ATAIS - Solution Design



Advanced Threat Analytics Implementation Services

Prepared for

Customer Name

10/19/2016

Version Draft

Prepared by

**[Update in doc Properties]**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

Revision and Sign-Off Sheet

Change Record

Table : Change Record

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

Reviewers

Table : Reviewers

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

Table of Contents

[1 Solution Design Summary 0](#_Toc464635849)

[1.1 Audience 0](#_Toc464635850)

[2 Detailed Solutions Design 1](#_Toc464635851)

[2.1 Solutions Architecture Overview 1](#_Toc464635852)

[2.2 Active Directory Domain Services 1](#_Toc464635853)

[2.2.1 Solution Architecture—Domain Controllers 2](#_Toc464635854)

[2.3 Solution Sizing 3](#_Toc464635855)

[2.3.1 Sizing—ATA Center 3](#_Toc464635856)

[2.3.2 Sizing—ATA Gateways 4](#_Toc464635857)

[2.3.3 Domain Controller Analysis for Sizing 6](#_Toc464635858)

[2.3.4 ATA Components Required for Solution Design 6](#_Toc464635859)

[3 Solution Configuration 8](#_Toc464635860)

[3.1 Certificate Configuration 8](#_Toc464635861)

[3.2 ATA Center 8](#_Toc464635862)

[3.2.1 Hardware Configuration 8](#_Toc464635863)

[3.2.2 Network Ports 9](#_Toc464635864)

[3.3 ATA Lightweight Gateway 10](#_Toc464635865)

[3.3.1 Hardware Configuration 10](#_Toc464635866)

[3.3.2 Network Ports 11](#_Toc464635867)

[3.4 ATA Gateway 11](#_Toc464635868)

[3.4.1 Hardware Configuration 11](#_Toc464635869)

[3.4.2 Network Ports 12](#_Toc464635870)

[3.4.3 Port-Mirroring Considerations 13](#_Toc464635871)

[3.4.4 Port-Mirroring Configuration—Hyper-V 14](#_Toc464635872)

[3.5 ATA Configuration 15](#_Toc464635873)

[3.5.1 ATA General Configurations 15](#_Toc464635874)

[3.5.2 ATA Gateways Configuration 16](#_Toc464635875)

[3.5.3 ATA Detection Configurations 17](#_Toc464635876)

[3.5.4 Email Server Configuration 19](#_Toc464635877)

[3.5.5 Syslog Server Configurations 19](#_Toc464635878)

[3.5.6 Notification Settings 20](#_Toc464635879)

[3.6 Additional Network Configuration Information 21](#_Toc464635880)

[3.6.1 Endpoint or Device Firewall Configuration 21](#_Toc464635881)

[3.7 Event Collection 21](#_Toc464635882)

[3.7.1 Configuration of ATA Gateway to Listen for SIEM Events 22](#_Toc464635883)

[3.7.2 Configuration of Windows Event Forwarding 22](#_Toc464635884)

## Tables

[Table 1: Change Record 3](#_Toc462985333)

[Table 2: Reviewers 3](#_Toc462985334)

[Table 3: Active Directory Configuration Items 2](#_Toc462985335)

[Table 4: Domain Controller Information 3](#_Toc462985336)

[Table 5: ATA Center Sizing 3](#_Toc462985337)

[Table 6: ATA Gateway Sizing 5](#_Toc462985338)

[Table 71: ATA Center Hardware for <type forest FQDN here> 9](#_Toc462985339)

[Table 82: Requirements—ATA Center Network Ports 10](#_Toc462985340)

[Table 93: Requirements—ATA Gateway Hardware 10](#_Toc462985341)

[Table 104: Requirements—ATA Lightweight Gateway Network Ports 11](#_Toc462985342)

[Table 115: Requirements—ATA Gateway Hardware 12](#_Toc462985343)

[Table 128: Port-Mirroring Configuration 15](#_Toc462985344)

[Table 13: ATA Center Configuration 15](#_Toc462985345)

[Table 14: ATA Console Configuration 15](#_Toc462985346)

[Table 14: ATA Console Configuration 16](#_Toc462985347)

[Table 15: ATA Gateway Configuration 16](#_Toc462985348)

[Table 16: ATA Gateway Configuration Details 17](#_Toc462985349)

[Table 179: Short-Term Lease Subnets 17](#_Toc462985350)

[Table 183: Email Alerting Configuration 19](#_Toc462985351)

[Table 19: Syslog server configuration 20](#_Toc462985352)

[Table 20: Email notifications configurations 20](#_Toc462985353)

[Table 21: Syslog notification settings 20](#_Toc462985354)

[Table 224: Endpoint Firewall Configuration 21](#_Toc462985355)

[Table 236: Windows Event Forwarding—Domain Controllers to Gateway 22](#_Toc462985356)

## Figures

[Figure 1: High-Level ATA Design 1](#_Toc462985357)

**Spell/grammar check is turned ON within all 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

1. Solution Design Summary

Provide an overall summary of the contents of this document. This should include the criteria by which the design was established and how it was validated. It should also clearly identify the intended audience.

