



# How to Deploy a Successful ATA POC?

Learn how to quickly implement Microsoft Advanced Threat Analytics in your environment.

*Prepared by*

**Yoann Mallet**

Sr Program Manager

C+E Security Customer Experience Team

*Contributor*

**Gershon Levitz**

Sr Program Manager

C+E Security Customer Experience Team

*Version 1.0*

## Content

Content .....	2
Training and Community Resources .....	3
What is Advanced Threat Analytics?.....	4
Overview .....	4
Architecture .....	4
ATA Gateways .....	4
ATA Center .....	4
POC Introduction .....	5
Deployment Environment.....	5
POC Implementation Phases.....	6
Planning and Design.....	6
Capacity Planning.....	6
Choosing the right Gateway type .....	6
Domain Membership .....	7
Event collection.....	8
Deploying .....	9
Prerequisites .....	10
Network requirements.....	10
Software requirements .....	10
POC Building blocks.....	10
Before you get started .....	10
General prerequisites .....	10
Prerequisites for Full Gateway deployment .....	11
Prerequisites for Lightweight Gateway Deployment.....	11
ATA Center Installation .....	11
Silent Installation .....	13
ATA Gateway Deployment.....	13
Basic installation .....	13
Silent and mass Deployment .....	15
Note on port mirroring .....	15

Validating deployment.....	15
ATA Configuration.....	17
Detection.....	17
Notifications.....	18
SSL Certificate Configuration .....	18
Licensing.....	19
Event Collection .....	20
Report Generation .....	21

## Training and Community Resources

[aka.ms/SecurityCommunity](http://aka.ms/SecurityCommunity)

<http://aka.ms/ataplaybook>

<http://aka.ms/atadocs>

(c) 2017 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

## What is Advanced Threat Analytics?

### Overview

Advanced Threat Analytics (ATA) is a platform that helps protect your enterprise from multiple types of advanced targeted cyber attacks and insider threats. It uses information from multiple data-sources in your network to learn the behavior of users and other entities in the organization and build a behavioral profile about them. It also leverages ATA's proprietary network parsing engine to capture and parse network traffic of multiple protocols. ATA will detect and alert IT and Security Operation Center (SOC) of post-infiltration activities, from internal reconnaissance to compromised credentials, including lateral movement, privilege escalation and domain dominance.

It uses the following three data sources

- Network traffic, to and from the Active Directory Domain controllers
- Active Directory itself
- Events from domain controllers

### Architecture

#### ATA Gateways

In order to provide a high level of visibility over the environment, ATA uses a number of Gateways that will monitor traffic going to and coming from Active Directory Domain Controllers.

The Gateways perform deep packet inspection (layer 7), extracting the required information, resolves the IP address to a computer object in the domain, and then sending the data to the ATA Center.

There are two versions of the Gateway, that can be deployed in any combination.

- Full Gateway: A dedicated machine that will receive the network traffic using port mirroring (configured at the network switch or virtualization layer).
- Lightweight Gateway: Gateway service that is directly installed on the Domain Controller, receiving and analyzing local traffic only. This option doesn't require a dedicated machine.

In addition to that, ATA will also collect some of the security events, and gather them using Syslog forwarding or Windows Event Forwarding to one of the Gateways (Lightweight Gateways collect events automatically).

#### ATA Center

The ATA Center performs the following functions:

- Manages ATA Gateways' configuration settings
- Receives data from ATA Gateways and ATA Lightweight Gateways
- Runs ATA behavioral machine learning algorithms to detect abnormal behavior
- Runs various deterministic algorithms to detect advanced attacks based on the attack kill chain
- Runs the ATA Console
- The ATA Center can be configured to send emails and events when a suspicious activity is detected

The ATA Center receives parsed traffic from the ATA Gateway and ATA Lightweight Gateway, performs profiling, runs deterministic detection and runs machine learning and behavioral algorithms to learn about your network to enable detection of anomalies and alert you of suspicious activities. One ATA Center can monitor a single Active Directory forest. If you have more than one Active Directory forest you will need one ATA Center per Active Directory forest.

