ATAIS - Operations Guide



Advanced Threat Analytics Implementation Services

Prepared for

Customer Name

June 27, 2016

Version Draft

Prepared by

**[Update Author in Doc Properties]**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

Revision and Sign-off Sheet

Change Record

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

Reviewers

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

Table of Contents

[1 Operations Guide Summary 1](#_Toc454799283)

[1.1 Objectives 1](#_Toc454799284)

[1.2 Tasks Summary 1](#_Toc454799285)

[1.3 Skill Requirements 2](#_Toc454799286)

[2 Threat Detection Console 4](#_Toc454799287)

[2.1 Logging on to the Console 4](#_Toc454799288)

[2.2 Console Elements 5](#_Toc454799289)

[3 Modifying ATA Center Configuration 7](#_Toc454799290)

[3.1 Modifying the IP Address 7](#_Toc454799291)

[3.1.1 Procedure for Modifying the IP Address 8](#_Toc454799292)

[3.2 Modifying the Certificate 9](#_Toc454799293)

[3.2.1 Procedure for Modifying the Certificate 9](#_Toc454799294)

[3.3 Modifying the Console IP Address 10](#_Toc454799295)

[3.3.1 Procedure for Modifying the IP Address of the Console 11](#_Toc454799296)

[3.4 Modifying the IIS Certificate 12](#_Toc454799297)

[3.4.1 Procedure for Modifying the IIS Certificate 13](#_Toc454799298)

[4 Modifying ATA Gateway Configuration 14](#_Toc454799299)

[4.1 Modifying Domain Connectivity Password 14](#_Toc454799300)

[4.1.1 Procedure for Modifying the Domain Connectivity Password 14](#_Toc454799301)

[5 ATA Alerting 16](#_Toc454799302)

[5.1 Configuring Language and Verbosity Alerting (brief or detailed) 16](#_Toc454799303)

[5.2 Configuring Email Alerting 17](#_Toc454799304)

[5.3 Configuring Syslog Alerts (informational) 19](#_Toc454799305)

[6 ATA Health Center 21](#_Toc454799306)

[6.1 Managing ATA Health and Alerts 21](#_Toc454799307)

[7 Suspicious Activities 22](#_Toc454799308)

[7.1 Review Suspicious Activities on the Attack Timeline 22](#_Toc454799309)

[7.2 Filtering the Activities List 23](#_Toc454799310)

[7.2.1 Suspicious Activity Severity and Status 23](#_Toc454799311)

[7.3 Updating a Suspicious Activity 24](#_Toc454799312)

[8 ATA Detection Settings 26](#_Toc454799313)

[9 ATA Database 27](#_Toc454799314)

[9.1 Database Backup 27](#_Toc454799315)

[9.2 Database Restore 27](#_Toc454799316)

[9.3 Database Move 27](#_Toc454799317)

[9.4 Database Management 28](#_Toc454799318)

[10 Port Mirroring Validation 29](#_Toc454799319)

[11 ATA Feedback Settings to Microsoft 32](#_Toc454799320)

## Tables

[Table 1: Task Summary 1](#_Toc454799321)

[Table 2: Skill Requirements and Recommendations 2](#_Toc454799322)

[Table 3: Console Elements 5](#_Toc454799323)

[Table 4: IP Address Modification Stages—Center 7](#_Toc454799324)

[Table 5: Certificate Update—ATA Center 9](#_Toc454799325)

[Table 6: Configuring Email Alerting 18](#_Toc454799326)

[Table 7: Suspicious Activity Severity 23](#_Toc454799327)

[Table 8: Suspicious Activity Status 24](#_Toc454799328)

[Table 9: Detection Configuration Options 26](#_Toc454799329)

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

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



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

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

**IMPORTANT – Finalize This Document**

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

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

Template Guidance

Description: The Operations Plan describes how day-to-day operations will occur when the solution is in place. It provides guidance for the organization to maintain the solution successfully over an extended period of time. It contains details on both ongoing and contingency operations and how to handle proactively whatever problems arise. Key components of this plan include backup recovery steps, managing configuration changes and the skills necessary to support the operations.

Justification: By planning for operations early in the project, the organization can take the time necessary to put operational success factors into place. These factors may include changes or additions to people resources, processes and infrastructure.

Team Role Primary: Release Management is responsible for planning and implementing the operations necessary to support the solution. Release Management derives the Operations Plan from requirements documents and functional specifications.

Team Role Secondary: Program Management approves this plan and verifies that it satisfies the project’s requirements. Development reviews the plan to understand how their work will be deployed and modifies their development plan if necessary. Test reviews the plan to verify their test environments are set up to reflect the operational environment in which the solution will be placed.

