Test Plan



Advanced Threat Analytics Implementation Services

Prepared for

[Type Customer Name Here]

Date

Version 1 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 Test Case Summary 1](#_Toc454802402)

[2 Test Case Approach and Assumptions 3](#_Toc454802403)

[3 Test Case Environment Specification 4](#_Toc454802404)

[3.1 Test Case Planning 4](#_Toc454802405)

[3.1.1 Test Case Scope 4](#_Toc454802406)

[3.1.2 Schedule 6](#_Toc454802407)

[3.2 Testing Environment 7](#_Toc454802408)

[3.3 Testing Environment Requirements 7](#_Toc454802409)

[3.3.1 Sizing Requirements 8](#_Toc454802410)

[3.3.2 Hardware Requirements 9](#_Toc454802411)

[3.3.3 Software Requirements 12](#_Toc454802412)

[3.3.4 Pre-deployment Requirements 14](#_Toc454802413)

[3.4 Testing Environment Configuration 14](#_Toc454802414)

[3.4.1 Lab Network Configuration 14](#_Toc454802415)

[3.4.2 ATA Center Configuration 14](#_Toc454802416)

[3.4.3 ATA Gateway Configuration 15](#_Toc454802417)

[4 Test Cases and Results 17](#_Toc454802418)

[4.1 Test Cases 17](#_Toc454802419)

[4.1.1 Test Case 1: Validate Port Mirroring 17](#_Toc454802420)

[4.1.2 Test Case 2: Validate Stable Network Communications 18](#_Toc454802421)

[4.1.3 Test Case 3: Installing the ATA Center 19](#_Toc454802422)

[4.1.4 Test Case 4: Configure the ATA Gateway Domain Connectivity Settings 20](#_Toc454802423)

[4.1.5 Test Case 5: Download the ATA Gateway Setup Package 21](#_Toc454802424)

[4.1.6 Test Case 6: Install the ATA Gateway 22](#_Toc454802425)

[4.1.7 Test Case 7: Configure the ATA Gateway Settings and Verify it is Operational 23](#_Toc454802426)

[4.1.8 Test Case 8: Configure Short-Term Lease Subnets and Honeytoken User 25](#_Toc454802427)

[4.1.9 Test Case 9: ATA Alerting (Notification Settings) 26](#_Toc454802428)

[4.1.10 Test Case 10: Identifying and Working with ATA Alerts and Suspicious Activities 27](#_Toc454802429)

[4.1.11 Test Case 11: Validate that ATA is functioning properly 28](#_Toc454802430)

[4.1.12 Test Case 12: ATA Heath Center 29](#_Toc454802431)

[4.1.13 Test Case 13: Database Management 29](#_Toc454802432)

[4.2 Test Case Results Summary 31](#_Toc454802433)

[5 Risks and Dependencies 33](#_Toc454802434)

[6 Open Issues 34](#_Toc454802435)

Tables

[Table 1: Test Case Scope Items 5](#_Toc454802557)

[Table 2: Requirements – ATA Center Sizing 8](#_Toc454802558)

[Table 3: Requirements – ATA Lightweight Gateway Sizing 8](#_Toc454802559)

[Table 4: Requirements – ATA Gateway Sizing 9](#_Toc454802560)

[Table 5: ATA Center Configuration 9](#_Toc454802561)

[Table 6: ATA Lightweight Gateway Hardware 10](#_Toc454802562)

[Table 7: Requirements—ATA Gateway Hardware 11](#_Toc454802563)

[Table 8: Requirements—ATA Center Software 12](#_Toc454802564)

[Table 9: Requirements—ATA Gateway Software 13](#_Toc454802565)

[Table 10: Lab Network Segments 14](#_Toc454802566)

[Table 11: ATA Center Configuration 14](#_Toc454802567)

[Table 12: ATA Gateway Configuration 15](#_Toc454802568)

[Table 13: Test Case 1 17](#_Toc454802569)

[Table 14: Test Case 2 18](#_Toc454802570)

[Table 15: Test Case 3 19](#_Toc454802571)

[Table 16: Test Case 4 20](#_Toc454802572)

[Table 17: Test Case 5 21](#_Toc454802573)

[Table 18: Test Case 6 22](#_Toc454802574)

[Table 19: Test Case 7 23](#_Toc454802575)

[Table 20: Test Case 8 25](#_Toc454802576)

[Table 21: Test Case 9 26](#_Toc454802577)

[Table 22: Test Case 10 27](#_Toc454802578)

[Table 23: Test Case 11 28](#_Toc454802579)

[Table 23: Test Case 12 29](#_Toc454802580)

[Table 24: Test Case 13 30](#_Toc454802581)

[Table 25: Test Results 31](#_Toc454802582)

[Table 26: Risk Identification 33](#_Toc454802583)

[Table 27: Open Issues 34](#_Toc454802584)

Figures

[Figure 1: High-level Architecture 7](#_Toc454802464)

**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](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

Template Guidance

Note there are samples of this document available. Please go to this [link](https://spsites.microsoft.com/sites/esaponline/Pages/Lessons_Learnt_Landing_Page.aspx?area=&discipline=&category=Deliverable%20Type%20%28SDM%29*&IsSubmitted=yes) to see a list.