Justification: Some project participants may need to know only the document’s highlights, and summarizing creates that user view. It also enables the full reader to know the essence of the document before they examine the details. Expand below on the customer architecture.

This solution is designed to meet the requirements or goals that were stated in the Vision and Scope document.

The goals for the solution design include:

**Instructions:** Please update the following goals to match your customer’s goals for the project. These should have been collected during the Envision phase and documented in the Vision and Scope document.

* Designing a solution that is based on a shared vision and meeting Customer Name requirements.
* Creating a design that is based on configuration items that were agreed upon during the solutions design workshop.
  1. Audience

This solutions design document is intended for Customer Name teams that are responsible for designing, implementing, and operating a Microsoft Advanced Threat Analytics (ATA) solution.

1. Detailed Solutions Design
   1. Solutions Architecture Overview

**Instruction:** Describe how the features and functions will operate together to form the solution. It identifies the specific components of the solution and their relationships. A diagram illustrating these components and relationships is an excellent communication device. Update the diagram below outlining the details of the architecture. A Visio file containing the base diagrams has been provided as a part of this offers materials. Please use those to assist you with this activity.

Figure 1 illustrates the solutions design architecture.

Figure 1: High-Level ATA Design

* 1. Active Directory Domain Services

**Instruction:** Update the table below and record all Active Directory configurations for the solution. There should be one table listing per forest. If you are monitoring multiple forests, please copy and paste the table so you have one table entry per forest.

The following table outlines the configuration of Customer Name’s Active Directory Domain Services (AD DS) infrastructure for which ATA will provide detection services.

Table 3: Active Directory Configuration Items

|  |  |  |
| --- | --- | --- |
| Type Active Directory Forest Name Here | | |
| Item | Details | Configuration |
| Number of domain controllers | The number of domain controllers that will be reached by ATA. See Port Mirroring Requirements. | Domain Controllers |
| Domain Controller Operating System | The standard operating system for Customer Name on all Domain Controllers. | Record OS version/versions here |
| Domain Controller Locations | Datacenter locations where Customer Name has domain controllers deployed which ATA will be required to provide detection services for. | Type in the datacenter location here |
| Standard User Object | * An Active Directory Domain Services user account and password that has been granted read access to **all objects** in the domains to be monitored. * This account should be locked down in a way that it is not allowed to have interactive logon capabilities to any system within the forest. | Record Username here. Domain/username |
| Optional:   * Standard User Object * (Read-Only) – Deleted Objects Container | An Active Directory Domain Services user (same as listed above) should have read only permissions on the Deleted Objects container. This will allow ATA to detect bulk deletion of objects in the domain in addition to keeping ATA up to date with deleted objects. | Record Username here. Domain/username |
| Optional:   * Standard User Object * Honey Token | A user account of a user who has no network activities. This account will be configured as the ATA Honey Token user. To configure the Honey Token user, you will need the SID of the user account, not the username. | Record Username here. Domain/username  See Operations Guide for extracting the SID using PowerShell |

* + 1. Solution Architecture—Domain Controllers

To provide more reliable detection services, ATA can monitor traffic to and from domain controllers. The following table provides information about domain controllers that ATA will monitor; this includes fully qualified domain name (FQDN) and datacenter location information.

**Instruction:** Please update the following table with information specific to the domain controllers that ATA will be monitoring for this delivery. Add rows to your solution as needed.

Table 4: Domain Controller Information

|  |  |  |  |
| --- | --- | --- | --- |
| DC FQDN | Forest Name | Domain Name | Datacenter Location |
| DC1.contoso.com | Contoso.Com | Contoso.Com | Contoso HQ |
|  |  |  |  |

* 1. Solution Sizing

**Instruction:** Modify the tables in this section to record the customer’s specific sizing needs for this solution. This can also be kept as informational for your design and record your configuration items in the hardware section.

To determine the appropriate sizing for your ATA deployment, it is highly recommended that you capture network statistics for your domain controllers. This helps provide the most detailed information possible to design your solution.

Ideally, you should capture seven (7) or more days of average packets per second including lows and peaks to gain an understanding of your environment. If you have this available to you from your network team, please use that. Otherwise, ATA has a sizing tool to assist you. Please visit [ATA Capacity Planning](https://docs.microsoft.com/en-us/advanced-threat-analytics/plan-design/ata-capacity-planning) located on Microsoft docs online for more information about this tool.

The following subsections outline the sizing of this solution.

