the ATA administrator. | For the ATA Gateway to register with the ATA Center, enter the username and password of the user who installed the ATA Center. This user must be a member of one of the following local groups on the ATA Center.   * Administrators * ATA administrators  |  | | --- | | System_CAPS_note**Note** | | These credentials are used only for registration and are not stored in ATA. | |

See the following example:

Figure 3: ATA Gateway - Installation Configuration



1. After the installation completes, click **Launch** to open your browser and log on to the ATA Console.
   1. Step 5: Configure the ATA Gateways
      1. Configure the ATA Lightweight Gateway

After the ATA Lightweight Gateway is installed, perform the following steps to configure the settings for the ATA Lightweight Gateway.

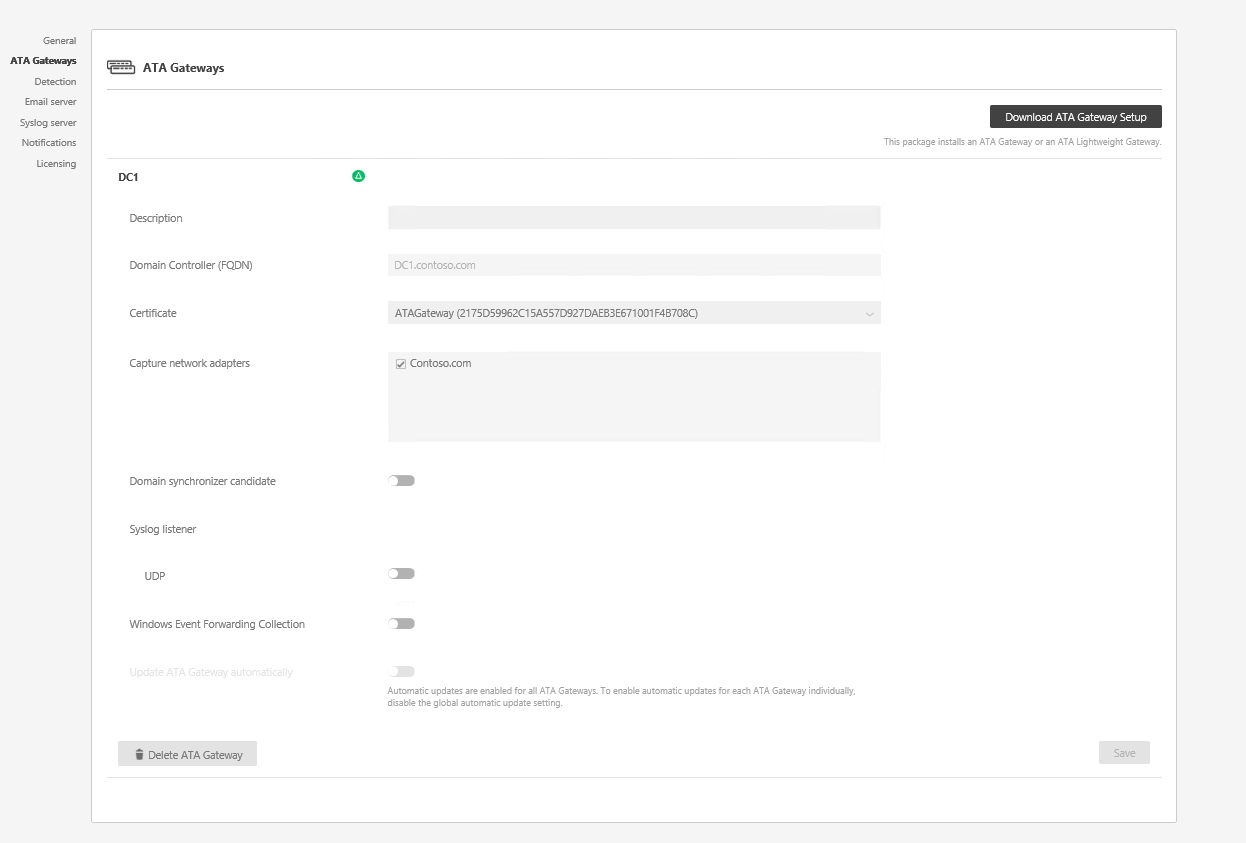
1. On the ATA Gateway machine, in the ATA Console, click the **Configuration** and select the **ATA Gateways** page
2. Enter the following information:

Table 10: ATA Gateway – Post-Installation Configuration

| Field | Description | Comments |
| --- | --- | --- |
| Description | Enter a description of the ATA Gateway (optional). |  |
| Domain controllers (required)  For additional information about the list of controllers, see the following. | The FQDN of your domain controller is already populated |  |
| Capture network adapters (required) | By default, all network adapters are selected |  |

See the following example:

Figure 4: ATA Lightweight Gateway – Post-Installation Configuration



1. By default, ATA Lightweight Gateways are not Domain Synchronizer candidates as they are typically deployed in branch sites and on small domain controllers. If this ATA Lightweight Gateway is to be a domain synchronizer, select the option, and click **Save**.
2. The configuration changes will be applied to the ATA Gateway on the next scheduled sync between the ATA Gateway and the ATA Center.
   * 1. Configure the ATA Gateway

After the ATA Gateway is installed, perform the following steps to configure the settings for the ATA Gateway.

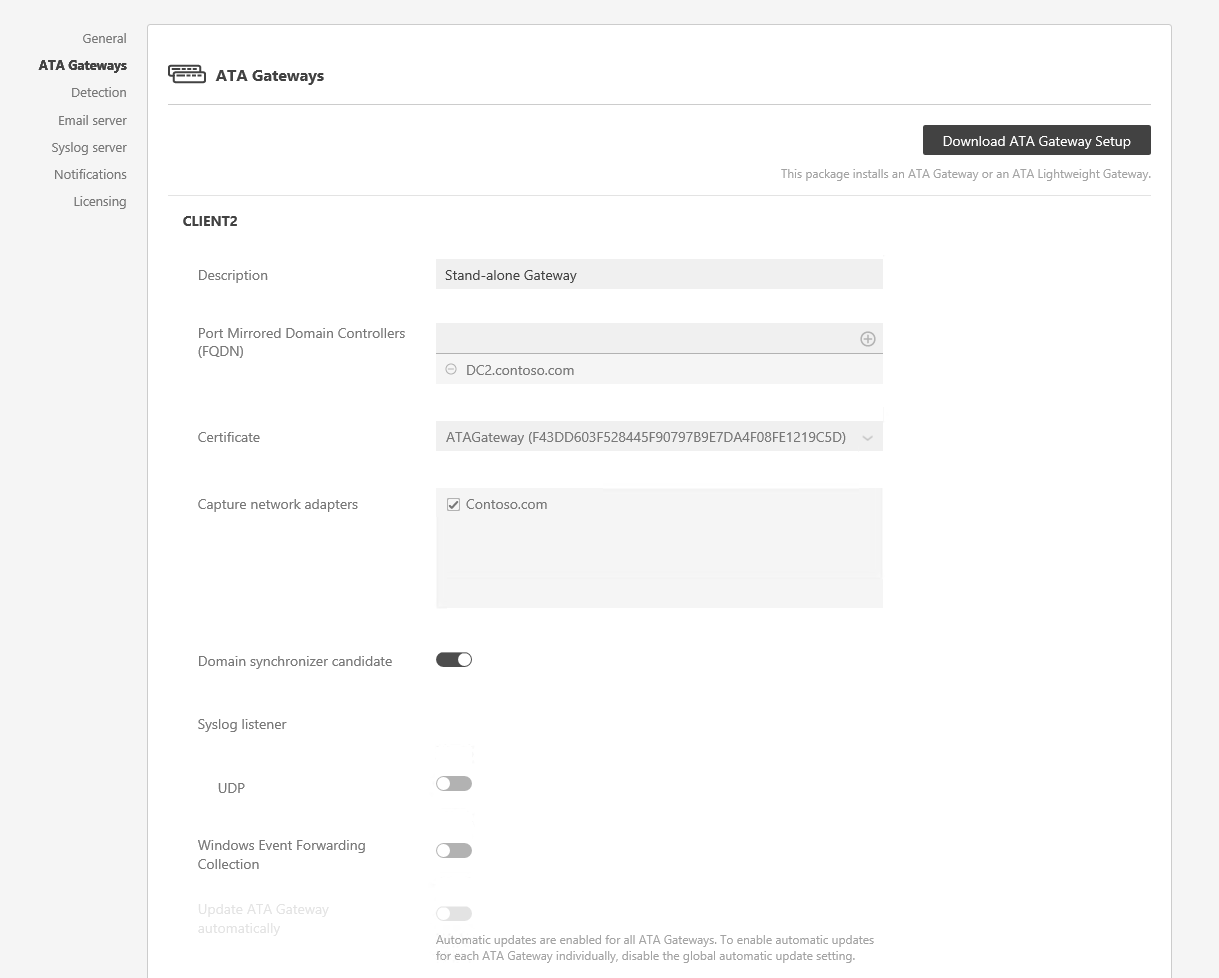
1. On the ATA Gateway machine, in the ATA Console, click on the **Configuration** and select the **ATA Gateways** page.
2. Enter the following information.