The Test Plan template examines the processes as they exist in a live testing environment where the Planning > Defining > Performing/Executing > Reporting test flow is followed, keeping in mind that often you need to refine the test process as the product is constructed.

Description: The Test Plan describes the strategy and approach used to plan, organize and manage the project’s testing activities. It identifies testing objectives, methodologies and tools, expected results, responsibilities and resource requirements. This document is the primary plan for the testing team.

Justification: A Test Plan ensures that the testing process will be conducted in a thorough and organized manner that enables the team to determine the stability of the ssolution. A continuous understanding of the solution’s status builds confidence in team members and stakeholders as the solution is developed and stabilized.

Team Role Primary: Test is responsible for the creating the Test Plan. This plan outlines the strategy the team will take to test the solution. The test role is responsible for setting the quality expectations and incorporating those into the testing plan.

Team Role Secondary: Program Management participates in developing the test plan by ensuring that the solution requirements are met, the correct components are tested, and appropriate strategies are adopted for bug reporting and resolution. Development needs to understand how their work will be tested and how the bugs will be reported, assigned, resolved, and verified. User Experience verifies that the Test Plan contains the strategies and methods to test accessibility, usability and interface features.

1. Test Case Summary

Provide an overall summary of the contents of this document.

Justification: Some readers may need to know only the highlights of the plan, and summarizing creates that user view. It also enables the full reader to know the essence of the document before they examine the details.

When planning projects, often delivery teams focus on implementing Microsoft Advanced Threat Analytics (ATA), which gains an immediate potential benefit from quicker results and apparent satisfaction from [Type Customer Name Here]. Focusing on the implementation of ATA first puts tasks such as planning and predeployment as secondary in importance. A significant number of these projects fail, not because of major issues or failings in the technology, but because they lack understanding of how the technology operates and how thorough testing of the deployed technology in a production-simulated environment is imperative to a viable solution.

To avoid failure, the delivery team needs to test ATA before the technology can be deployed and operated in the actual production environment. This is done by:

* Determining how the completed solution works and interacts with the production environment.
* Verifying the constraints and assumptions about ATA.
* Making sure that the solution design elements meet business requirements before proceeding with production deployment.

It is in the test environment, not in the production environment, that the teams will make sure that the ATA solution works as expected. This verifies that the support staff understands how to operate the solution and how to validate the technical solutions design. When performed in a test environment that simulates [Type Customer Name Here]’s exact production environment, the tests referred to in this document can help build a high degree of confidence in the solution and in the skills and abilities of those involved.

By creating a thorough test plan, and performing good testing throughout the development process of the ATA solution, [Type Customer Name Here] will:

* Minimize risk.
* Provide support staff with needed skills and experience.
* Reduce the costs associated with poor or weak solutions design elements.

Without affecting the user, in a test environment, technical staff members will:

* Observe a solution design in operation.
* Change configuration settings.
* Fine-tune the design to confirm improved performance.

1. Test Case Approach and Assumptions

Use this section to describe at a high level the approach, activities, and techniques (including techniques for designing tests) to be followed in testing the solution. If different approaches are required for the solution’s various components, this section should define which components would be tested by each approach.

This section also describes the processes (criteria and techniques) that will be used to verify that the testing approach chosen will effectively guarantee the required degree of test completeness. A process could be as simple as requiring all appropriate groups to review, comment and sign off on the document. A process could be more complex, requiring the use of tools to verify statement and path coverage.

The tests were conducted in an isolated lab environment that represents the [Type Customer Name Here] architecture as closely as possible to conduct the verification tests.

A combination of virtual and physical resources was used to build and manage the environment. This document works in conjunction with the Implementation Guide and the Operations Guide that form part of this engagement.

1. Test Case Environment Specification

Use this section to detail the test plan including Team Model, Scope of the Test, and to set standards and requirements for the documentation to be generated during the process.

Justification: the Testing Team must decide on what tool/process to use for reporting the results of testing. A computer-based tool allows the coordinator to monitor test results, develop result reports that can be passed on to the core team and other stakeholders, and track testing status. The test team should also specify tools needed to monitor operating effects of the new release on the computing environment.

It is important for the test team to establish and maintain the test environment as if it were [Type Customer Name Here]’s live environment. Adequate testing of the ATA solution design can only be performed in a test environment that is as close as possible to the live environment. Coordinating the establishment of the test environment with the core team helps to determine the requirements for mirroring the live environment.

* 1. Test Case Planning

The testing team is responsible for developing an overall test plan that includes the following for each individual test to be performed:

* Test case scope
* Schedule
* Risks
* Test design
* Documentation requirements
* Resource requirements
* Problem and issue resolution
  + 1. Test Case Scope

Describe what will and will not be covered in the testing activity. Emphasize the testing areas where potential problems pose the greatest risk to the organization or have the greatest probability of occurring. As the Testing Team develops the test designs and gains a better understanding of the time required performing them, they will further refine the testing scope.

Justification: the objectives section should clearly state the test objectives so that anyone reviewing the documentation can easily understand what the testing is intended to accomplish. Clear and meaningful objectives also help shed light on the importance of the service the Testing Team is providing through their testing efforts. Modify this table as appropriate. TS= TEST CODE

The following test scope items will be verified as part of this test plan.