* + 1. Sizing—ATA Center

The following information provides ATA Center system–sizing recommendations. The size of the ATA Center will depend on how much network traffic your domain controllers generate and how many suspicious activities that ATA detects and stores in its database. The following table provides general guidelines that can help you determine what size an ATA Center should be.

We recommend gathering ATA Center data for 30 days to determine normal user behaviors and produce behavioral analytics. The required disk space for the ATA database (on a per-domain controller basis) is defined in the following table. The recommendations are based on Customer Name–specific domain controller statistics.

This methodology will be used to determine the overall computational requirements for your ATA Center. That information will be documented in section 2.4.1 of this document.

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 5: ATA 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 hyper-threaded 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 free 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 free 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. Sizing—ATA Gateways
       1. ATA Lightweight Gateway

An ATA Lightweight Gateway is installed directly on the Domain Controller and monitors their 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 7: 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

**\*\*** Hyper-threading 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 6: 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 network interface card (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 hyper-threaded cores

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

* + 1. Domain Controller Analysis for Sizing

As noted previously, the size of the ATA Center and the number and placement of ATA Gateway or ATA Lightweight Gateway components depends on how much network traffic a domain controller receives. This traffic is sent to the ATA Gateway or gathered locally by the ATA Lightweight Gateway for further distribution to the ATA Center.

As a part of the design sessions, analysis was completed to determine how many packets each in-scope domain controllers handle. The following table provides this information.

**Instruction:** Please update the following table with specific packet information for each of the in-scope domain controllers that ATA will monitor. More specific information may be found at <https://technet.microsoft.com/en-us/library/mt429323.aspx> to assist you with this process.

Table 8: Analyzed Packets per Second

|  |  |  |
| --- | --- | --- |
| Domain Controller FQDN | Analyzed Packets per Second | Comments |
| DC FQDN | #### |  |

* + 1. ATA Components Required for Solution Design

ATA design, as noted, is largely based on how much network traffic is generated to and from the in-scope domain controllers. Making use of the information that was collected during the design workshops, the required ATA components for Customer Name are as follows.

**Instruction:** Update the following table with specifics regarding the number of ATA components required for your delivery. Use the following guidelines for filling out the table:

**Component** – the component column represents either the ATA Center or ATA Gateway component. If your deployment is not a mix of ATA Gateways and ATA Lightweight Gateways, remove the row corresponding to the Gateway type that is not being deployed.

**Number** – the number column represents the total number of the components the solution requires. If you are monitoring a single forest, you would only have 1 ATA Center. Therefore, the value in this column would be “1”.

**Location Placement** – use this column to illustrate which datacenter or network location the components will be deployed to.

**Details** – the details column is where you provide commentary on the information for that row. For example, using the ATA Center component, if you were monitoring multiple forests, you would have 1 ATA Center per forest. Your details would explain that you would have 1 ATA Center monitoring forest A (e.g. contoso.com) and another ATA Center monitoring forest B (e.g. fabrikam.com). Use this to add that detail or any other specifics you feel would be helpful for your customer.

**Note:** The information provided in sections 2.3.4 will help you determine the number of ATA Gateway’s you need to deploy to support your customer’s delivery. You may only deploy 1 ATA Center per Active Directory forest so the number of Centers should match the number of forests that are in scope.

Table 9: ATA Components for Solution Design

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Number | Location Placement | Details |
| ATA Center | 1 | Primary Datacenter | One ATA Center will be deployed to provide detection services for the contoso.com forest. |
| ATA Gateway | 2 | Primary Datacenter | Two ATA Gateways will be deployed to provide detection services for domain controllers located in the contoso.com forest which are in the primary datacenter location. |
| ATA Lightweight Gateway | 2 | Domain Controller Name | 2 ATA Lightweight Gateways will be deployed to provide detection services for domain controllers located in the contoso.com forest which are in the Branch Office Datacenter |

1. Solution Configuration

**Instructions:** Sections 3.1 through 3.6 have been created assuming a single forest deployment of ATA. If your engagement includes deploying ATA to multiple forests, please copy the entire contents of section 3 for each forest and title the primary section header as “ATA Solution Configuration – ForestName” (e.g. ATA Solution Configuration – Contoso.com)

**Gateway Configuration:** If your solution includes only ATA Gateways, remove section 3.3; otherwise if your solution contains only ATA Lightweight Gateways, remove section 3.4. If your solution contains a mix of both, keep both sections and document accordingly.

* 1. Certificate Configuration

The following table outlines the certificate configuration that will be used for the ATA Center and Gateway. These certificates will be issued by the Customer Name internal certificate authority.

**Instruction:** Update the following table with information about how the certificates will be issues for each of the listed needs.