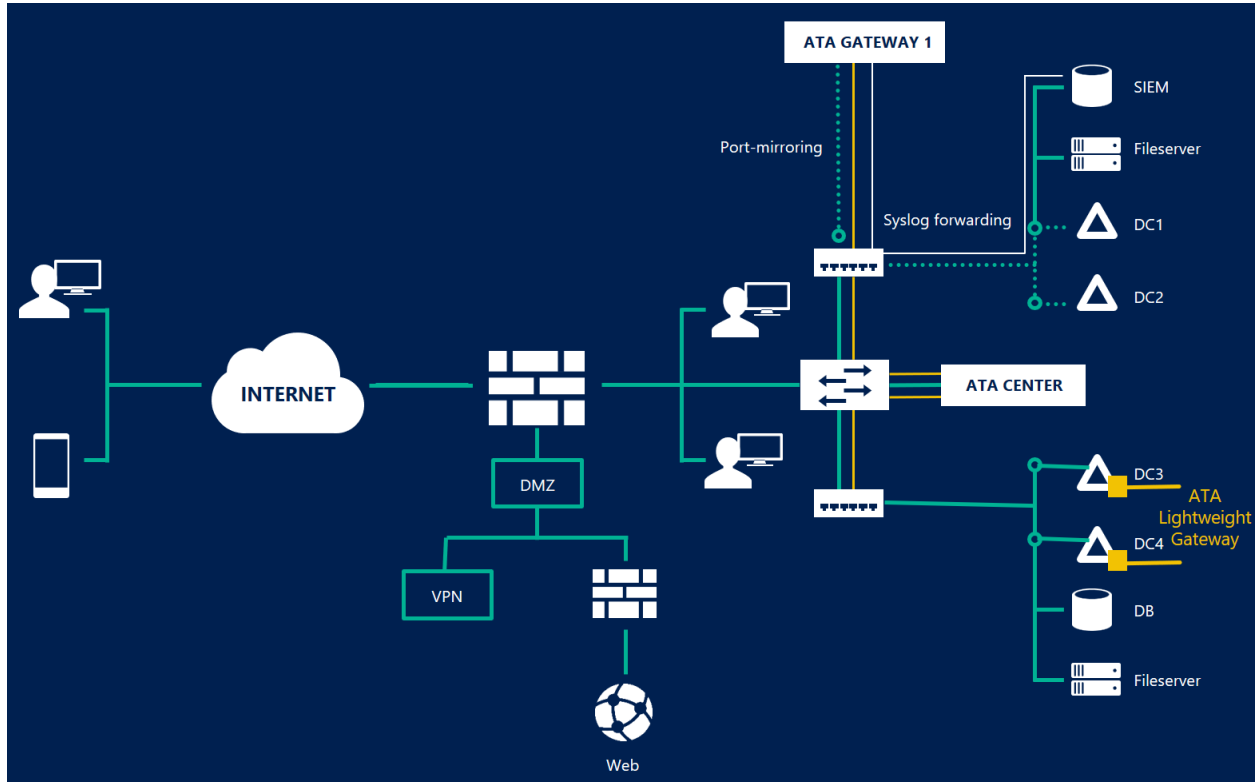


Figure 1: A sample ATA Topology

## POC Introduction

## Deployment Environment

The first decision to make when deploying ATA is which environment it will be deployed in. Production or Test environment?

While for most products it is often recommended to fully validate their features in a test environment, doing so with ATA may bring limited results:

- The abnormal behavior detection will not be triggered if there is a limited activity or limited amount of users
- Results in a test environment may not be indicative of the results in the production environment

When deploying a Proof of Concept, the ideal solution is to start with deploying to a subset of the production environment. Often a medium size AD site or domain (relative to the size of the overall environment) is selected.

If the goal is simply to ensure that the deployment team will be familiar with the procedures to install ATA, it is obviously fine to push it to a test environment. However, it is important to note that ATA's features may not be properly reflected on it.

## POC Implementation Phases

### Planning and Design

#### Capacity Planning

To understand the capacity needed for the ATA Center, which is based on packets per second sent from and to the Domain Controllers, running the ATA Sizing tool is needed.

Properly planning for the capacity of your ATA deployment is very important to a successful PoC. The sizing of the Center and Gateways is based on the packets / second of the domain controllers that will be monitored by ATA.

In order to accurately measure traffic, Microsoft developed a sizing tool, that can be downloaded here: <http://aka.ms/atasizingtool>.

The ATA Sizing Tool is run from a member server and will record a number of performance counters for each domain controller during 24 hours (Default setting can be changed).

The tool will then track the "busy" period for packets / sec, CPU utilization and available memory for each domain controller and collectively for all of the domain controllers.

The "busy" period is the 15 minutes which is the busiest for each of the counters listed.

Using the output of the ATA Sizing Tool you are able to determine the following:

- Sizing of the ATA Center
- Assess if the listed domain controllers can support the installation of Lightweight Gateways and if additional resources will be required.

#### Choosing the right Gateway type

The first design decision when deploying ATA is the Gateway type:

- Full Gateway: Is a dedicated machine, using port mirroring to gather network traffic. It requires a minimum of two network adapters. Additionally this will typically require collaborating with the Network Management team to configure port mirroring. A Gateway can monitor the network traffic of multiple domain controllers.
- Lightweight Gateway: Is installed on the domain controller itself. This will require working closely with the Active Directory management team to install Lightweight Gateways on the Domain Controllers. The Lightweight Gateway can only monitor the network traffic of the domain controller it is installed on.

Each option has pros and cons as depicted below:

Gateway type	Benefits	Cost	Deployment topology	Domain controller use
--------------	----------	------	---------------------	-----------------------

<b>ATA Full Gateway</b>	The out of band deployment makes it harder for attackers to discover ATA is present	Higher	Installed alongside the domain controller (out of band)	Supports up to 50,000 packets per second
<b>ATA Lightweight Gateway</b>	Doesn't require a dedicated server and port-mirroring configuration.  Allows monitoring IaaS VM running on Azure or AWS  Resource Limitations: Monitors and adapt to DC Performances to avoid overloading them.	Lower	Installed on the domain controller	Supports up to 10,000 packets per second

In general, the Lightweight Gateway will provide an easier deployment and the Full Gateway provides greater security and stability.

Finally, there are cases where the Lightweight Gateway will not be supported. The sizing tool described above will provide guidance for each individual DC on whether it can sustain a Lightweight Gateway, and if so, what would its hardware requirements be.

In those cases, the use of a Full Gateway will be the best course of action.

### Domain Membership

ATA Centers and Gateways can be either part of the domain or installed in the workgroup. Here are some of the pros and cons of each option.

**Domain Join** – From an IT Ops perspective this is recommended. It brings central management to ATA as a system. Group Policy, patching, monitoring and reporting are much easier to accomplish when ATA is centrally managed and domain joined. But from a security perspective, you have a system which is monitoring that same domain for compromise. Using the “assume breach” mindset, if an attacker compromises the domain ATA is joined to, the attacker could thus work around ATA or disable ATA altogether.

We continue to enhance health monitoring which should help reduce this risk or likelihood of an attacker being successful at disabling ATA.

In ATA 1.8 you can use SSO to the ATA Console, which can only be achieved when ATA Center is a member of the domain / forest which the admins are members of.

**Workgroup** – From a security operations perspective this is recommended. It allows the ATA system to remain out of band removing the opportunity of an attacker to disable the ATA system, especially if you are using port mirroring and the Full Gateway. From an IT Operations perspective, this increases operations overhead. Now policies have to be applied manually. Patching, monitoring and reporting do not fit into the centralized process IT has created.

Other things to consider include: Windows Event Forwarding, ATA console authentication and PKI. In a domain-join scenario these are much easier to configure and get working. In a workgroup, additional steps and configuration will be required.

For smaller organizations, domain join will likely be the best option. The risk of disabling or getting around ATA is low and with a smaller number of IT personnel, centralized management is key. For large organizations, either configuration option works, due to the larger number of staff and tools which work across workgroup machines. The security posture may be preferred.