Table 1: Test Case Scope Items

| Identification Code | Test Item | Details |
| --- | --- | --- |
| TC1 | Validate port mirroring. | This item is a requirement for the implementation and operation of the solution to provide detection data. |
| TC2 | Validate stable network communications between the ATA Center and the Gateway servers. | No ATA components are installed at this time, only the communications test. |
| TC3 | Install the ATA Center. | Installing the ATA Center successfully will allow the rest of the solution to be implemented successfully. |
| TC4 | Configure the ATA Gateway domain connectivity settings. | This will make sure that ATA can be set up successfully and be able to catalog entities from Active Directory Domain Services (AD DS), such as users, groups, and computer objects. |
| TC5 | Download the ATA Gateway setup package. | This package prepares the user for the installation of the ATA Gateway. |
| TC6 | Install the ATA Gateway. | Installing the ATA Gateway successfully will allow the solution to start intercepting network traffic for analysis and alerting. |
| TC7 | Configure the ATA Gateway settings. | The ability to manipulate ATA Gateway configuration items. |
| TC8 | Configure short-term lease subnets and a honeytoken user. | **Optional if configured in the Solutions Design document:** Configuration of  short-term leased subnets, such as a virtual private network (VPN) or others, and a honeytoken user account security identifier (SID). |
| TC9 | Configure ATA Alerting (notification settings). | The ability to successfully set up email alerting when ATA detects suspicious activities; alerts are sent to a distribution list or administrator. |
| TC10 | Identify and work with ATA alerts and suspicious activities. | Updating, resolving, or dismissing alerts in the ATA Console. |
| TC11 | Install ATA Heath Center. | The ATA Health Center provides a view of the health of ATA. This includes the communication status between the ATA Center and the ATA Gateway. |
| TC12 | Install database management. | The ability to backup, restore, and manage the ATA MongoDB database. |

* + 1. Schedule

Draft schedule, including all of the tests listed in the Test Design section of the Overall Test Plan, to show when each test will be performed and who will perform it. If the test environment is being used for more than one purpose, the schedule can help testers coordinate availability with other possible testing teams. You can provide the project plan timeline here for the stabilization phase of this project.

The following schedule outlines the timeline that will be followed to start and complete the testing phase of this engagement.

<<Paste timeline for the stabilization phase here from the master project plan>>

* 1. Testing Environment

Identify the approach and procedures that will be used for the initial phase of the test. This approach should define the steps of the setup process. The setup process should include the staging requirements for the testing and the procedures to initialize the testing matrix. Update the diagram below to reflect your customer’s testing environment.

The following diagram shows the high-level architecture deployed in the lab environment. A minimum of two domain controllers will be required for this environment.

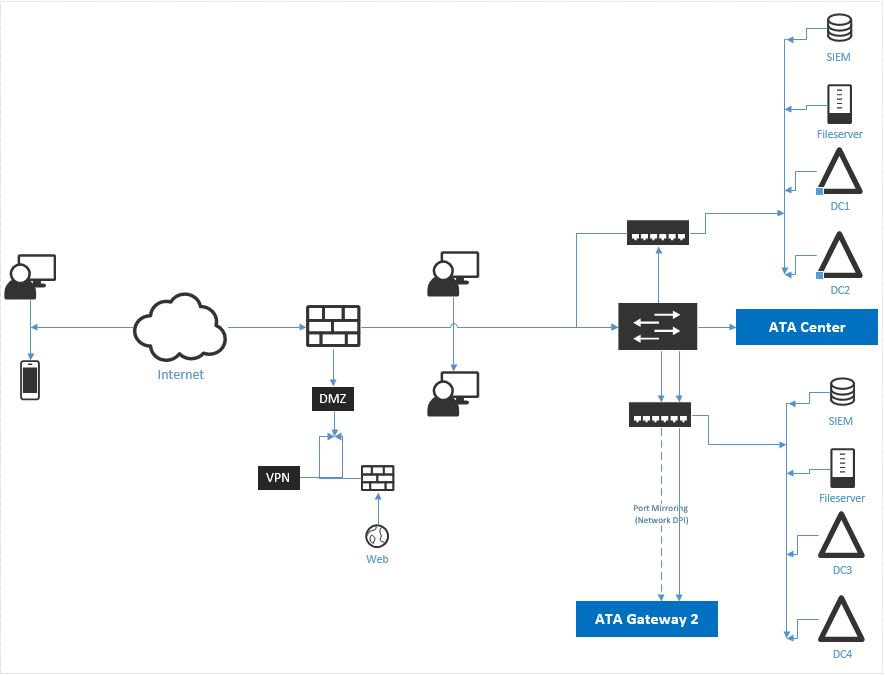


Figure 1: High-level Architecture

* 1. Testing Environment Requirements

Update this section to reflect the relevant sizing of the testing environment.

* + 1. Sizing Requirements
       1. ATA Center

Table 2: Requirements – 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 domain controllers being monitored by ATA Gateways.

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

* + - 1. ATA Gateway

Table : 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 number of packets-per-second on the domain controller being monitored by the specific ATA Lightweight Gateway.

\*\* Total amount of non-hyperthreaded cores that this domain controller has installed. While hyperthreading 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.