Monitoring Guidance

Service monitoring allows the operations staff to observe the health of an IT service in real time. Accurate monitoring of a system is a complicated puzzle within a distributed process environment, complicated even more by the integration with systems operated by trading partners. With this in mind, the following list is an example of system components that are typically monitored to verify the IT service remains available:

* Process heartbeat
* Job status
* Queue status
* Server resource loads
* Response times
* Transaction status and availability

However, knowing the current health of a service or determining that a service outage may occur is of little benefit unless the operations staff has the ability to do something about it, or at the very least notify the appropriate group that a specific type of reactive or proactive action needs to occur. This is what is meant by the term "control." When combined and implemented properly, this service management function provides the critical capability to ensure that service levels are always in a state of compliance.

1. Operations Guide Summary

This document lists the operations activities for Microsoft Advanced Threat Analytics (ATA) and discusses when these activities should be performed by Customer Name. It also considers the response plan to be part of operations for this engagement.

This document assumes that ATA has already been installed and configured and is properly running in the Customer Name’s environment. This document does not cover installing, configuring, or troubleshooting ATA. It covers what an ATA administrator should check on a daily, weekly, monthly, and quarterly basis to assist in keeping ATA running as expected.

* 1. Objectives

The objectives of this document are to guide Customer Name to effectively operate, administer, and manage the ATA solution that is deployed by this engagement.

The following topics are covered as part of the ATA operations:

* Working with the ATA Console
* Modifying ATA configuration
* Working with ATA alerts
* ATA Health Center
* Working with suspicious activities
* Working with ATA detection settings
* ATA database management
* Manage telemetry settings
  1. Tasks Summary

**Instruction:** Update as needed for your customer.

The following table lists all of the administrative tasks that this guide covers and how frequently they should be performed.

Table 1: Task Summary

| Task Name | Frequency |
| --- | --- |
| Dashboard monitoring | Daily |
| Working with suspicious activities | Daily |
| Review alerts in the dashboard | Daily |
| Monitor memory usage (center and gateway) | Daily |
| Review performance logs and alerts | Weekly |
| Security updates to servers | Monthly |
| Policies and configuration analysis | Quarterly |
| Alert review modifications | As needed |
| Review and update response plan | As needed |
| Change ATA configuration | As needed |
| Back up, move, or restore the ATA databases | As needed |
| Manage membership of security groups | As needed |
| Port mirroring validation | As needed |

* 1. Skill Requirements

**Instruction:** Use this section to identify the job roles and associated skill requirements necessary to operate the solution. This information could be placed in a matrix that identifies: 1) types of operational functions; 2) the job roles that work within each function; and 3) the skill requirements for each job role.

The following skillsets are preferred for operating the ATA solution that has been deployed in the Customer Name’s environment as part of this engagement. This recommendation could be a combination of teams or individuals.

Table 2: Skill Requirements and Recommendations

| Role | Description |
| --- | --- |
| Threat detection team | This team is responsible for performing threat analysis and review. |
| Threat response team | This team is responsible for responding to an indicator of threat that is discovered by the threat detection team. |
| Network management teams | This team configures port mirroring on both the physical network and the virtual networks that are located in virtual hosts. |
| Individuals that have knowledge of threat detection and response | These individuals understand the threats to the enterprise and how to identify them, and have the effective knowledge of response processes required to respond to the identified threats. |
| Individuals with knowledge of port mirroring | Having such individuals on the team would be advantageous. Port mirroring would normally be managed by dedicated network management teams. |
| Individuals with X.509 certificate experience | A good understanding of public key infrastructure and third-party certificates is a requirement. This is required with the request, import, export, and transfer of certificates between the Center and the Gateway. |

1. Threat Detection Console

Any user who is a member of the local Administrators group on the ATA Center server has permission to log on to the ATA Console and manage ATA settings. To allow a user to log on to the ATA Console without making them a local administrator, add them to the local group: **Microsoft Advanced Threat Analytics Administrators.**