Table 10: ATA Certificate Configuration

|  |  |  |
| --- | --- | --- |
| Role | Certificate Configuration | Certificate Details |
| Center | The ATA Center requires certificates for the following services:  Internet Information Services (IIS) – Web server certificate - Client, Server authentication certificate  ATA Center Service – Server authentication certificate | Web server certificate:  Enter in the ATA Portal FQDN:  e.g. ATAportal.contoso.com  ATA Center service:  Enter the ATA Center Service URL. e.g. ATAservername.contoso.com |
| Gateway | A certificate supporting **Server Authentication** is required to be installed in the Computer store of the ATA Gateway (and ATA Lightweight Gateway) in the Local Computer store. This certificate must be trusted by the ATA Center. | Enter in the specific URL for this certificate. |

**Note:** Self-signed certificates should be used for lab deployment or testing only.

* 1. ATA Center

This section details the specific configuration that is required for the ATA Center deployment.

* + 1. Hardware Configuration

**Instruction:** using the data you captured in section 2.3.3, and the location information listed in section 2.2.1, provide specific details surrounding the ATA deployment.

Each section will have tables to help you illustrate the eventual ATA design and configuration. Please modify the tables in this section to record the customer’s specific configuration needs for this solution.

The following section outlines the hardware configuration for the Center and the Gateway.

**Instruction:** You should have a single table listed for each in-scope forest. If you have more than one forest, please copy and paste the following table as many times as needed. Update the table caption to be specific to the forest.

The following table provides information about the computational resources that will be needed to support this ATA Center deployment.

Table 71: ATA Center Hardware for <type forest FQDN here>

|  |  |  |
| --- | --- | --- |
| Component | Center Hardware Details | Configuration |
| Processor | See center-sizing section (Table 5: ATA Center Sizing). | Update based on sizing exercise here |
| Memory | See center-sizing section (Table 5: ATA Center Sizing). | Update based on sizing exercise here |
| Available disk space  Database storage | See center-sizing section (Table 5: ATA Center Sizing). | Enter based on sizing exercise here  Record Database location here. Review operations and implementation guides for further requirements. Its recommended to move the database to dedicated disks and drive |
| Network | One network adapter, two IP addresses:   * ATA service * ATA management (IIS) | 2 IP Addresses are required. Enter both IP addresses that will be used here:  ATA Service IP: x.x.x.x  ATA Management IP (IIS): x.x.x.x |
| Virtual machine  Physical computer | Installation of the ATA Center as a virtual machine is supported.  <<Update this section to reflect choice reasoning>> | Physical or Virtual |
| BIOS | The ATA database requires that Customer Name DISABLE nonuniform memory access (NUMA) in the BIOS. | Confirm Disabled (Y, N) and add commentary if the answer is “N”. |

* + 1. Network Ports

**Instruction:** Modify the tables in this section to record the customer’s specific configuration needs for this solution. Remove or configure optional configuration items.

The following table lists the minimum ports that are needed by the ATA Center.

Table 82: Requirements—ATA Center Network Ports

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Protocol | Transport | Port | To or From | Direction | IP Address |
| SSL (ATA communications) | TCP | 443 | ATA Gateway | Inbound | ATA Center Service IP Address: x.x.x.x |
| HTTP | TCP | 80 | Customer Name network | Inbound | Management IP (IIS) Address: x.x.x.x |
| HTTPS | TCP | 443 | Customer Name network and ATA Gateway | Inbound | Management IP (IIS) Address: x.x.x.x |
| SMTP (optional) | TCP | 25 | SMTP server | Outbound | Management IP (IIS) Address: x.x.x.x |
| SMTPS (optional) | TCP | 465 | SMTP server | Outbound | Management IP (IIS) Address: x.x.x.x |
| Syslog (optional) | TCP | 514 | Syslog server | Outbound | Management IP (IIS) Address: x.x.x.x |

* 1. ATA Lightweight Gateway
     1. Hardware Configuration

**Instruction:** it is recommended that the customer, where possible and where existing DC compute resources can handle it, deploy the lightweight Gateway where possible. Please modify the tables in this section to record the customer’s specific configuration needs for this solution.

**Note:** If the Domain Controller does not have the necessary amount of resources required by the ATA Lightweight Gateway, the domain controller performance will not be effected, but the ATA Lightweight Gateway might not operate as expected.

**Caution Note:** The ATA Lightweight Gateway includes a monitoring component which evaluates the available compute and memory capacity on the domain controller on which is is running. The monitoring process runs every 10 seconds and dynamically updates the CPU and memory utilization quota on the ATA Lightweight Gateway process to make sure that at any given point in time, the domain controller has at least 15% of free compute and memory resources.

An ATA Lightweight Gateway will support and monitor only the Domain Controller it is installed on. The following table details the in-scope Domain Controllers that the ATA Lightweight Gateway is installed on.