Table 4: 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 average number of packets-per-second from all domain controllers being monitored by the specific ATA Gateway during their busiest hour of the day. Furthermore, the total amount of domain controller port-mirrored traffic cannot exceed the capacity of the capture network interface card (NIC) on the ATA Gateway.

\*\*Hyperthreading must be disabled.

* + 1. Hardware Requirements
       1. ATA Center

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

Table 5: ATA Center Configuration

| Component | ATA 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 Gateway is encrypted using Secure Sockets Layer (SSL) on port 443. Additionally, the ATA Management Console runs on Internet Information Services (IIS) and is secured 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:** Confirm a stable and effective network connection between the ATA 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 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 Center as a virtual machine is supported. |
| BIOS | The ATA database requires that [Type Customer Name Here] 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

Table : ATA Lightweight Gateway Hardware

| Component | ATA Lightweight Gateway Hardware Requirements |
| --- | --- |
| Processor | Refer to sizing requirements. |
| Memory | Refer to sizing requirements**.** |
| Network | **Note:** The ATA Lightweight Gateway monitors local traffic on all of the domain controller’s network adapters. After deployment, you can use the ATA console if you want to modify which network adapters are monitored.  **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 |
| Virtualization | Installation of the ATA Lightweight Gateway as a virtual machine is supported on Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Standard and Datacenter editions. The Lightweight Gateway is *not supported on Server Core*. The domain controller can be a read-only domain controller (RODC). |

* + - 1. ATA Gateway

An ATA Gateway can support monitoring multiple domain controllers (depending on the amount of network traffic to and from the domain controllers), or a single domain controller, where the ATA Lightweight Gateway is installed.

Table 7: Requirements—ATA Gateway Hardware

| Component | ATA 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 send it to the ATA Center. This is at a default setting of 1,000,000 entities and is configurable. Depending on the load of the domain controller connected to the ATA Gateway, this can generate a tremendous amount of data.  **Caution:** If communication between the ATA Center and the ATA Gateway is disrupted, the ATA 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 ATA Center. Depending on the domain controller load, this can be hours or minutes. |
| 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:   * A static IP address, including a default gateway. * Preferred and alternate Domain Name System (DNS) servers. * “DNS suffix for this connection” should be the DNS name of the domain being monitored.   **Capture adapter:** Will be used to capture traffic to and from the domain controller:   * Configure port mirroring for the capture adapter as the destination of the domain controller network traffic. * Configure a static nonroutable 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 can capture 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 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 virtual machine is supported when the domain controllers being monitored are also running as virtual machines on the same virtualization host.  **Important:** 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 8: Requirements—ATA Center Software

| Component | Center Software Requirements |
| --- | --- |
| Certificates | ATA Center requires certificates for the following services:   * IIS, which is a web server certificate * ATA Center service, which is a server authentication certificate |
| Operating System | Use 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. |
| User Account | **Local Administrator (non-domain joined)**  **Standard User Account (domain joined)**—Added to local admin, 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 Windows 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 the latest Microsoft updates have been installed on the server. |

* + - 1. ATA Gateway

This section provides the software requirements for the ATA Gateway.

Table 9: Requirements—ATA Gateway Software

| Component | 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 if using the ATA Gateway.  Only the ATA Lightweight Gateway can be installed on Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Standard or Datacenter Edition domain controllers. *Server Core is not supported.* |
| Domain or Workgroup Membership | The ATA Gateway can be installed on a server that is a member of a domain or workgroup. The ATA Lightweight Gateway *must* be installed on a domain controller. RODCs are supported. |
| User Accounts | **Local Administrator (non-domain joined)**  **Standard User Account (domain joined)**—Added to local admin, ATA Administrators.  **Standard Service Account**—Used to query Active Directory for indexing and object or entity cataloguing. (Domain Connectivity)  **Honeytoken account**—SID to be used (optional). A user account of 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) TechNet article. |
| 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 * .NET Framework 4.6.1 * Custom Performance Monitor data collection set |
| Microsoft Updates | Run Windows Update and make sure the latest updates have been installed prior to the installation of the ATA Gateway or ATA Lightweight Gateway. |
| Network Tracing Software | Do not install Microsoft 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. On the ATA Gateway, make sure that [KB 2919355](http://support.microsoft.com/kb/2919355/) has been installed. Run the following Microsoft PowerShell cmdlet to check if the hotfix is installed: Get-HotFix -Id kb2919355.
2. 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.
3. To validate port mirroring, see the ATAIS-Operations Guide as part of this engagement.
   1. Testing Environment Configuration
      1. Lab Network Configuration

Table 10: Lab Network Segments

|  |  |
| --- | --- |
| Network Segment Name | IPv4 Address |
| Lab network | <<10.0.0.0/24>> |
| Short-lease subnets |  |
| Other subnets |  |