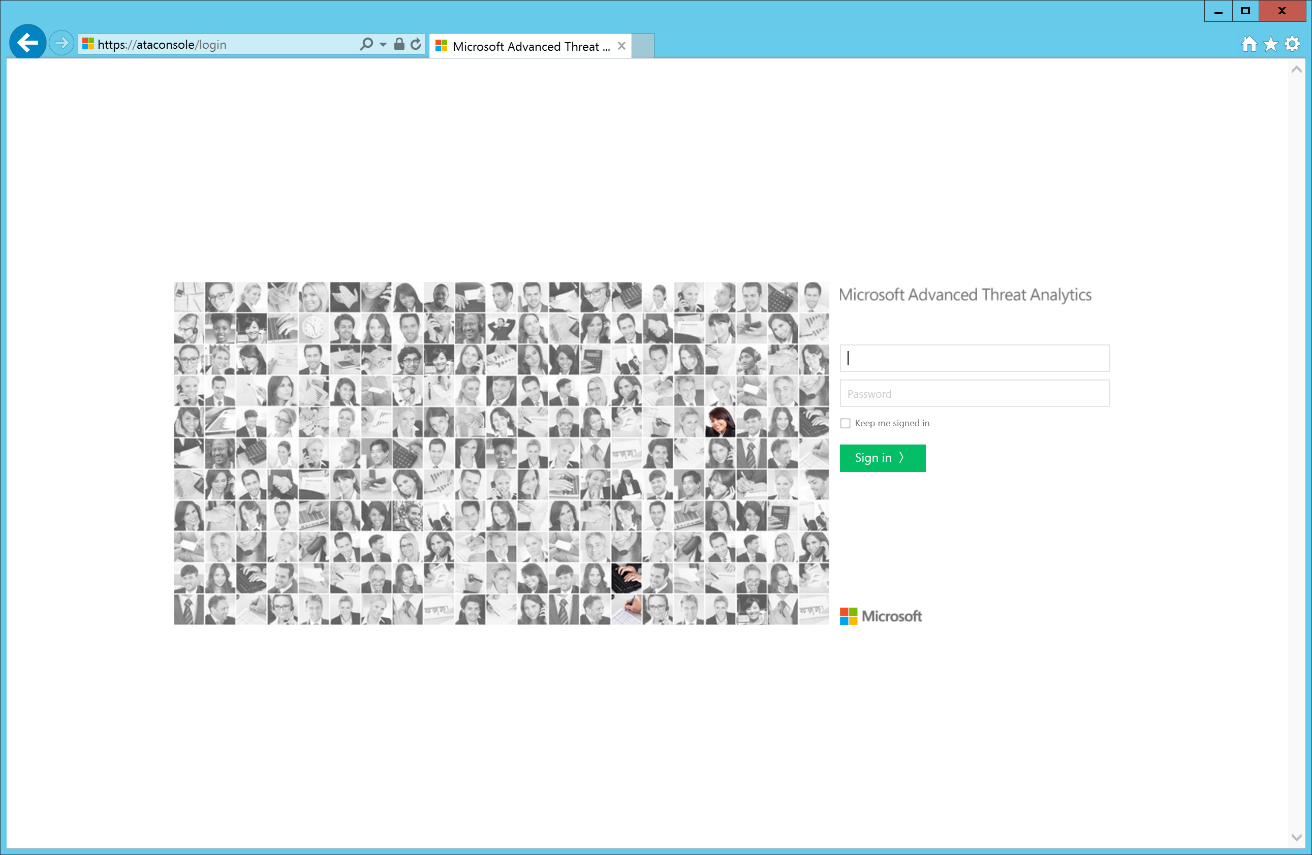
* 1. Logging on to the Console

1. In the ATA Center server, click the **Microsoft ATA Console** icon on the desktop, or open a browser and browse to the ATA Console.

Alternatively, the administrator can open a browser from either the ATA Center or the ATA Gateway and browse to the IP address that the administrator has configured in the ATA Center installation for the ATA Console.

1. Enter the username and password, and click **Log in**.

The administrator has to log on with a user who is a member of the local administrator group or of the Microsoft Advanced Threat Analytics Administrators group.



* 1. Console Elements

After you have been authenticated to the ATA Console, the following elements will be visible.

Table 3: Console Elements

| Element | Details |
| --- | --- |
| Attack timeline | This is the default page that you are taken to when the administrator logs in to the ATA Console. By default, all open suspicious activities are shown on the attack timeline. The administrator can filter the attack timeline to show All, Open, Dismissed, or Resolved suspicious activities. Suspicious activities are listed chronologically, with the newest entries shown first on the list. |
| Suspicious activity | When ATA detects a suspicious activity, an entry is created in the attack timeline. |
| Notification bar | When a new suspicious activity is detected, the notification bar will open automatically on the right side. If there are new suspicious activities since the last time the administrator logged on, the notification bar will open after the administrator has successfully logged on. To access it, the administrator can click the arrow on the right at any time. |
| Filtering | The administrator can filter which suspicious activities are displayed in the attack timeline or displayed in the entity profile suspicious activities tab based on Status and Severity. |
| Search bar | On the top of the screen, the administrator will find a search bar. The administrator can search for a specific user, computer, or groups in ATA. |
| Health Center[[1]](#footnote-2) | The Health Center provides the administrator with alerts when something is not working properly in the ATA network.  Any time the system encounters a problem, such as a connectivity error or a disconnected ATA Gateway, the Health Center icon will let the administrator know by displaying a red dot. |
| Configuration | To modify and view the ATA Configuration, click the settings icon (three dots) on the menu bar, and then click **Configuration**. |
| User and computer profiles | ATA builds a profile for each user and computer in the domain. In the user profile ATA will display general information about the user and will provide additional information on the following pages: Summary, Activities, and Suspicious activities. |
| Mini profiles | Anywhere in the console where a single entity is presented, such as a user or computer, if the administrator hovers the mouse cursor over the entity, a mini profile will open automatically. The profile lists:   * Name * Picture * Email * Telephone * Number of suspicious activities by severity |

1. Modifying ATA Center Configuration

After the initial deployment, modifications to the ATA Center should be made carefully. Use the following procedures when updating the IP address and port or the certificate.