Table 93: Requirements—ATA Gateway Hardware

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

* + 1. Network Ports

Table 104: Requirements—ATA Lightweight Gateway Network Ports

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protocol | Transport | Port | To or From | Direction |
| DNS | TCP and UDP | 53 | DNS Servers | Outbound |
| NTLM over RPC | TCP | 135 | All devices on the network | Outbound |
| NetBIOS | UDP | 137 | All devices on the network | Outbound |
| SSL | TCP | 443 | Update this cell to include the ATA Center service IP address and the ATA Console IP address.  ATA Center:  Center Service IP Address  IIS IP Address | Outbound |
| Syslog (optional) | UDP | 514 | SIEM Server | Inbound |

**Note:** As part of the resolution process performed by the ATA Lightweight Gateway, the following ports need to be open inbound on devices on the network from the ATA Lightweight Gateways:  
 NTLM over RPC  
 NetBIOS

* 1. ATA Gateway
     1. Hardware Configuration

**Instruction: i**f you are not deploying any full ATA Gateway systems, you may delete this section. Otherwise, modify the tables in this section to record the customer’s specific configuration needs for this solution if the deployment consists of deploying full ATA Gateways.

**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 5GB of memory. Once this limit is reached, it will stop collecting network traffic until communication is restored with the Center. Depending on the domain controller load, this can be hours or minutes.

An ATA Gateway will support multiple domain controllers and is based on the amount of traffic domain controllers send and receive; the following configuration is recorded.

Table 115: Requirements—ATA Gateway Hardware

|  |  |  |
| --- | --- | --- |
| Component | Gateway Hardware Details | Configuration |
| Processor | See Gateway-sizing section (Table 6: ATA Gateway Sizing). | Update based on sizing exercise here |
| Memory | See Gateway-sizing section (Table 6: ATA Gateway Sizing) | Update based on sizing exercise here |
| Network | The Gateway requires two or more network adapters:   * A **management adapter** will be used for communications on the company network. * A **capture adapter** will be used to capture traffic to and from the domain controllers. | **Management:**  This adapter will be configured as follows:  Management IP: x.x.x.x  Preferred and Alternate DNS Servers: x.x.x.x & x.x.x.x  DNS Suffix for Connection: contoso.com  DNS suffix for this connection” should be the DNS name of the domain being monitored  **Capture:**  This adapter will be configured as follows:  Capture IP Address: 1.1.1.1  Capture Subnet: 255.255.255.255  Configure port mirroring for the capture adapter as the destination of the domain controller network traffic. |
| Virtual machine  Physical computer | Update this section to reflect choice reasoning  Installation of the ATA Gateway as a virtual machine is supported if the domain controllers that are being monitored are also running as virtual machines on the same virtualization host. | Type in “Physical” or “Virtual” depending on customer’s choice. If virtual, list the virtualization platform. |

* + 1. Network Ports

**Instruction:** modify the tables in this section to record the customer’s specific configuration needs for this solution. Remove or configure optional configuration items.

The following table lists the minimum ports that the ATA Gateway requires to be configured on the management adapter.

Table 16: Requirements—Gateway Network Ports

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protocol | Transport | Port | To or From | Direction |
| LDAP | TCP and UDP | 389 | Domain controllers | Outbound |
| Secure LDAP (LDAPS) | TCP | 636 | Domain controllers | Outbound |
| LDAP to Global Catalog | TCP | 3268 | Domain controllers | Outbound |
| LDAPS to Global Catalog | TCP | 3269 | Domain controllers | Outbound |
| Kerberos | TCP and UDP | 88 | Domain controllers | Outbound |
| Netlogon | TCP and UDP | 445 | Domain controllers | Outbound |
| Windows Time | UDP | 123 | Domain controllers | Outbound |
| DNS | TCP and UDP | 53 | DNS Servers | Outbound |
| NTLM over RPC | TCP | 135 | All devices on the network | Outbound |
| NetBIOS | UDP | 137 | All devices on the network | Outbound |
| SSL | TCP | 443 | Update this cell to include the ATA Center service IP address and the ATA Console IP address.  ATA Center:  Center Service IP Address  IIS IP Address | Outbound |
| Syslog (optional) | UDP | 514 | SIEM Server | Inbound |

* + 1. Port-Mirroring Considerations

The main data source ATA uses comes from deep-packet inspection of network traffic to and from your domain controllers. Port mirroring needs to be configured before ATA can access that network traffic. Port mirroring copies the traffic from the source port to the destination port. ATA works with most solutions that can mirror traffic—if the traffic can be port-mirrored to ATA, it can be used to analyze threats to your system.

The following table outlines Gateway considerations for port mirroring in physical computer or virtual machine scenarios.