Summary:

	Domain Join	Workgroup
<b>Pros</b>	Centralized Management (patching, reporting) Single Sign on	Separate out of band system, less risk of disable or compromise
<b>Cons</b>	Low Risk of disabling or work around of ATA during a compromise	No Centralized Management or more difficult

#### Event collection

In addition to the deep packet inspection of the domain controller network traffic, ATA also uses information from the following Events from each domain controller.

Event ID	Comment
<b>4776</b>	Used to build the entity behavior profiles and can be used to assist in the following detections: <ul style="list-style-type: none"> <li>• PtH</li> <li>• Honeypot user</li> <li>• Bruteforce</li> </ul>
<b>4728, 4729, 4732, 4733, 4756, and 4757</b>	Required for Sensitive Group modification suspicious activity and reporting. New for ATA 1.8

To get these events will depend on the version of the Gateway being deployed.

- Lightweight Gateway – No additional configuration is required. Starting in ATA 1.8, the Lightweight Gateway will automatically read the events needed directly from the Event Viewer. You will need to confirm the Domain Controller is configured to log these events.
- Full Gateway – There are two options for the Gateway to receive these events.
  - Windows Event Forwarding – Configure WEF on each domain controller monitored by a Gateway to forward the listed event IDs to the Gateway. The events must be forwarded to the “Forwarded Events” log on the Gateway. Starting in ATA 1.8 you do not need to configure the Gateway for WEF, it will automatically check the Forwarded Events log.



- If you are collecting the events from the domain controllers to a central SIEM you can configure your SIEM to forward the events to the Gateway. The following SIEMs are supported:
  - HP Arcsight
  - Splunk
  - QRadar
  - RSA

### Catalog of actors

Actor	Description	PoC Responsibility
<b>Information Security Team</b>	This team manages the security of the information systems. It defines security strategies and policies for other teams within the organization. It also administers and monitor security solutions.	Leading the deployment of ATA in the environment.
<b>Network Team</b>	Owners of the network infrastructure and firewall devices.	When working with Full Gateways, the network team will be in charge of configuring the requirements for Port Mirroring of the DCs.
<b>Active Directory Management Team</b>	In charge of managing and/or maintaining the on-premises Active Directory environment of the organization.	They will need to provide a service account for ATA to operate properly. When working with Lightweight Gateways, they will be in charge of installing the software on the DCs in collaboration with the InfoSec team.
<b>Security Operations Team</b>	Manage daily operations and monitor alerts from various monitoring systems (including security).	Once ATA is deployed, their goal is to monitor its activity and trigger the incident response process when relevant activity is reported.

### Deploying

While deploying ATA is a relatively simple process, it requires ensuring that all Domain Controllers are monitored by ATA.

#### Manual deployment

For small to medium size environments, a manual deployment is often the best option. ATA Installation Wizard, whether it is for the center or the Gateway, is very straightforward and only has a minimum amount of settings to configure.

For environments with a large number of Gateways, it can be very time consuming.

### *Automated deployment*

ATA Centers and Gateway can also be deployed silently and en masse, using command line parameters.

This allows to push the ATA Gateway using a deployment software, such as SCCM.

More info on command line parameters is available here: <https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/ata-silent-installation>

### Prerequisites

The full list of ATA's requirements is available here: <https://docs.microsoft.com/en-us/advanced-threat-analytics/plan-design/ata-prerequisites>.

A summary is available below:

#### Network requirements

- **Port Mirroring:** If Full Gateways are planned to be used, the traffic from domain controllers will have to be mirrored to a Gateway. This can be done using physical switches or virtualization solutions (Hyper-v and VMWare both support it).
- **Network communication Ports:** Several ports will need to be open to allow communication between the ATA Center and the Gateways, communication with SIEMs and name resolution of end-point hosts. All details are available [here](#).

#### Software requirements

- The ATA Center is supported on Windows Server 2012 R2 and above.
- The ATA Gateway (Full Gateway) is supported on Windows Server 2012 R2 and above.
- The ATA Lightweight Gateway is supported on Windows Server 2008 R2 and above.
- ATA Requires a minimum of .Net Framework version 4.6.1 and is optimized for .Net Framework 4.6.2. If .Net Framework is not installed, the ATA installation will install .Net Framework 4.6.1 which could potentially require a reboot of the domain controller.
- The following hotfix is required by ATA: [KB2919355](#).

## POC Building blocks

### Before you get started

Full requirements for ATA are available here: <https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites#ata-center-requirements>

#### General prerequisites

The following are required prior to start configuring ATA:

- Credentials of a user account with admin rights to the ATA Center.
- A service account that is a simple Domain User of a domain in the monitored forest.
- SSL port between the ATA Center and the Gateways (by default 443).
- SSL Port from machines that need to reach the console (443).
- .Net Framework 4.6.1 or above installed on the ATA Center and the ATA Gateways machines.

- It is recommended to install a server certificate on the ATA Center for production deployment (alternatively self-signed certificates can be used and are simpler for POC Deployments).

#### Prerequisites for Full Gateway deployment

The ATA Gateway will require two network adapters, one for management and the other for packet capture.

The main requirement for an ATA Gateway is port mirroring. It will need to receive all the inbound and outbound traffic from the DCs it is monitoring.

For physical machines, it can be configured at the network switch level (most hardware configuration support this). When running with Virtual Machines, the two main actors in the market support port mirroring (Hyper-V and VMWare). Cloud solutions such as Azure or AWS do not support any type of port mirroring as of now, therefore, they will only be supported in a Lightweight Gateway Configuration.

It is strongly recommended to validate that port mirroring is properly functioning using [Netmon 3.4](#).