Table 10: ATA Gateway – Post-Installation Configuration

| Field | Description | Comments |
| --- | --- | --- |
| Description | Enter a description of the ATA Gateway (optional). |  |
| Domain controllers (required)  For additional information about the list of controllers, see the following. | Enter the complete FQDN of your domain controller and click the plus sign to add it to the list. For example, **dc01.contoso.com** | The objects in the first domain controller in the list will sync with the Lightweight Directory Access Protocol (LDAP) queries. Depending on the size of the domain, this might take some time.   |  | | --- | | System_CAPS_note**Note** | | Make sure that the first domain controller is **not** an RODC.  RODCs should be added only after the initial sync completes. | |
| Capture network adapters (required) | Select the network adapters that are connected to the switch that are configured as the destination mirror port to receive the domain controller traffic. | Select the Capture network adapter. |

See the following example:

Figure 4: ATA Gateway – Post-Installation Configuration



1. Click **Save**.
2. It takes a few minutes for the ATA Gateway service to start the first time because it builds the cache of the network capture parsers used by the ATA Gateway.
3. The configuration changes will be applied to the ATA Gateway on the next scheduled sync between the ATA Gateway and the ATA Center.

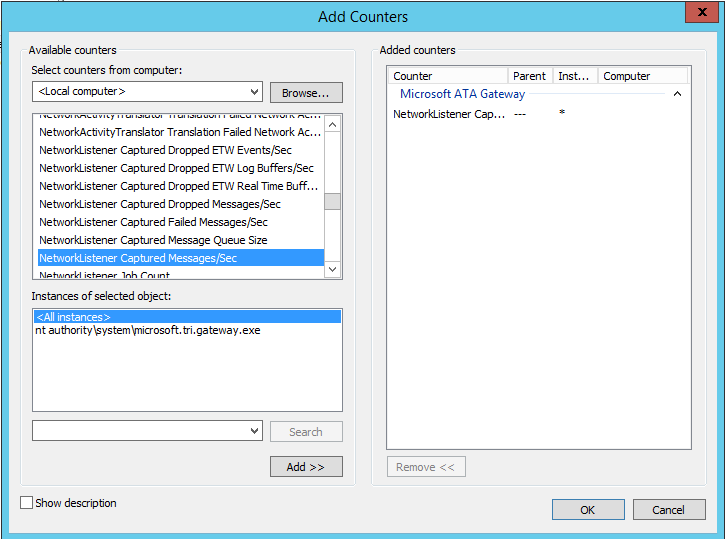
The following information applies to the servers you enter in the **domain controllers** list:

* The first domain controller in the list will be used by the ATA Gateway to sync the objects in the domain through LDAP queries. Depending on the size of the domain, this might take some time.
* The domain controllers, whose traffic is being monitored through port mirroring by the ATA Gateway, must be listed in the **domain controllers** list. If a domain controller is not listed in the **domain controllers** list, detection of suspicious activities might not function as expected.
* Make sure that the first domain controller is **not** an RODC.
* RODCs should be added only after the initial sync completes.
* At least one domain controller in the list must be a global catalog server. This will facilitate ATA to resolve computer and user objects in other domains in the forest.
  + 1. Validating the ATA Gateway Installation

To validate that the ATA Gateway has been successfully distributed, verify the following:

1. Check that the ATA Gateway service is running. After you have saved the ATA Gateway settings, it might take a few minutes for the service to start.
2. If the service does not start, review the “Microsoft.Tri.Gateway-Errors.log” file located in the following default folder:   
   “%programfiles%\Microsoft Advanced Threat Analytics\Gateway\Logs”   
   Search for entries with “transfer” or “service start.”
3. Check the following ATA Gateway performance counters:
   1. **NetworkListener Captured Messages / sec**: This counter tracks how many messages are being captured by the ATA per second. The value should be from the middle hundreds to thousands depending on the number of domain controllers being monitored and how busy each domain controller is. Single or double-digit values can indicate an issue with the port-mirroring configuration.
   2. **EntityTransfer Activity Transfers/Sec**: This value should be in the range of a few hundred every few seconds.
4. If this is the first ATA Gateway installed, after a few minutes, log on to the ATA Console and open the notification pane by swiping the right side of the screen open. You should see a list of **Entities Recently Learned** in the notification bar on the right side of the console.
5. In the console, search for something in the search bar, such as a user or a group on your domain.
6. Open Performance Monitor. In the Performance tree, click on **Performance Monitor** and then click the plus sign to **Add a Counter**. Expand **Microsoft ATA Gateway** and scroll down to **Network Listener Captured Messages per Second** and add it. Then, make sure you see activity on the graph.

Figure 5: Performance Monitor - Adding Counters



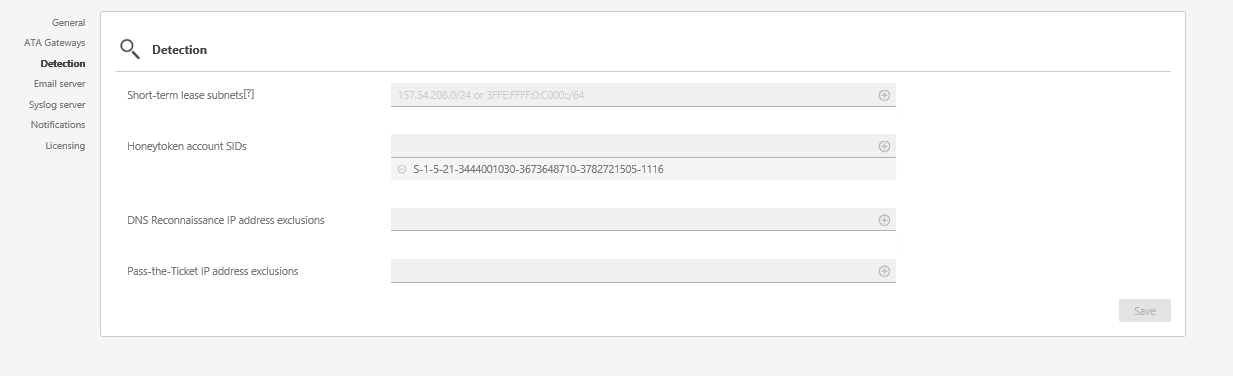
* 1. Step 6: Configure Short-Term Lease Subnets

Short-term lease subnets are subnets in which the IP address assignment changes very rapidly—within seconds or minutes. For example, IP addresses used for your VPNs and wireless IP addresses.

To enter the list of short-term lease subnets used in your organization, follow these steps:

1. From the ATA Console on the ATA Gateway machine, click on the settings icon and select **Configuration**.
2. Under **Detection**, enter the following for short-term lease subnets. Enter the short-term lease subnets using slash notation format, for example, 192.168.0.0/24, and click the plus sign.
3. Configure exclusions: You can configure IP addresses to be excluded from specific suspicious activities.
   1. Step 7: Configure the Honeytoken User
4. From the ATA Console on the ATA Gateway machine, click on the settings option and select **Configuration**.
5. Under **Detection**, enter the honeytoken user information:
   1. For the honeytoken account SIDs, enter the SID for the user account that will have no network activity, and click the plus sign. For example: S-1-5-21-72081277-1610778489-2625714895-10511.
   2. To find the SID for a user, run the following Windows PowerShell cmdlet -> Get-ADUser UserName –Properties.

Figure 6: ATA Detection Configuration



* 1. Step 8: Post-Installation Information

Monitor the attack timeline to view detected suspicious activities, search for users or computers, and view their profiles.

It takes up to 30 days for ATA to build behavioral profiles for the environment. As ATA continues to learn the environment, it might begin to detect suspicious behavioral activities. Each of these activities should be researched accordingly.

1. Appendix
   1. Configure Port Mirroring

The main data source used by ATA is deep-packet inspection of the network traffic to and from Customer Name’s domain controllers.

For ATA to see the network traffic, port mirroring needs to be configured. Port mirroring copies the traffic on one port, known as the source port, to another port, known as the destination port. ATA works with many solutions that can mirror traffic—if the traffic can be port mirrored to ATA, it can be used to analyze threats to your system. To configure port mirroring, refer to Customer Name vendor's documentation.