* 1. Modifying the IP Address

The ATA Gateways locally store the IP address of the ATA Center to which they need to connect. On a regular basis, they connect to the ATA Center and pull down configuration changes. Making a change to how the ATA Gateways connect to the ATA Center is done in two stages.

Table 4: IP Address Modification Stages—Center

|  |  |
| --- | --- |
| Stage | Details |
| One | Update the IP address and port that the administrator wants the ATA Center service to use.  At this point the ATA Center is still listening on the original IP address. The next time the ATA Gateway syncs its configuration, it will have two IP addresses for the ATA Center.  As long as the ATA Gateway can connect by using the first IP address, it will not try the new IP address and port. |
| Two | After all the ATA Gateways have synced with the updated configuration, activate the new IP address and port that the ATA Center listens on. When the administrator activates the new IP address, the ATA Center service will bind to the new IP address.  ATA Gateways will not be able to connect to the original address and now will attempt to connect with the second IP address that they have for the ATA Center.  After connecting to the ATA Center with the new IP address, the ATA Gateway will pull down the latest configuration and will have a single IP address for the ATA Center (unless the administrator started the process again). |

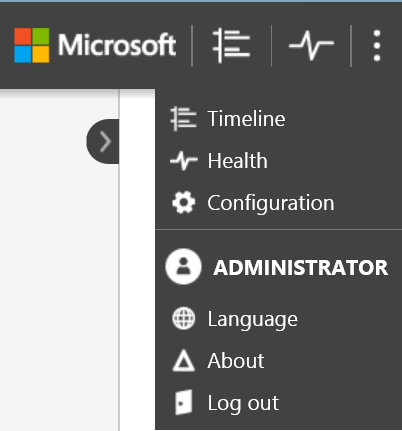
**Note:** if an ATA Gateway was offline during the first stage and never got the updated configuration, the administrator will need to update the configuration JavaScript Object Notation (JSON) file manually on the ATA Gateway.

If the new IP address is installed on the ATA Center server, the administrator can select it from the list of IP addresses when making the change. However, if for some reason the administrator cannot install the IP address on the ATA Center server, the administrator can choose to add a custom IP address manually. The administrator will not be able to activate the updated IP address until the IP address is installed on the server.

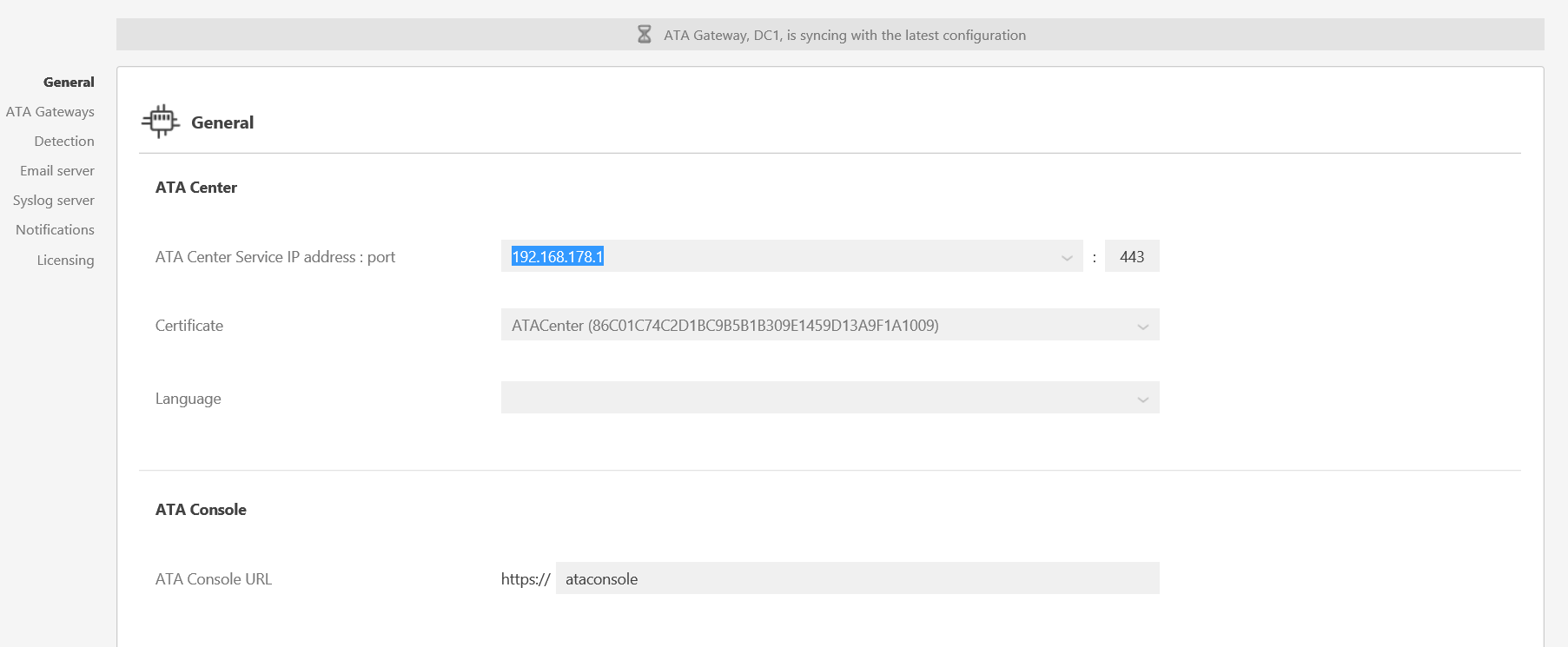
If the administrator needs to deploy a new ATA Gateway after activating the new IP address, the administrator needs to download the ATA Gateway Setup package again.