* + 1. ATA Center Configuration

Table 11: ATA Center Configuration

| Component | Center Hardware Details | Configuration |
| --- | --- | --- |
| Processor | See Center sizing section. | <<Based on Sizing. Record here.>> |
| Memory | See Center sizing section. | <<Based on Sizing. Record here.>> |
| Available Disk Space  Database Storage | See Center sizing section. | <<Based on Sizing. Record here.>>  <<Record Database location here. Review operations and implementation guides for further requirements. It’s recommended to move the database to dedicated disks and drive.>> |
| Network | One network adaptor, two IP addresses:  ATA Center service  ATA Management (IIS) | <<IP1>>  <<IP2>> |
| Virtual Machine  Physical Machine | Installation of the ATA Center as a virtual machine is supported.  <<Update this section to reflect choice reasoning.>> | <<Virtual or Physical>> |
| BIOS | The ATA database requires that [Type Customer Name Here] DISABLE NUMA in the BIOS. | <<Confirm disabled>> |

* + 1. ATA Gateway Configuration

Table 12: ATA Gateway Configuration

| Component | Gateway Hardware Details | Configuration |
| --- | --- | --- |
| Processor | See Gateway sizing section. | <<Based on Sizing. Record here.>> |
| Memory | See Gateway sizing section. | <<Based on Sizing. Record here.>> |
| Available Disk Space | See Gateway sizing section. | <<Based on Sizing. Record here.>> |
| Gateway Type | ATA Lightweight Gateway or ATA Gateway | <<Based on Sizing. Record here.>> |
| Network | The Gateway requires two or more network adapters.  **Management adapter**: Will be used for communications on the company network.  **Capture adapter**: Will be used to capture traffic to and from the domain controllers.  **If the ATA Lightweight Gateway is used (preferred), make sure that the sizing and hardware requirements are met.** | **Management:**  This adapter will be configured as follows:   * <<Static IP>> * <<Preferred and alternate DNS servers>> * <<“DNS suffix for this connection” should be the DNS name of the domain being monitored.>>   **Capture:**  This adapter will be configured as follows:   * 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 /0.>> |
| Virtual Machine  Physical Machine | Installation of the ATA Gateway as a virtual machine is supported when the monitored domain controllers are also running as virtual machines on the same virtualization host.  <<Update this section to reflect choice reasoning>> | <<Virtual or physical>> |

1. Test Cases and Results

Use this section to provide a general description of the steps the tests will go through to ensure quality tests. Describe the detailed steps to be followed by testers during the testing cycle. Include a description of points where testing is suspended for documentation of results, expectations on re-initialization of the environment, and tests that are to be performed in sequence. Update the table below as the stages progress.

Remember, the customer will be signing and accepting this document so make sure you record your results thoroughly.

This section shows the steps and results of the testing performed by implementing ATA in a lab environment.

* 1. Test Cases
     1. Test Case 1: Validate Port Mirroring

Table : Test Case 1

| Test Case 1: Validate Port Mirroring | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | The process for validating that port mirroring is properly configured and operational. This test case is not required if the ATA Lightweight Gateway is used. | | | | | |
| Completion Steps | 1. Install [Microsoft Network Monitor 3.4](https://www.microsoft.com/download/details.aspx?id=4865) or another network sniffing tool on to the ATA Gateway system. 2. Enter the following filter: **Internet Control Message Protocol** (**ICMP),** and then click **Apply**. 3. Click **Start** to start the capture session. 4. From another host on the network that is not a domain controller, an ATA Center, or ATA Gateway, launch the Command Prompt window. 5. Ping (if ICMP is allowed) the first domain controller that the ATA Gateway will monitor continuously for about five minutes using **ping <hostname or IP> -t.** 6. Switch to the ATA Gateway system. 7. While on the Gateway, in Network Monitor, validate you can see the ping request being sent to the domain controller. 8. While on the Gateway, in Network Monitor, validate you can see the ICMP response being sent from the domain controller to the initiating host. | | | | | |
| Usage Scenario | Port mirroring is correctly configured and operational on the domain controllers. If port mirroring does not work, review the configuration of the network or virtual host. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 1.1 | Select only the **Capture** network adapter or the network adapter that is connected to the switch port that is configured as the port mirroring destination. | | It is important to make sure the administrator sees traffic to and from the domain controllers that the ATA Gateway will monitor. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 2: Validate Stable Network Communications

Table : Test Case 2

| Test Case 2: Validate Stable Network Communications | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | This is to make sure that the communications between the ATA Center and the ATA Gateway are stable with no timeouts or minimal latency. | | | | | |
| Completion Steps | 1. Install [Microsoft Network Monitor 3.4](https://www.microsoft.com/download/details.aspx?id=4865) or another network sniffing tool on the ATA Gateway. 2. Launch the Command Prompt window. 3. Ping (if ICMP is allowed) the first domain controller and ATA Center from the ATA Gateway continuously for about five minutes using **ping <hostname or IP> -t.** | | | | | |
| Usage Scenario | Testing network communications are stable between the first domain controller, the ATA Center, and the ATA Gateway. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 2.1 | Ping | | No network timeouts with a 0% packet loss. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 3: Installing the ATA Center