Table 17: Port-Mirroring Considerations

|  |  |  |
| --- | --- | --- |
| ATA Gateway | Domain Controller | Considerations |
| Virtual | Virtual on same host | * The virtual switch needs to support port mirroring. * Moving one of the virtual machines to another host by itself might cause port mirroring to not work. |
| Virtual | Virtual on different hosts | Confirm that your virtual switch supports this scenario. |
| Virtual | Physical | This requires a dedicated network adapter. Otherwise ATA will see the traffic that is coming in and out of the host, including the traffic it sends to the ATA Center. |
| Physical | Virtual | Confirm that your virtual switch supports this scenario and that the port-mirroring configuration of your physical switches is 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 a remote switched port analyzer (RSPAN) or an encapsulated remote switched port analyzer (ERSPAN)\*. |
| Physical | Physical on the same switch | The physical switch must support a switched port analyzer (SPAN) or port mirroring. |
| Physical | Physical on a different switch | This requires physical switches to support RSPAN or ERSPAN\*. |

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

Virtual Gateways are required for each virtualization host on which a virtual domain controller is running.

To configure port mirroring, Customer Name needs to refer to the vendor's documentation.

* + 1. Port-Mirroring Configuration—Hyper-V

**Instruction:** Modify the tables in this section to record the customer’s specific configuration needs for this solution. Remove or configure optional configuration items. Elaborate on the configuration below.

The following table outlines the Hyper-V configuration that will be used for this solution:

Table 8: Port-Mirroring Configuration

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Type | Virtual Machine Name | Virtual Machine Host |
| Center | Destination | Enter VM Name | Enter Host Name |
| Gateway | Source | Enter VM Name | Enter Host Name |

**Note:** This is a feature in Microsoft Hyper-V Virtual Switch that was added to Windows Server 2012. Thus, the virtualization hosts need to run (at minimum) Windows Server 2012.

* 1. ATA Configuration

The information in this section is configured through the ATA portal (that is, the management interface) and helps configure ATA to verify that it is capturing information about your environment in an efficient manner.

* + 1. ATA General Configurations

**Instruction:** Update the information in this section with the settings that you applied for the customer’s ATA deployment. Each subsection lists a table that has entries you will update to depict their final ATA deployment configuration. These items are located under the “ATA General” section of the “Configuration” window.

* + - 1. ATA Center

**Instruction:** Update the following table with information specific to your customer deployment.

Table : ATA Center Configuration

|  |  |  |
| --- | --- | --- |
| Setting | Value | Comments |
| ATA Center Service IP Address and Port |  |  |
| Certificate |  |  |
| Language |  |  |

* + - 1. ATA Console

**Instruction:** Update the following table with information specific to your customer deployment.

Table : ATA Console Configuration

|  |  |  |
| --- | --- | --- |
| Setting | Value | Comments |
| ATA Console URL |  |  |

* + - 1. ATA Role Based Access Control – RBAC

ATA includes three roles with different sets of permissions. These groups are created as local security groups.

**Instruction:** Update the following table with information specific to your customer deployment.

Table : ATA Console Configuration

|  |  |  |  |
| --- | --- | --- | --- |
| Group Name | Members | | Comments |
| Microsoft Advanced Threat Analytics Administrators  *Team in charge of deploying and managing ATA (adding new gateways, etc).* | Username/group:  Domain: |  | |
| Microsoft Advanced Threat Analytics Users  *Permissions to change and manage alert states (team in charge to follow-up / handle alerts generated by ATA).* | Username/group:  Domain: |  | |
| Microsoft Advanced Threat Analytics Viewers  *Team(s) that might be interesting to leverage ATA information for their daily activities (security team, misc. admins, etc.)* | Username/group:  Domain: |  | |

* + - 1. ATA Gateways

**Instruction:** Update the following table with information specific to your customer deployment.

Table : ATA Gateway Configuration

|  |  |  |
| --- | --- | --- |
| Setting | Value | Comments |
| Domain Connectivity | Username:  Domain: |  |
| Update ATA Gateways automatically |  |  |

* + 1. ATA Gateways Configuration

**Instructions:** Update the following table with information for all Gateways that are being deployed for this customer.

Table : ATA Gateway Configuration Details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gateway Name | Gateway Type | DC’s Monitored | Domain Synchronizer Candidate (Yes/No) | Syslog Listener (Yes/No) | Windows Event Forwarding Collection (Yes/No) | Comments |
| ATA GW1 | Lightweight | DC1.Contoso.Com | Yes | No | Yes | This Gateway has been installed onto DC1. |
| ATA GW2 | Full | DC2.Contoso.Com  DC3.Contoso.Com | Yes |  |  | This Gateway is monitoring multiple DC’s in the “Seattle” AD site. |

* + 1. ATA Detection Configurations
       1. Short-Term Lease Subnets

**Instruction:** Identify the subnets in which IP addresses are reassigned between devices within a very short period of time (seconds or minutes) and update the following table with appropriate information for each subnet.