* + 1. Procedure for Modifying the IP Address

1. Open the **ATA Console**.
2. On the toolbar, click the settings icon , and then click **Configuration**.



1. Click **General**.
2. Under **ATA Center Service IP address: port**, select one of the existing IP addresses, or click **Add custom IP address**, and then enter an IP address.
3. Click **Save**.
4. The administrator will see a notification of how many ATA Gateways have synced to the latest configuration.



1. After all the ATA Gateways have synced, click **Activate** to activate the new IP address. If the administrator entered a custom IP address, the administrator will not be able to click **Activate** until the administrator has installed the IP address on the ATA Center.
2. After the new IP address is activated, verify that all the ATA Gateways are able to sync their configurations. The notification bar will indicate how many ATA Gateways synced their configuration successfully.
   1. Modifying the Certificate

If the certificates expire and need to be renewed or replaced after installing the new certificate in the local computer store on the ATA Center server, replace the certificate by following this two-stage process.

Table 5: Certificate Update—ATA Center

|  |  |
| --- | --- |
| Stage | Details |
| One | Update the certificate that the administrator wants the ATA Center service to use. At this point the ATA Center service is still bound to the original certificate. When the ATA Gateways sync their configuration, they will have two potential certificates that will be valid for mutual authentication. As long as the ATA Gateway can connect by using the original certificate, it will not try the new one. |
| Two | After all the ATA Gateways have synced with the updated configuration, the administrator can activate the new certificate to which the ATA Center service is bound. When the administrator activates the new certificate, the ATA Center service will bind to the certificate. ATA Gateways will not be able to mutually authenticate the ATA Center service properly and will attempt to authenticate the second certificate. After connecting to the ATA Center service, the ATA Gateway will pull down the latest configuration and will have a single certificate for the ATA Center (unless the administrator started the process again). |

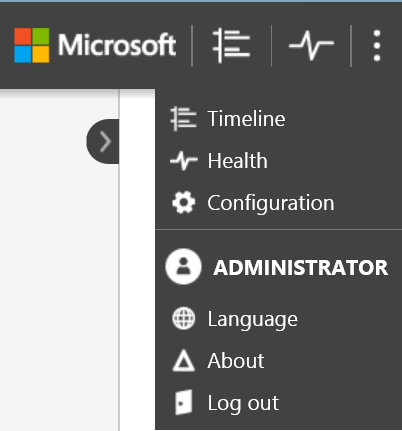
**Note:** if an ATA Gateway was offline during the first stage and never got the updated configuration, the administrator will need to update the configuration JSON file manually on the ATA Gateway.

The certificate that the administrator is using must be trusted by the ATA Gateways.

If the administrator needs to deploy a new ATA Gateway after activating the new certificate, the administrator will need to download the ATA Gateway Setup package again.