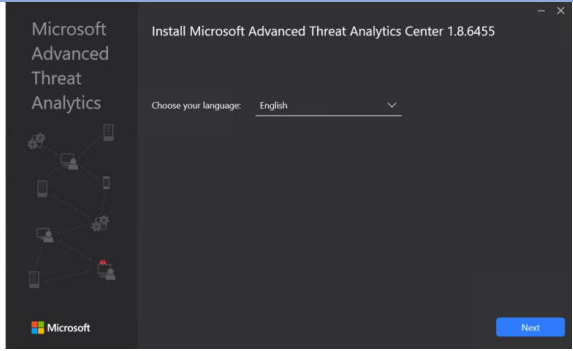
#### Prerequisites for Lightweight Gateway Deployment

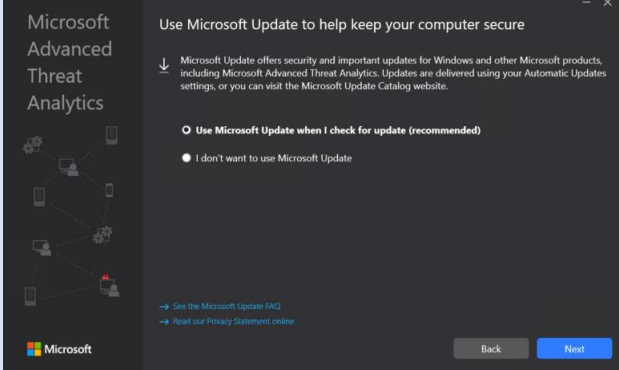
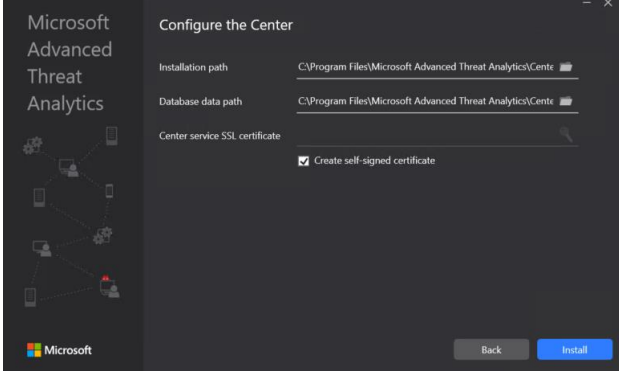
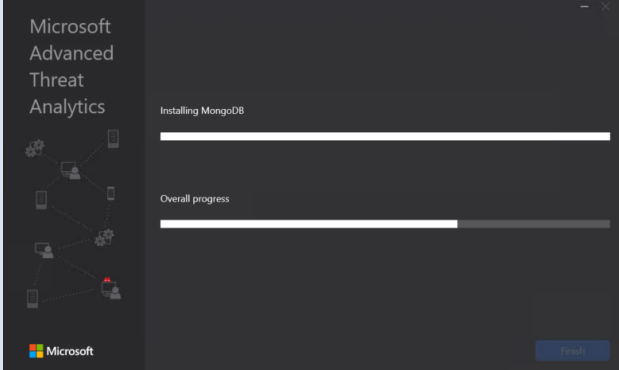
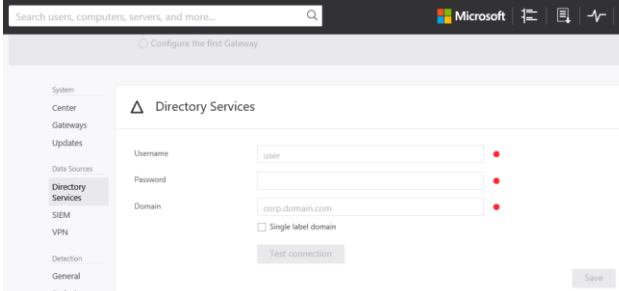
It is recommended to install the .Net Framework 4.6.1 or above prior to the Lightweight Gateway installation. This will limit the need for a reboot of the Domain Controllers.

.Net Framework is available here: <https://www.microsoft.com/en-us/download/details.aspx?id=53345> (version 4.6.2).

#### ATA Center Installation

The steps required to install the ATA center in your environment are below:

Step	Capture / Comment
1. <b>Download the ATA Center Setup file and run it on the machine dedicated for your ATA Center</b>	Center setup is available here: <a href="https://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-advanced-threat-analytics">https://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-advanced-threat-analytics</a>
2. <b>On the welcome screen, click next.</b> <b>Note: Before being able to install the ATA Center, you may be required to install Microsoft .Net framework. The installation wizard will automatically take your through those steps, default options are recommended.</b>	
3. <b>Review and Accept the License Terms and click next.</b>	

<p>4. Review the update settings and choose the most appropriate for your organization. We recommend to configure ATA to use Microsoft Update.</p>	
<p>5. Select the installation folders for the ATA bits and for the ATA database. Select a certificate if you do not wish to use a self-signed certificate (not recommended in production). It is strongly recommended to configure the database to be stored on a separate drive. Click Next.</p>	
<p>6. Wait until the installation is complete, then click Launch to open the configuration page.</p>	
<p>7. The ATA Portal will open and require that you configure your service account (the account only needs to be a standard domain user account). 8. Click Test Connection to ensure the user name and password entered is working.</p>	
<p>9. You are now ready to move on to the Gateway installation.</p>	

## Silent Installation

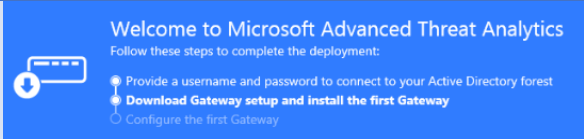
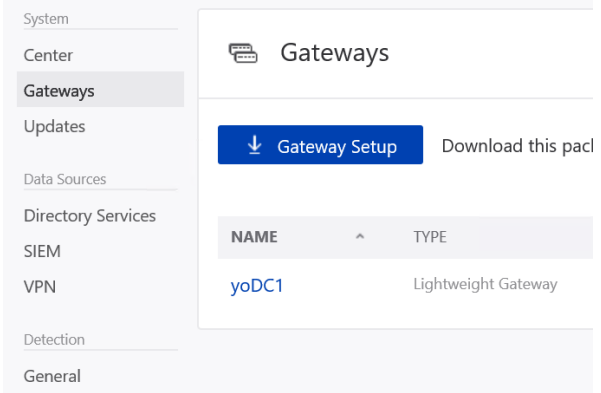
There are only rare cases where a silent or scripted installation are relevant for the ATA Center (especially in a PoC Environment). However, if it becomes a requirement, the following can be used:

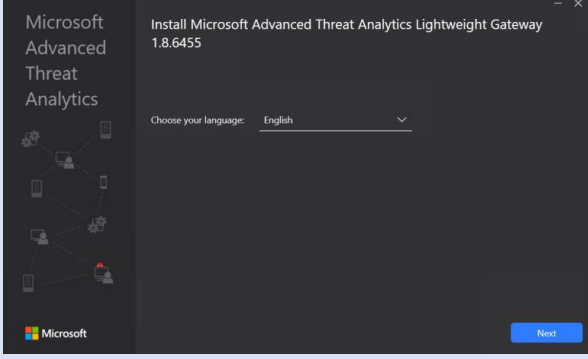
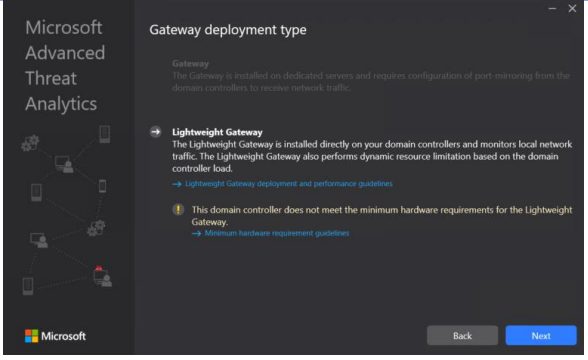
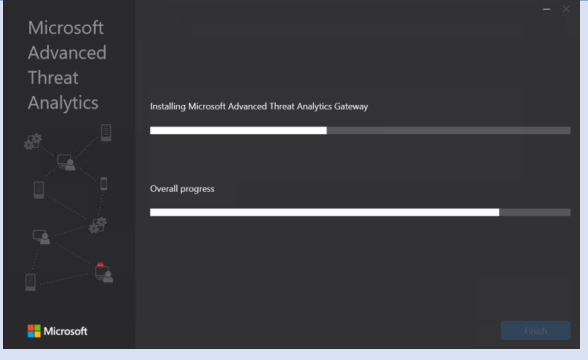
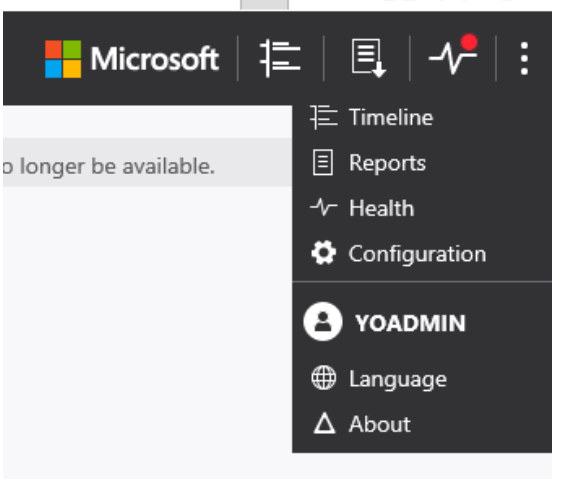
More info on silent installation can be found here: <https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/ata-silent-installation>

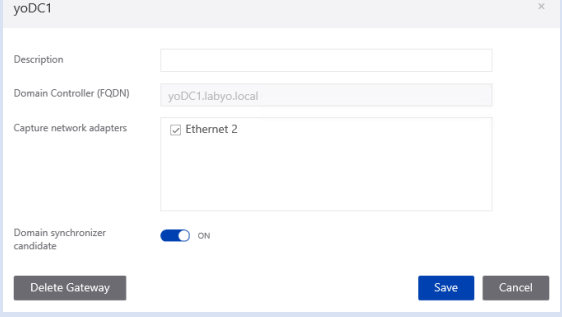
## ATA Gateway Deployment

### Basic installation

The following procedure is below:

Step	Capture / Comment				
<ol style="list-style-type: none"> <li>1. <b>Connect to the machine used as a Gateway, or to a Domain Controller for a Lightweight Gateway, and connect to the ATA Portal, using an account member of the local ATA Administrator Group or Administrators on your ATA Center.</b> <b>Note: the ATA Portal address is simply https://&lt;ATA Center IP Address&gt;/</b></li> <li>2. <b>For your first Gateway, simply click on the link to download the Gateway Setup.</b></li> </ol>	 <p>Welcome to Microsoft Advanced Threat Analytics</p> <p>Follow these steps to complete the deployment:</p> <ul style="list-style-type: none"> <li>1 Provide a username and password to connect to your Active Directory forest</li> <li>2 <b>Download Gateway setup and install the first Gateway</b></li> <li>3 Configure the first Gateway</li> </ul>				
<ol style="list-style-type: none"> <li>3. <b>For subsequent Gateways, go to the Configuration page in the ATA Console, and then on the Gateways section.</b></li> <li>4. <b>Click the button to download the Gateway Setup.</b> <b>The same installation package can be used for all the other Gateways.</b></li> </ol>	 <p>System</p> <p>Center</p> <p><b>Gateways</b></p> <p>Updates</p> <p>Data Sources</p> <p>Directory Services</p> <p>SIEM</p> <p>VPN</p> <p>Detection</p> <p>General</p> <p>Gateways</p> <p>↓ Gateway Setup Download this pack</p> <table> <thead> <tr> <th>NAME</th> <th>TYPE</th> </tr> </thead> <tbody> <tr> <td>yoDC1</td> <td>Lightweight Gateway</td> </tr> </tbody> </table>	NAME	TYPE	yoDC1	Lightweight Gateway
NAME	TYPE				
yoDC1	Lightweight Gateway				