Customer Name’s domain controllers and ATA Gateways can be either physical or virtual based on the solutions design.

The following are common methods for port mirroring and some considerations. Customer Name needs to refer to their switch or virtualization server product documentation for additional information. Your switch manufacturer might use different terminology.

* **Switched Port Analyzer (SPAN)**: Copies network traffic from one or more switch ports to another switch port on the same switch. Both the ATA Gateway and domain controllers must be connected to the same physical switch.
* **Remote Switch Port Analyzer (RSPAN)**: The use can monitor network traffic from source ports distributed over multiple physical switches. RSPAN copies the source traffic into a special RSPAN configured VLAN. This VLAN needs to be trunked to the other switches involved. RSPAN works at Layer 2.
* **Encapsulated Remote Switch Port Analyzer (ERSPAN)**: Is a Cisco-proprietary technology working at Layer 3. With ERSPAN the user can monitor traffic across switches without the need for VLAN trunks. ERSPAN uses generic routing encapsulation to copy monitored network traffic. ATA currently cannot directly receive ERSPAN traffic. For ATA to work with ERSPAN traffic, a switch or router that can decapsulate the traffic needs to be configured as the destination of ERSPAN where the traffic will be decapsulated. The switch or router will then need to be configured to forward it to the ATA Gateway using either SPAN or RSPAN.
  + 1. Supported Port Mirroring Options

Table 11: Port Mirroring Options

|  |  |  |
| --- | --- | --- |
| ATA Gateway | Domain Controller | Considerations |
| Virtual | Virtual on same host | The virtual switch needs to support port mirroring.  Moving one of the VMs to another host by itself might break the port mirroring. |
| Virtual | Virtual on different hosts | Make sure your virtual switch supports this scenario. |
| Virtual | Physical | Requires a dedicated network adapter otherwise ATA will see the traffic coming in and out of the host, even the traffic it sends to the ATA Center. |
| Physical | Virtual | Make sure your virtual switch supports this scenario—and port mirroring configuration on your physical switches based on the scenario:   * If the virtual host is on the same physical switch, you will need to configure a switch level span. * If the virtual host is on a different switch, you will need to configure RSPAN or ERSPAN\*. |
| Physical | Physical on the same switch | Physical switch must support SPAN/port mirroring. |
| Physical | Physical on a different switch | Requires physical switches to support RSPAN or ERSPAN\*. |

\* ERSPAN is only supported when decapsulation is performed before the traffic is analyzed by ATA.

* + 1. Hyper-V Virtual Switch – Windows Server 2012

With port mirroring, traffic sent to or from a Hyper-V Virtual Switch port is copied and sent to a mirror port. There are a range of applications for port mirroring—an entire ecosystem of network visibility companies exists that have products designed to consume port mirror data for performance management, security analysis, and network diagnostics. With Hyper-V Virtual Switch port mirroring, you can select the switch ports that are monitored as well as the switch port that receives copies of the traffic.

The following examples configure port mirroring so that the traffic that is sent and received by both MyVM and MyVM2 is also sent to the VM named MonitorVM.

Set-VMNetworkAdapter –VMName MyVM –PortMirroring Source

Set-VMNetworkAdapter –VMName MyVM2 –PortMirroring Source

Set-VMNetworkAdapter –VMName MonitorVM –PortMirroring Destination

Also see <http://blogs.technet.com/b/networking/archive/2015/01/06/setting-up-port-mirroring-to-capture-mirrored-traffic-on-a-hyper-v-virtual-machine.aspx>