* + 1. Procedure for Modifying the Certificate

1. Open the ATA Console.
2. On the toolbar, click the settings icon , and then click **Configuration**.



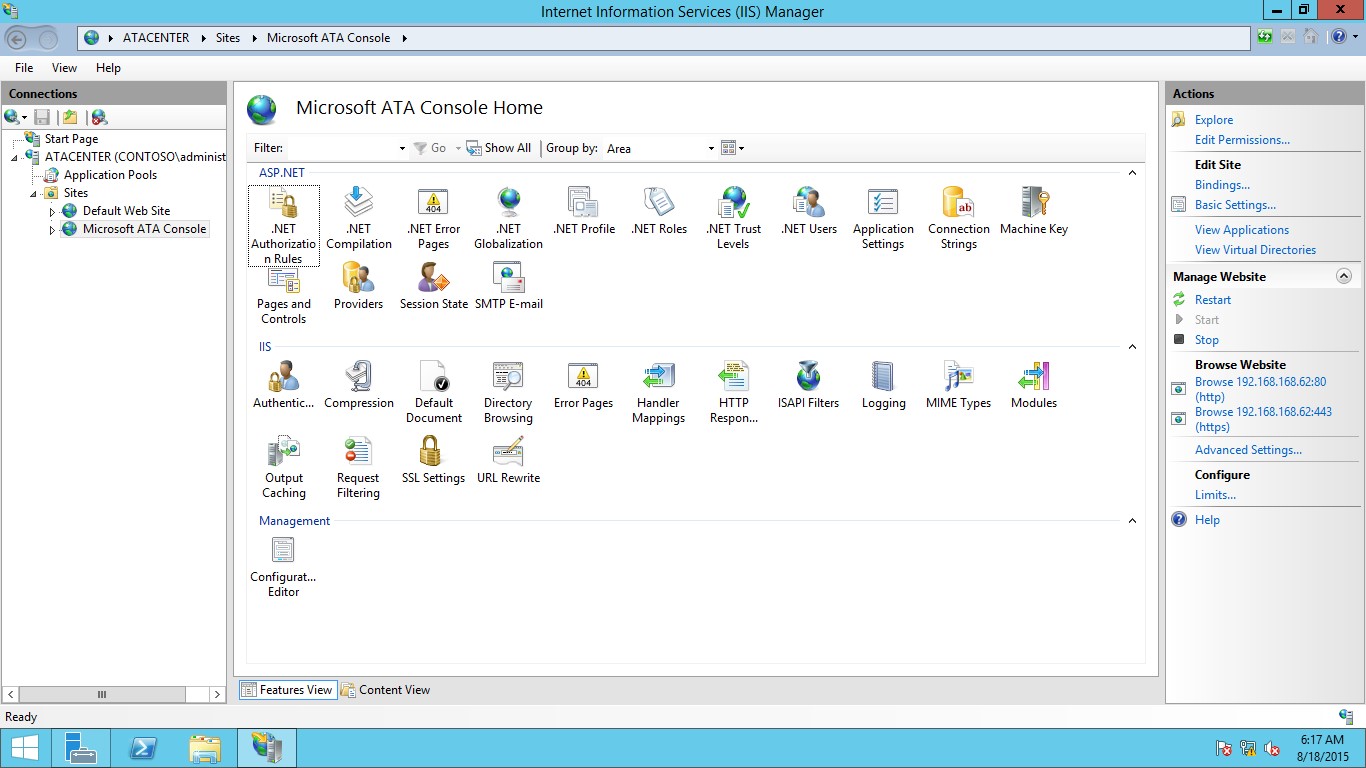
1. Click **General**.
2. Under **Certificate**, select one of the certificates in the list.
3. Click **Save**.
4. The administrator will see a notification of how many ATA Gateways have synced to the latest configuration.
5. After all the ATA Gateways have synced, click **Activate** to activate the new certificate.
6. Verify that all the ATA Gateways are able to sync their configurations after the change was activated.
   1. Modifying the Console IP Address

By default, the ATA Console URL is the IP address that was selected for the ATA Console IP address when the administrator installed the ATA Center.

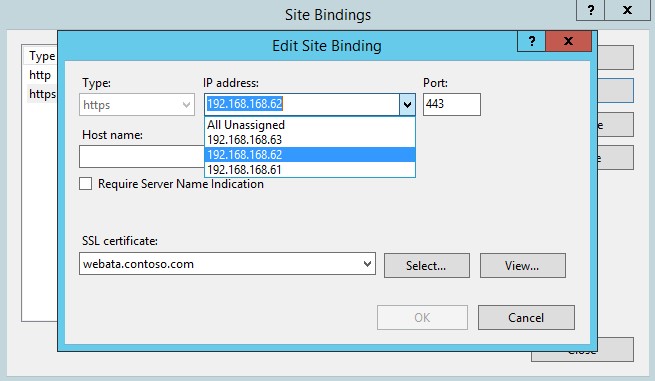
The URL is used in the following scenarios:

* **Installation of ATA Gateways**—When an ATA Gateway is installed, it registers itself with the ATA Center. This registration process is accomplished by connecting to the ATA Console. If the administrator enters a fully qualified domain name (FQDN) for the ATA Console URL, the administrator needs to validate that the ATA Gateway can resolve the FQDN to the IP address that the ATA Console is bound to in Internet Information Services (IIS) Manager. Additionally, the URL is used to create the shortcut to the ATA Console on the ATA Gateways.
* **Alerts**—When ATA sends out a security information and event management (SIEM) or email alert, it includes a link to the suspicious activity. The host portion of the link is the ATA Console URL setting.
* If the administrator installed a certificate from the internal certification authority, the administrator will probably want to match the URL to the subject name in the certificate so that users will not get a warning message when they connect to the ATA Console.
* By using an FQDN for the ATA Console URL, the administrator can modify the IP address that is used by IIS for the ATA Console without breaking alerts that have been sent out in the past or needing to download the ATA Gateway package again. The administrator only needs to update the Domain Name System (DNS) with the new IP address.
  + 1. Procedure for Modifying the IP Address of the Console

1. Install the IP address on the ATA Center server.
2. Open IIS Manager.
3. Expand the name of the server, and expand **Sites**.
4. Select the Microsoft ATA Console site.
5. In the **Actions** pane, in the **Edit Site** section, click **Bindings**.