<ol style="list-style-type: none"> <li>Unzip the file and run the setup (note: the setup cannot be run from within the zip file).</li> <li>Choose your language and click Next.</li> </ol>	
<ol style="list-style-type: none"> <li>On the Gateway deployment type, verify that the proper type is selected, and click next.</li> <li>Select the proper installation path and click Install.</li> </ol>	
<ol style="list-style-type: none"> <li>Wait until the installation completes.</li> <li>Click finish, and open the ATA Console (from any computer).</li> </ol>	
<ol style="list-style-type: none"> <li>Open the Configuration page.</li> <li>Click on Gateways.</li> </ol>	

<p>13. Click on the Gateway that you installed and verify its status and configuration.</p> <p><b>Note: If it is a Lightweight Gateway, and the first Gateway in your environment, check Domain Synchronizer Candidate and click save.</b></p>	
<p>14. For the Full Gateway, the proper capture adapter must be select. The names of the DCs monitored by the Gateway must also be entered.</p>	
<p>15. Repeat the same operation for each Gateway, or automate it follow instructions below.</p>	

### Silent and mass Deployment

While most organizations will use only one center, they will often have several gateways. Deploying them manually can be time consuming. The instructions below can be passed to any deployment tool (such as SCCM) or script in order to automate the deployment of a large number of Gateways.

More info on silent installation can be found here: <https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/ata-silent-installation>

### Note on port mirroring

The ATA Full Gateway can only function when traffic to and from domain controllers is redirected to it.

Most hardware network devices and virtualization platforms support this type of capabilities. Refer to your vendor for exact guidance on how to properly configure port mirroring.

The procedure to configure port mirroring with Microsoft Hyper-V is available here:

[https://technet.microsoft.com/library/jj679878.aspx#bkmk\\_portmirror](https://technet.microsoft.com/library/jj679878.aspx#bkmk_portmirror)

### Validating deployment

Some activities can easily simulated and will appear as attacks to ATA. A full range of pen test examples are available in the ATA Suspicious Activity Playbook: <http://aka.ms/ataplaybook>.

Here are two examples:

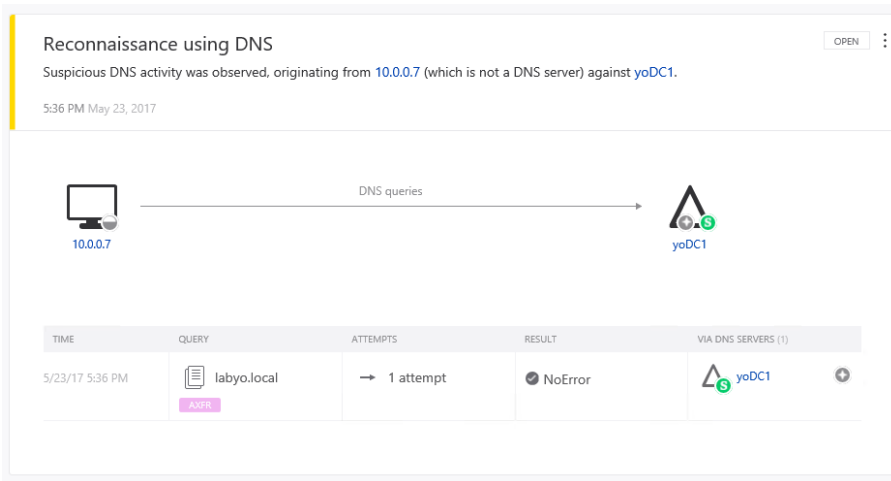
### DNS Reconnaissance

DNS Reconnaissance is the concept of trying to obtain information on DNS names in the environment.

This can be attempted fairly easily by running the following command:

```
nslookup -query=AXFR domain.com 10.0.0.x
```

When ATA detects such a query from a machine is not part of the name server list, it will trigger the following alert:



### Remote execution attempts

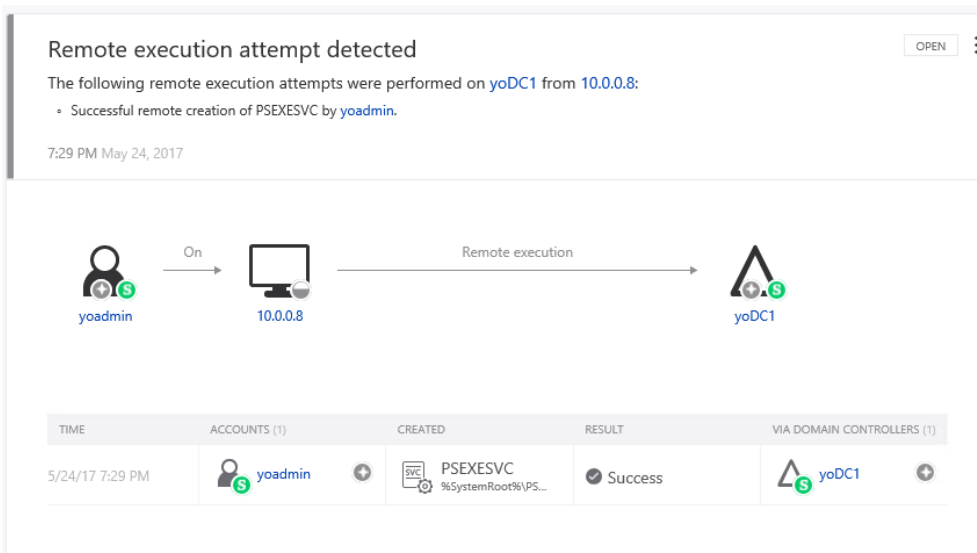
Remote execution attempts can be tested using PSEXec (available here: <https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>).

The following command line can be run:

Psexec.exe \\dc01 cmd

Then any command can be executed remotely on the machine.