Table : Test Case 3

| Test Case 3: Installing the ATA Center | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | This will make sure that the ATA Center has been successfully installed and that the ATA Console can be successfully accessed in preparation for the ATA Gateway setup. | | | | | |
| Completion Steps | 1. Log on to the ATA Center server with a user who is a member of the local administrators group. 2. From an elevated Command Prompt window, 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 ATA Center configuration page, enter the configuration based on the solutions design document. 6. Click **Install** to install ATA and its components and create the connection between the ATA Center and the ATA Console. 7. After the installation completes, click **Launch** to connect to the ATA Console. | | | | | |
| Usage Scenario | Installation of the ATA Center and verifying the installation was successful. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 3.1 | Verify that the ATA Center service is running by locating **Services.msc** on the Windows Start menu and selecting Run. | | That the ATA Center service is in a running state. | |  |
| 3.2 | 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. | |  |
| 3.3 | 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. | | There should be no errors in this log file. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 4: Configure the ATA Gateway Domain Connectivity Settings

Table : Test Case 4

| Test Case 4: Configure the ATA Gateway Domain Connectivity Settings | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | The settings in the domain connectivity settings section apply to ATA Gateways managed by the ATA Center. | | | | | |
| Completion Steps | 1. Open the ATA Center 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.** | | | | | |
| Usage Scenario | The ability to configure the domain connectivity settings in preparation for the ATA Gateway installation package. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 4.1 | On the **Gateways** page, click on **Domain connectivity settings**, enter the configuration items specified in the solutions design and click **Save**. | | The configuration settings should be accepted after clicking **Save**. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 5: Download the ATA Gateway Setup Package

Table : Test Case 5

| Test Case 5: Download the ATA Gateway Setup Package | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | After configuring the domain connectivity settings, the administrator can download the ATA Gateway setup package. | | | | | |
| Completion Steps | 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 **Settings** option and select **Configuration**. 3. In the **ATA Gateways** tab, click **Download ATA Gateway Setup**. 4. Save the package locally. | | | | | |
| Usage Scenario | Downloading the ZIP package successfully for setup of the ATA Gateway servers. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 5.1 | Download of the ZIP package. | | The ZIP file should be successfully downloaded and include the following:   * ATA Gateway installer * Configuration setting file with the required information to connect to the ATA Center | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 6: Install the ATA Gateway

Table : Test Case 6

| Test Case 6: Install the ATA Gateway | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | This test case confirms the successful installation of the ATA Gateway or ATA Lightweight Gateway. | | | | | |
| Completion Steps | 1. Extract the files from the ZIP file. 2. From an elevated Command Prompt window, 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 deployment type**, select the configuration based on the Solutions Design document. | | | | | |
| Usage Scenario | Installation of the ATA Gateway or Lightweight Gateway and verifying access to the Gateway Console. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 6.1 | After the installation completes, click **Launch** to open your browser and log on to the ATA Console. | | Log on with the same user credentials that you used to install the ATA Gateway. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 7: Configure the ATA Gateway Settings and Verify it is Operational

Table : Test Case 7

| Test Case 7: Configure the ATA Gateway Settings and Verify it is Operational | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | Once the ATA Gateway is installed, the configuration for the ATA Gateway must be set and the installation for the ATA Gateway needs to be verified. | | | | | |
| Completion Steps | 1. On the ATA Gateway machine, in the ATA Console, click on the **Configuration** and select the **ATA Gateways** page. 2. Enter the configuration as per the Solutions Design document. 3. Click **Save**. 4. Log on to the ATA Console and open **Performance Monitor**. 5. 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. | | | | | |
| Usage Scenario |  | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 7.1 | At least one domain controller in the list must be a global catalog server. This will activate ATA to resolve computer and user objects in other domains in the forest. | | The configuration changes will be applied to the ATA Gateway on the next scheduled sync between the ATA Gateway and the ATA Center. | |  |
| 7.2 | Make sure that the first domain controller is **not** an RODC. | | RODCs should be added only after the initial sync completes. | |  |
| 7.3 | Check that the ATA Gateway service is running by locating **Services.msc** on the Windows Start menu and selecting **Run**. | | That the ATA Gateway service is in a running state.  After you have saved the ATA Gateway settings, it might take a few minutes for the service to start the first time because it builds the cache of the network capture parsers used by the ATA Gateway. | |  |
| 7.4 | 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.” | |  |
| 7.5 | Check the following Microsoft ATA Gateway performance counter. | | **NetworkListener PEF Parser Messages/Sec**: This counter tracks how many messages are being captured by the ATA per second. The value should be from the  mid-hundreds to thousands depending on the number of monitored domain controllers and how busy each domain controller is. Single- or double-digit values can indicate an issue with the port-mirroring configuration. | |  |
| 7.6 | Check the following Microsoft ATA Gateway performance counter. | | **EntityResolver Activity**: This value should be in the range of a few hundred every few seconds. | |  |
| 7.7 | Verify that the domain, forest object, and entity cataloguing is taking place. | | You should see a list of **Entities Recently Learned** in the notification bar on the right side of the console. | |  |
| 7.8 | Search for an object in the search bar. | | Such as a user or a group on your domain. This should be successfully resolved. | |  |
| 7.9 | Performance monitor | | Make sure you see activity on the graph. Follow step 5 of this section. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 8: Configure Short-Term Lease Subnets and Honeytoken User