1. Click **http,** and then click **Edit** to select the new IP address. Do the same for **https,** selecting the same IP address.



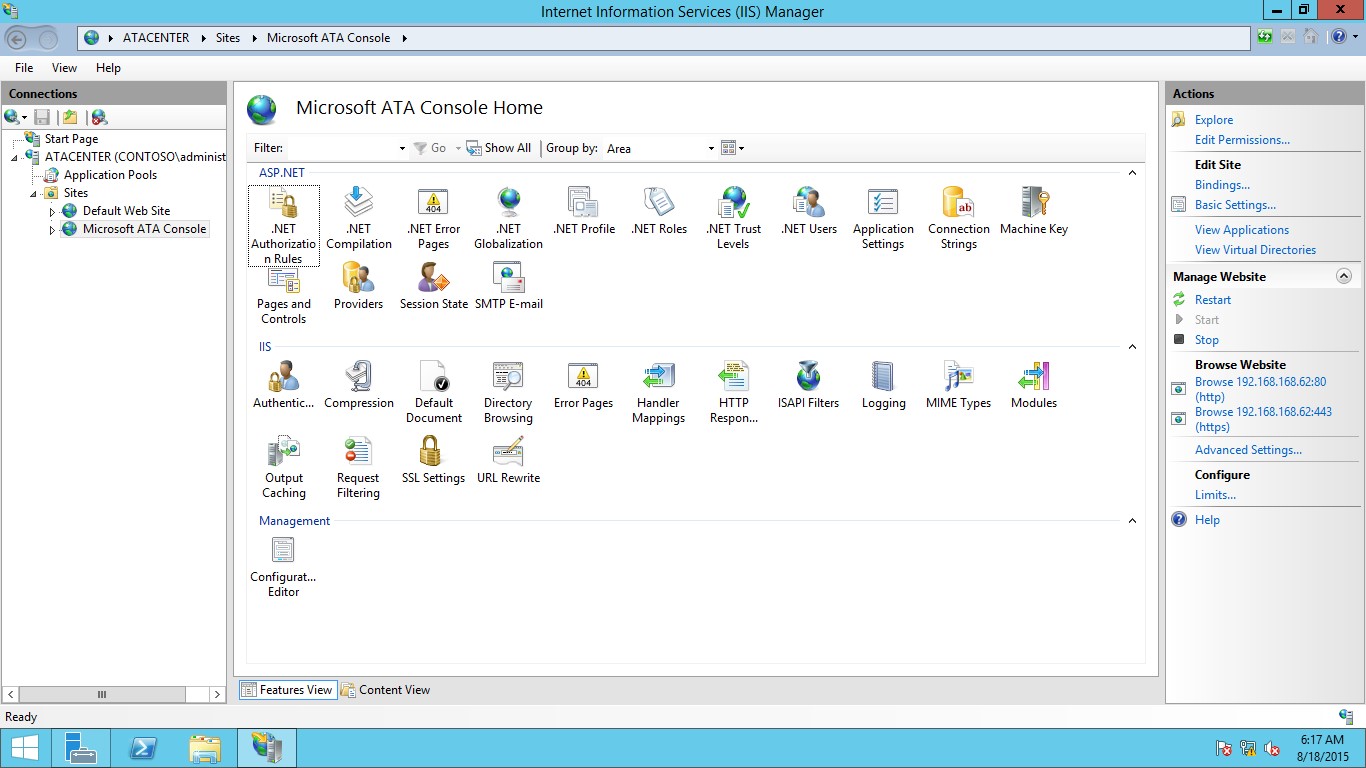
1. In the **Action** pane, in the **Manage Website** section, click **Restart**.
2. Open an Administrator command prompt, and type the following commands to update the HTTP.sys driver:
   1. To add the new IP address: **netsh http add iplisten ipaddress=newipaddress**
   2. To see that the new address is being used: **netsh http show iplisten**
   3. To delete the old IP address: **netsh http delete iplisten ipaddress=oldipaddress**
3. If the ATA Console URL is still using an IP address, update the ATA Console URL to the new IP address, and download the ATA Gateway Setup package before deploying new ATA Gateways.
4. If the ATA Console URL is an FQDN, update the DNS with the new IP address for the FQDN.
   1. Modifying the IIS Certificate

In the console, the administrator can select and change the certificate for the ATA Center service, but the administrator cannot change the certificate that IIS uses. If the administrator needs to modify the certificate that IIS uses for the ATA Center, follow these steps from the ATA Center server.

**Note:** after modifying the IIS certificate, the administrator should download the ATA Gateway Setup package before installing new ATA Gateways.

* + 1. Procedure for Modifying the IIS Certificate

1. Install the new certificate on the ATA Center server.
2. Open IIS Manager.
3. Expand the name of the server, and expand **Sites**.
4. Select the Microsoft ATA Console site.
5. In the **Actions** pane, in the **Edit Site** section, click **Bindings**.