ATA reduces the cache lifetime for all IP addresses in these subnets to accommodate the fast reassignment between devices. VPN or Wi-Fi networks are common examples of short-term lease subnets.

Short-term lease subnets are subnets in which IP address assignment changes within seconds or minutes. This includes IP addresses that are used for VPNs and wireless networks. It is important to configure ATA to recognize those subnets to avoid the possibility of ATA flagging legitimate activities from these devices as suspicious. This can help keep ATA from issuing warnings about activities that are in fact expected (this is called false positive identification).

ATA will be configured to consider the following subnets as short-term lease subnets.

**Instruction:** Update the following table with specific information about network subnets that ATA will exclude using the short-term lease configuration option.

Table 189: Short-Term Lease Subnets

|  |  |  |
| --- | --- | --- |
| Lease Function | Details | Subnet/Bit Range |
| Enter Subnet ID/Name | Provide details about subnet | Enter Subnet Range and Bit Mask Info:  e.g. 1.2.3.4/24 |

* + - 1. Honey Token Configuration

A honey token account is a user account that has been created to attract a potential attacker. This account is typically set up to appear as a higher-level access account but it is actually configured with minimal capabilities and is monitored heavily. This account should be named in a way that would attract unwanted use but it should be heavily locked down so that if it is actually used, it cannot do anything in the environment. If you use this type of an account, verify that it does not have the ability to log on interactively or be used to enumerate your directory.

ATA has the ability to monitor such an account and will alert you if it is used. The following table provides information about a honey token user that you can configure ATA to monitor:

**Instructions:** Update the following table with the information of the honey token account that will be used for your customer’s ATA deployment. If monitoring more than one forest, please add additional rows.

Table 21: Honey Token Configuration

|  |  |  |  |
| --- | --- | --- | --- |
| Account Name | SID | AD Forest Location | Explanation |
| IMADomanAdmin | S-1-5-21-3557858698-2536648719-2954018678-1141 | Contoso.com | This account is located in the contoso.com forest and has been restricted to not logon interactively nor can it read AD. ATA will monitor the attempted use of this account object. |

* + - 1. DNS Reconnaissance Exclusions

ATA can determine whether someone is attempting (as a possible attack tactic) to capture Domain Name System (DNS) information. Such an attack often consists of attempting to complete zone transfers or obtaining information from a DNS zone in hopes of gaining valuable information about your overall network and your devices.

Such an attack could be mistaken as a legitimate DNS zone transfer from another DNS server in the environment. To help avoid an inaccurate identification, ATA can be configured to exclude addresses of such DNS servers. You would not be alerted if, or when, updates are made to their zone databases. The following table lists the systems that your ATA configuration will exclude from your DNS reconnaissance activities.

**Instruction:** update the following table with a list of DNS servers that ATA will be configured to exclude from DNS reconnaissance reviews.

Table 20: Customer Name DNS Server Exclusions

|  |  |
| --- | --- |
| DNS Server Name | IP Address |
|  |  |

* + - 1. Pass-the-ticket IP address exclusions

**Instruction:** If the customer has Pass-the-ticket exclusions, please fill out this section. Otherwise remove the last sentence, delete the table and type a statement stating that the customer does not have any Pass-the-ticket exclusions.

Some applications may perform authentication in a manner that ATA determines is a Pass-the-ticket suspicious activity. If after investigation, you have determined that the application is functioning accordingly, you should consider excluding it from the Pass-the-ticket detection rule. To do so, you add a pass-the-ticket exclusion listing the IP address of the host where the application is running. The following table illustrates which areas were excluded:

|  |  |
| --- | --- |
| Server Name | IP Address |
|  |  |

* + 1. Email Server Configuration

The following table contains the email alerting configuration.

**Instruction:** Please update the following table to illustrate specific configuration information for your customer.

Table 193: Email Alerting Configuration

|  |  |  |
| --- | --- | --- |
| Field | Description | Value |
| SMTP server endpoint (required) | The FQDN of the SMTP server. | For example: smtp.contoso.com |
| SSL | Toggle SSL if the SMTP server required SSL.   |  | | --- | | **System_CAPS_noteNote** | | **If the administrator enables SSL, Customer Name will also need to change the Port number.** | | Default is disabled |
| Authentication | Enable if the SMTP server requires authentication.   |  | | --- | | **System_CAPS_noteNote** | | **If Customer Name enable authentication, the administrator must provide the user name and password of an email account that has permission to connect to the SMTP server.** | | Default is disabled |
| Send from (required) | The email address that the alert will be sent from. | For example: ATA@contoso.com |

* + 1. Syslog Server Configurations

ATA may be configured to forward information about the suspicious activities it detects to Security Information and Event Management (SIEM) systems. ATA may send information using two specific RFC formats; 5424 and 3164. The settings are specific to the listening SIEM endpoint system. The following table lists the settings for Customer Name’s SIEM integration:

**Instruction:** Update the following table to reflect the settings used by your customer. If you are not configuring SIEM integration as a part of this deployment, you may add the following statement:

Table : Syslog server configuration

|  |  |  |  |
| --- | --- | --- | --- |
| Syslog Server Endpoint | Port | Transport | Format |
| Syslog.contoso.com | 514 | UDP | RFC5424 |

* + 1. Notification Settings
       1. Email Notifications

**Instruction:** the following section is the recording of the e-mail notifications configuration. Please update with your customer’s settings.