Table : Test Case 8

| Test Case 8: Configure Short-Term Lease Subnets and Honeytoken User | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | 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.  Honeytoken users accounts are Active Directory user accounts that are intended to lure the attacker into thinking the account is of value so they focus on the honeytoken when attempting credential theft. If an attacker attempts to use one, ATA will detect that as a suspicious activity. | | | | | |
| Completion Steps | 1. From the ATA Console, on the ATA Gateway machine, click on the settings icon and select **Configuration**. 2. Under **Detection**, add your defined 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. 4. To find the SID for a user, run the following Windows PowerShell cmdlet -> Get-ADUser UserName –Properties. 5. 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. | | | | | |
| Usage Scenario | Configuring and saving detection settings for short-term leased subnets and honeytoken user. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 8.1 | Save the short-term leased subnets. | | The configuration should be successfully saved after steps 1-3. | |  |
| 8.2 | Enumerate the SID for the honeytoken user. | | To find the SID for a user, run the following Windows PowerShell cmdlet -> Get-ADUser UserName –Properties. | |  |
| 8.3 | Populate the honeytoken user details under the detection configuration. | | The SID is successfully accepted in the console and Saved. Steps 4-5. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 9: ATA Alerting (Notification Settings)

Table : Test Case 9

| Test Case 9: ATA Alerting (Notification Settings) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | ATA can alert the administrator when it detects a suspicious activity, health issue, or available software update by email as well as the verbosity of the alert (frequency and details). Syslog testing is out of scope. | | | | | |
| Completion Steps | 1. On the ATA Center server, click the **Microsoft Advanced Threat Analytics Management** icon on the desktop. 2. Enter the username and password and click **Log in**. 3. Select the settings option on the toolbar and select **Configuration**. 4. Select **Notifications**. 5. Click **Email server settings** to activate email alerts and enter the configuration specified in the solutions design. | | | | | |
| Usage Scenario | Configuring the settings for email and notification type. ATA can alert the administrator when it detects a suspicious activity, health issue, or available software update. Syslog testing is out of scope. Microsoft cannot perform a “hack” scenario to generate alerts. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 9.1 | Alerts configuration | | Alerts configuration successfully saved. | |  |
| 9.2 | Email alert received | | Once ATA detects a suspicious activity, health issue, or available software update, it should be received by the administrator. Make sure that the Simple Mail Transfer Protocol (SMTP) server activates relay of the ATA Center and ATA Gateway IPs. | |  |
| 9.2 | Notification type | | Ensure that an email is received based on the intended notification type. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  |  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 10: Identifying and Working with ATA Alerts and Suspicious Activities

Table : Test Case 10

| Test Case 10: Identifying and Working with ATA Alerts and Suspicious Activities | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | Suspicious activities are listed in chronological order, with the newest suspicious activities on the top of the timeline. | | | | | |
| Completion Steps | 1. After logging on to the ATA Console, the administrator is automatically taken to the open **Suspicious Activities Time Line**. 2. In the **Filter by** pane on the left side of the screen, select one of the following: **All**, **Open**, **Resolved**, or **Dismissed**. 3. To further filter the list, select **High**, **Medium,** or **Low**. 4. For suspicious activities that activate [Type Customer Name Here] to provide input, the input question opens automatically. 5. However, if the administrator answers yes, the suspicious activity might be dismissed and future activities of this type from this computer might not generate a suspicious activity or will generate an activity that is automatically dismissed. 6. If the ATA administrator is not sure, click **Cancel**, and follow up with the entity owner. 7. The administrator can change the status of a suspicious activity by clicking the current status of the suspicious activity and selecting one of the following: **Open**, **Resolved,** or **Dismissed**. | | | | | |
| Usage Scenario | To activate ATA to learn about [Type Customer Name Here]’s network and some suspicious activities (DNS reconnaissance, Pass the Ticket, Abnormal Behavior, and Remote Execution), request input to enhance the detection of suspicious activities going forward. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 10.1 | Update activity | | The administrator can successfully update and provide input into an activity. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 11: Validate that ATA is functioning properly

Table : Test Case 11

| Test Case 11: Validate that ATA is functioning properly | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | Run a simple test to validate that ATA is receiving a suspicious event and mark the suspicious activity as resolved. | | | | | |
| Completion Steps | 1. Logon to another client or server (not the ATA Gateway, Center or Domain Controller). 2. Launch cmd.exe. 3. Type nslookup and press **Enter**. 4. Type ls domain.com where domain.com is the name of the domain in your environment and press **Enter**. This will trigger a suspicious DNS activity, Reconnaissance using DNS in the **Suspicious Activities Time Line**. 5. Logon to the ATA Console. The administrator is automatically taken to the open **Suspicious Activities Time Line**. 6. Validate that there is a **Reconnaissance using DNS** activity in the timeline. 7. Click **Details** for this suspicious event. 8. Click **Note** and type in *Test:* *Validating ATA functionality.* Click **Save**. 9. Select **Open** and mark this suspicious activity as **Resolved**. | | | | | |
| Usage Scenario | To validate [Type Customer Name Here]’s network with a simple, test suspicious activity and go through the process of adding a note and marking it as Resolved. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 11.1 | Logon to a client/server and run nslookup with the options above. | | The administrator can successfully logon to a system and launch nslookup to perform the test. | |  |
|  | 11.2 | Validate result in ATA Console. | | Reconnaissance using DNS suspicious activity is present in the Suspicious Activities timeline. | |  |
|  | 11.3 | Add a Note and mark the event as Resolved. | | The event should now be tagged as resolved. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 12: ATA Heath Center