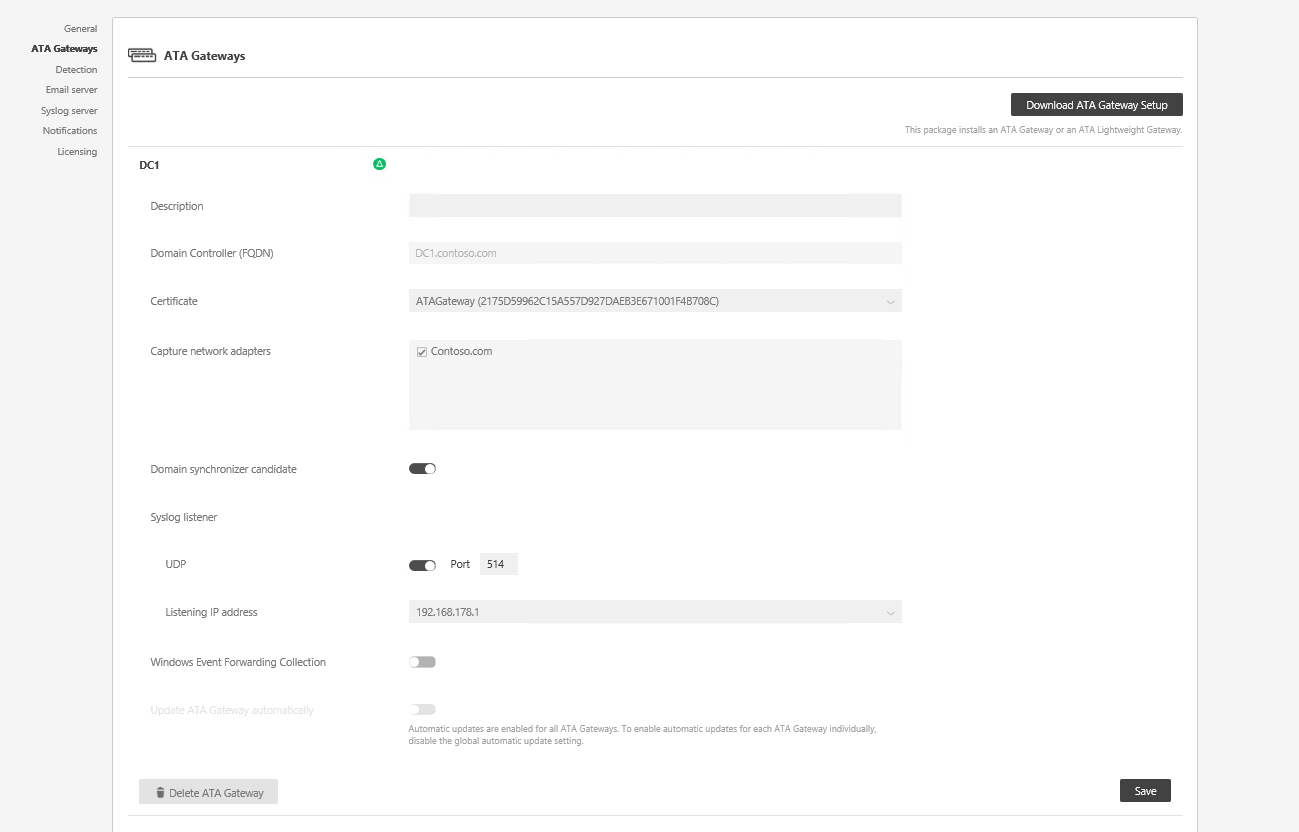
* 1. Configuring Security Information and Event Management (SIEM) Integration

To enhance ATA detection of Pass the Hash (PtH), ATA needs Windows Event log ID 4776. This can be forwarded to the ATA Gateway in one of two ways—by configuring the ATA Gateway to listen for SIEM events or by using Windows Event Forwarding (WEF).

* + 1. Configuring the ATA Gateway to Listen for and Accept SIEM Events

1. On the ATA Gateway configuration, activate **Syslog Listener UDP**.

Set the Listening IP Address as described in the following figure. The default port is 514.



Customer Name needs to configure their SIEM or Syslog server to forward Windows Event ID 4776 to the IP address selected in the previous figure. For additional information on configuring your SIEM, refer to the SIEM online help or technical support options for specific formatting requirements for each SIEM server.

* + 1. Supported SIEM Solutions

To view the supported SIEM solutions, see <https://technet.microsoft.com/en-us/library/dn707705.aspx>.

* 1. Configuring Windows Event Forwarding (WEF)

If Customer Name does not have a SIEM server, the administrator can configure Customer Name’s domain controllers to forward Windows Event ID 4776 directly to one of your ATA Gateways.

**NOTE:** These same steps must be completed for the Lightweight Gateway as well.

The following section is informational and is out-of-scope of this engagement.

1. On the ATA Gateway configuration, activate **Windows Event Forwarding Collection**.
2. When the administrator activates this setting the ATA Gateway will look in the Forwarded Events log for Windows Events that have been forwarded to it from the domain controllers.
3. Configure the domain controllers to forward Windows Event ID 4776 to the ATA Gateways. For additional information on Windows Event Forwarding, see [Configure Computers to Forward and Collect Events](https://technet.microsoft.com/en-us/library/cc748890).