This section outlines the email notification configuration that will be used for Customer Name’s ATA deployment. Using this configuration, ATA will send email alerts using the following settings:

Table : Email notifications configurations

|  |  |
| --- | --- |
| Value | Setting |
| New suspicious activity is detected | Enabled |
| New health issue is detected |  |
| New software update is available |  |
| Email recipients |  |

* + - 1. Syslog notifications

**Instruction:** the following section is the recording of the syslog notifications configuration. Please update with your customer’s settings. If you are not configuring SIEM integration as a part of this deployment, you may add the following statement:

SIEM integration is out of scope for this deployment and there has not been any configuration settings set for this configuration option.

This section outlines the syslog notification configuration that will be used for Customer Name’s ATA deployment. Using this configuration, ATA will send information to syslog servers (e.g. SIEM systems) using the following settings:

Table : Syslog notification settings

|  |  |
| --- | --- |
| Value | Setting |
| New suspicious activity is detected | Enabled |
| Existing suspicious activity is updated |  |
| New health issue is detected |  |

* 1. Additional Network Configuration Information

**Instruction:** modify the tables in this section to record the customer’s specific configuration needs for this solution.

This section provides network configuration information that can help with the deployment of the ATA solution for Customer Name.

* + 1. Endpoint or Device Firewall Configuration

To adequately provide detection services, ATA needs access to information about the devices that are on the network. To do this, a series of network ports must be opened between the ATA Gateways and devices that are located in the environment that ATA is reviewing. The following table illustrates the ports that must be opened if there are firewalls between the ATA Gateway and the devices in your network environment.

Table 234: Endpoint Firewall Configuration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port Name | Type | Port | Entities | Direction |
| NetBIOS | UDP | 137 | All devices on the network | Inbound |
| NTLM over RPC | TCP | 135 | All devices on the network | Inbound |

* 1. Event Collection

**Instructions:** This section is **optional**. The scope of the default offer does not include SIEM integration. If your deliver has included it, please leverage this section for configuration specific details for your delivery. If not, please delete this section.

Modify this section to record the customer’s specific configuration needs for this solution. Remove or configure optional configuration items. If not relevant to the design, please remove this section. Note: Configuration of the SIEM servers is the customer’s responsibility.

To enhance ATA detection of Pass-the-Hash malicious hacking attempts, ATA requires Windows Event Log ID 4776. This can be forwarded to the ATA Gateway in one of two ways—by configuring the ATA Gateway to monitor SIEM events or by using Windows event forwarding to capture specific Windows events that are logged and captured within the domain controllers event logs.

* + 1. Configuration of ATA Gateway to Listen for SIEM Events

**Instruction:** Update the following table with specific information.

Table 25: SIEM Configuration—Gateway

|  |  |  |
| --- | --- | --- |
| Listening IP Address (Gateway) | Port Type | Port (Default) |
| <<EnterIPHere>> | UDP | 514 |

* + 1. Configuration of Windows Event Forwarding

**Instructions:** If the customer does not have a SIEM server you can configure your domain controllers to forward Windows Event ID 4776 directly to one of your ATA Gateways. This is out of scope for this engagement by default. Customer needs to configure WEF on the Domain Controllers. This is a pure record if the customer configures WEF.

Customer Name can collect events from remote computers and store them in logs on a local computer. The following section contains the configuration for Customer Name related to specific events that are to be collected through the creation of a subscription.

The following table lists Customer Name domain controllers that will be used to forward Windows Event ID 4776 to the ATA Gateways.

**Instruction:** Update the following table with specific information for Windows Event Forwarding for your customer’s deployment. If you are configuring multiple listeners for multiple forests, please add a subsection for each forest name and copy/paste the sample table provided.

Table 246: Windows Event Forwarding—Domain Controllers to Gateway

|  |  |  |
| --- | --- | --- |
| Configuration Item | Computers | Details |
| Source | Enter DomainControllerFQDN | Source domain controllers |
| Collector | Enter ATAGateway FQDN | ATA Gateway |
| Subscription name | Enter Subscription Name | Created on the collector |
| Event log readers group | Enter Source Computers FQDN | Created on the collector |