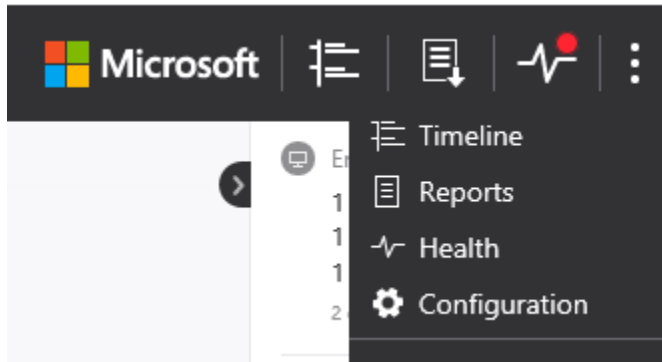
This will trigger the alert below:





## ATA Configuration

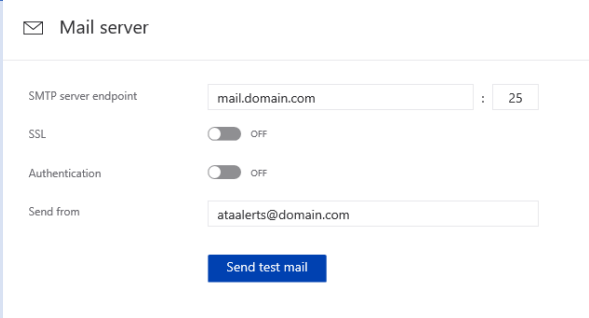
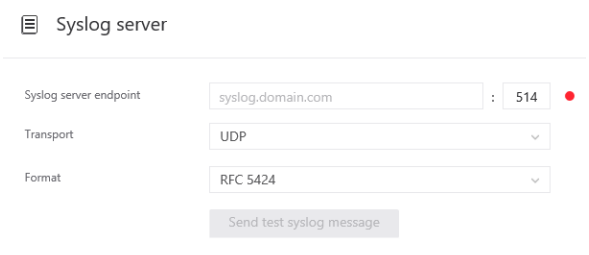
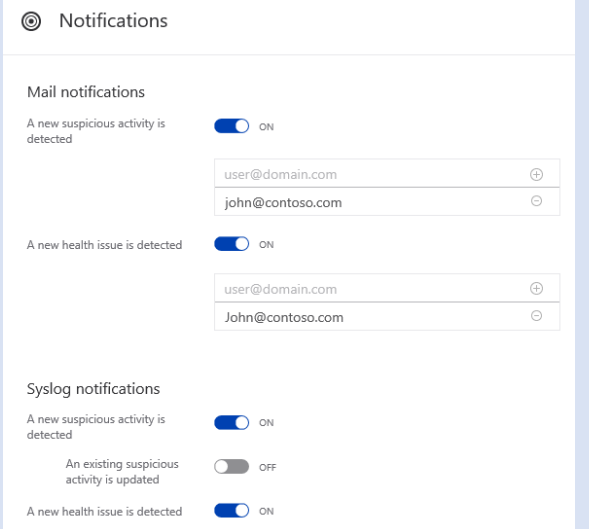
All of the following configuration options are done from the ATA Portal Configuration page, which can be accessed from the top right menu on the ATA Portal.



## Detection

Setting and steps	Capture / Comment
<p><b><u>Honeytoken accounts:</u></b> To configure a honey token account, type the name of the user you would like to use. Click the arrow in the dropdown menu. Click Save.</p>	
<p><b><u>Exclusions:</u></b> Can be configured for several type of suspicious activities, in order to limit the number of false positive coming up.</p> <p><b>It is recommended to keep this configuration with default settings unless you experiment specific false positives.</b></p>	

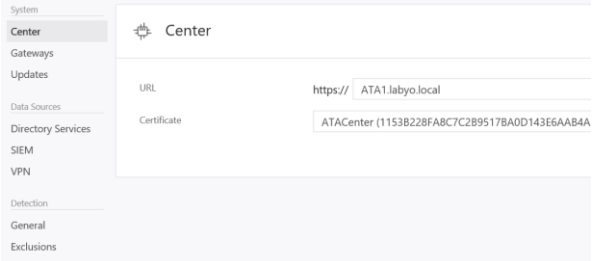
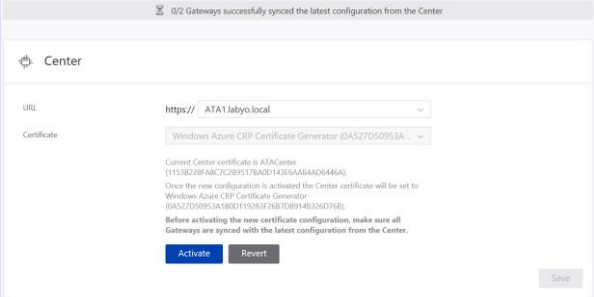
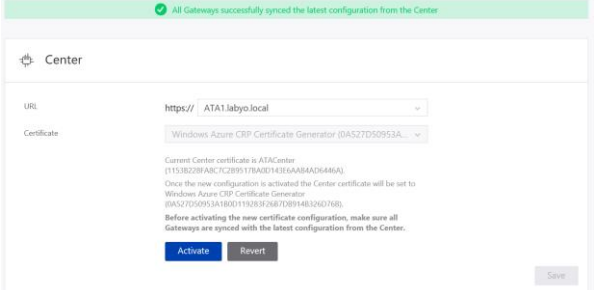
## Notifications

Setting and steps	Capture / Comment
<b>Mail Server:</b> Configure your SMTP mail server to be used for email alerts. SSL and authentication can also be configured.	
<b>Syslog Server:</b> If you are using a Syslog server / SIEM, you can configure ATA to send its events to it, using one of the supported RFCs.	
<b>Notifications:</b> Configure the required notification to be sent. Notifications can be sent by email and / or by way of a syslog server.	