Table : Test Case 12

| Test Case 12: ATA Heath Center | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | Review of the overall health of the ATA infrastructure. | | | | | |
| Completion Steps | 1. To check up on the system's overall health, click the **Health Center icon** in the menu bar. 2. In the Alert, click **Open** and scroll down to either **Resolved** or **Dismissed**. | | | | | |
| Usage Scenario | The ATA Health Center lets the administrator know that there's a problem by raising an alert. | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 11.1 | Heath Center | | The administrator should successfully view the Health Center and update the alerts logged in the Center, if any. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* + 1. Test Case 13: Database Management

**Instruction:** We recommend at minimum to test the backup procedure. Restore should only be done in a lab or isolated environment for testing and process refinement. Management – Robomongo is used to view the database.

Table : Test Case 13

| Test Case 13: Database Management | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Description | ATA uses an open-source database with the relevant agreements in place as part of the ATA installation. This database is called MongoDB. Out of the box, MongoDB does not provide any GUI for administration (command line tools only). **Note:** Microsoft does not support modification of the ATA database. | | | | | |
| Completion Steps | Backup or restore—refer to the [relevant MongoDB documentation](http://docs.mongodb.org/manual/administration/backup/).  Management—Refer to the [relevant Robomongo documentation](https://robomongo.org/). | | | | | |
| Usage Scenario | Backup, Restore, Management (as needed) | | | | | |
| Test Case Validation Items | **ID** | **Validation Step** | | **Expected Result** | | **Actual Result** |
| 12.1 | Backup | | Backup is successful | |  |
| 12.2 | Restore | | Restore is successful and ATA Center and Gateway services are in a running state. | |  |
| 12.3 | Management | | Database is accessible through Robomongo. | |  |
| Test Results | **Test Date** | | **Tested By** | | **Result** | |
|  | |  | |  | |
|  | |  | |  | |
| Comments |  | | | | | |

* 1. Test Case Results Summary

TR = Test Results = Success/Failure,

Summary Comments = Summarize on the test case results as notes for the production deployment e.g. Challenges, failures, notes.

If port mirroring as example is on a pure virtual environment in a lab, but production will be a combination of virtual and physical port mirroring requirements, make a note here of your result during testing, but also make a note in the risk section later in this document.

Refer to the ATAIS-Implementation and ATAIS-Operations Guides for detailed steps on completing and verifying the elements discussed in this section.

Table 25: Test Results

| Identification Code | Test Item | Test Results | Summary Comments |
| --- | --- | --- | --- |
| TR1 | Validate port mirroring. |  |  |
| TR2 | Validate that there is a stable network communication between the Center and the Gateway servers. |  |  |
| TR3 | Install the ATA Center. |  |  |
| TR4 | Configure ATA Gateway domain connectivity settings. |  |  |
| TR5 | Download the ATA Gateway setup package. |  |  |
| TR6 | Install the ATA Gateway. |  |  |
| TR7 | Configure the ATA Gateway settings. |  |  |
| TR8 | Configure short-term lease subnets and a honeytoken user. |  |  |
| TR9 | Configure ATA Alerting (notification settings). |  |  |
| TR10 | Identify and work with ATA alerts and suspicious activities. |  |  |
| TR11 | Validate that ATA is functioning properly |  |  |
| TR12 | Install the ATA Health Center. |  |  |
| TR13 | Install Database Management tool |  | This is third-party testing with MongoDB and Robomongo defined processes. |

1. Risks and Dependencies

Use this section to identify three items: assumptions, risks, and dependencies. The assumptions are those that have been made while developing the test plan. The risks are those that arise from either the assumptions or they are anticipated during the testing process. For each risk, indicate the probable impact if the assumption turns out to be incorrect, and the measures employed to correct the situation. Dependencies include things such as the Development Plan and Functional Specification that will help create details for the test plan procedures. There is an example in the table below. Please modify or remove.

Justification: Identifying risks early enables the team to begin managing those risks. Some potential risks include:

* Problems with establishing a comprehensive test environment (that is, hardware)
* Inability to obtain the resources necessary to perform all tests adequately
* Inadequate time to perform detailed tests
* Changes not being made in a timely manner when errors are detected
* Poor designs
* Unplanned schedule changes
* RC = Risk Code

The following table shows the risks identified as a result of the testing performed for [Type Customer Name Here]’s ATA Solution.

Table 26: Risk Identification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identification Code | Risk Item | Mitigation Plan | Mitigation Completion Date | Production Impact |
| RC1 | Port mirroring: Only virtual networks in lab. Production will require physical switch setup for port mirroring with virtual networks. | [Type Customer Name Here] will be verifying and testing the port mirroring setup. Results will be shared for test plan document acceptance. | <dd/MM/yyyy> | [Type Customer Name Here] accepted this item as a production-ready risk. |

1. Open Issues

Use this section to identify any key concerns and tasks that need to be followed up on in order to ensure the plan’s completeness. OC=Open Issue Code

The following table shows the open issues that will follow through to production deployment and their effect to the production environment.

Table : Open Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identification Code | Open Issue Item | Mitigation Plan (if any) | Mitigation Completion Date | Production Impact |
| OC1 |  |  |  |  |