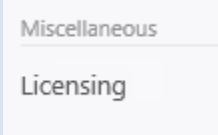
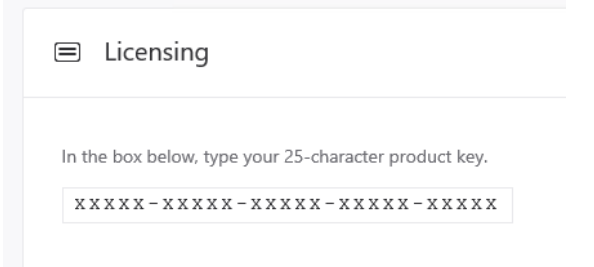
## SSL Certificate Configuration

While it is ok to install a Proof of Concept using a self signed certificate, it is recommended to use a CA issued certificate for the ATA Portal once it is used in production.

Steps	Capture / Comment
1. Request a certificate from a public or internal Certificate Authority and install	This certificate must be valid for SSL. Full requirements are available here:

it on the computer store of the ATA Server.	<a href="https://docs.microsoft.com/en-us/advanced-threat-analytics/plan-design/ata-prerequisites">https://docs.microsoft.com/en-us/advanced-threat-analytics/plan-design/ata-prerequisites</a>
<ol style="list-style-type: none"> <li>2. Connect to the ATA Portal and go to the configuration page.</li> <li>3. In the left side column, click Center.</li> </ol>	
<ol style="list-style-type: none"> <li>4. In the certificate field, select the certificate that was just installed on the ATA Center machine.</li> <li>5. Click Save.</li> <li>6. The following message, in a grey background will appear.</li> </ol>	
<ol style="list-style-type: none"> <li>7. <b>WAIT</b>, until the following message, in green appears. (failure to wait until this process is complete will prevent proper communication with all the Gateways).</li> <li>8. Click Activate (if any Gateway cannot synch at this point, click the revery button).</li> </ol>	

## Licensing

Step	Capture / Comment
1. In the configuration page, under miscellaneous, click Licensing.	
2. Enter your product key in the field and click Save.	

### 3. Verify that you receive the proper confirmation as captured here.

#### Licensing

✓ Microsoft Advanced Threat Analytics is activated.

Product ID 00000000-0000-0000-0000-000000000000

## Event Collection

For Full Gateways and earlier versions of ATA (1.7 and below), SIEM Event forwarding or Windows Event Forwarding must be configured to gather required events.

To ensure that ATA is collecting the required events for Sensitive Group Modification the domain controller needs to be configured to record it, by default it is collected.

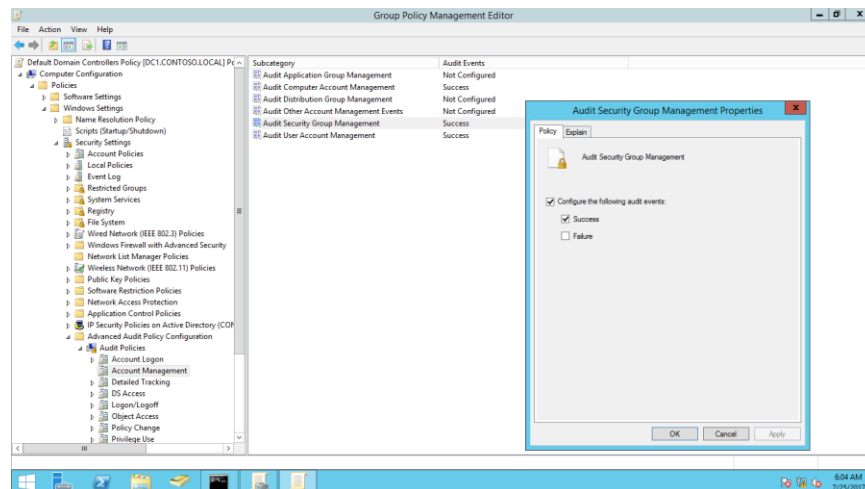
The following command on the domain controller should be used to verify that it is being collected:

```
auditpol /get /category:"Account Management"
```

If Security Group Management is set to Success, no change is needed.

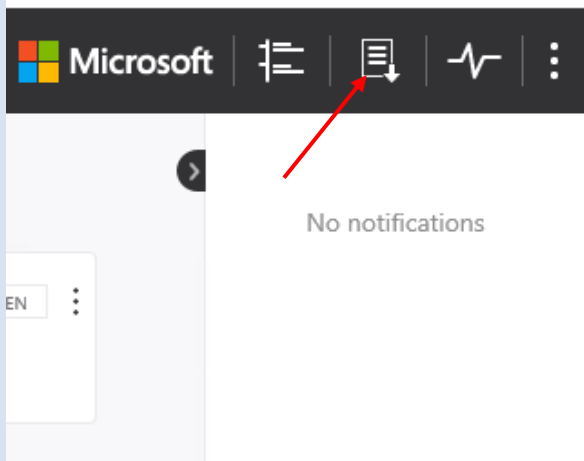
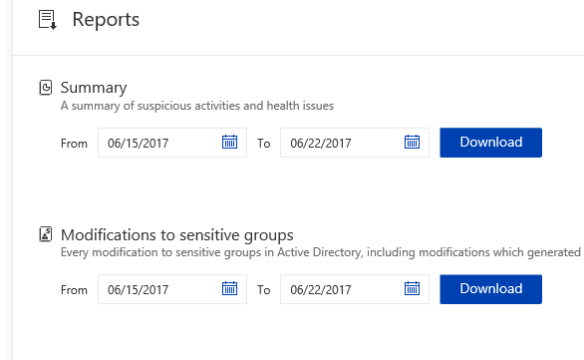
```
C:\Users\Administrator>auditpol /get /category:"Account Management"
System audit policy
Category/Subcategory          Setting
Account Management
Computer Account Management    Success
Security Group Management      Success
Distribution Group Management  No Auditing
Application Group Management   No Auditing
Other Account Management Events No Auditing
User Account Management        Success
```

If it says “No Auditing”, the Domain Controller GPO will have to explicitly configure to enable Auditing of Security Group Management for Success.



## Report Generation

ATA 1.8 introduces a reporting feature. Below are the steps to use it.

Steps	Capture / Comments
1. In the ATA Web Console, click on the Reporting Icon on the top right of the page.	
2. Choose the report and select required dates, then click Download.	
3. Open the Excel spreadsheet to review the report	