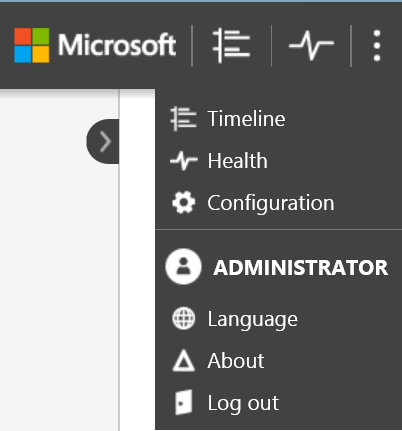


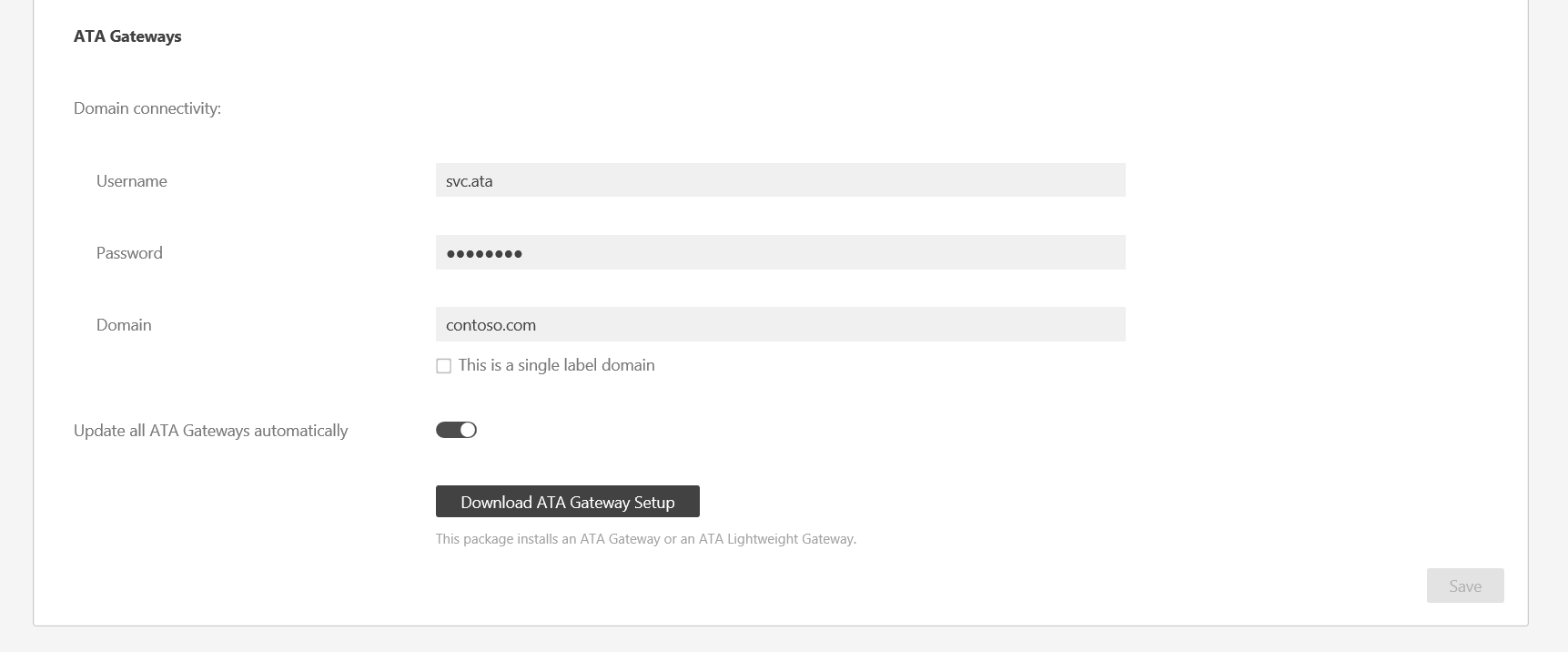
1. Click **https,** and then click **Edit**.
2. Under **SSL certificate**, select the new certificate.
3. Download the ATA Gateway Setup package before installing a new ATA Gateway.
4. Modifying ATA Gateway Configuration
   1. Modifying Domain Connectivity Password

If the administrator modifies the Domain Connectivity Password, make sure that the password the administrator enters is correct. If it is not, the ATA Service will stop running on the ATA Gateways.

If the administrator suspects that this has happened, on the ATA Gateway, look at the **Microsoft.Tri.Gateway-Errors.log** file for the following: The supplied credential is invalid.

* + 1. Procedure for Modifying the Domain Connectivity Password

1. Open the ATA Console on the ATA Gateway.
2. On the toolbar, click the settings icon , and then click **Configuration**.
3. Click **General**.



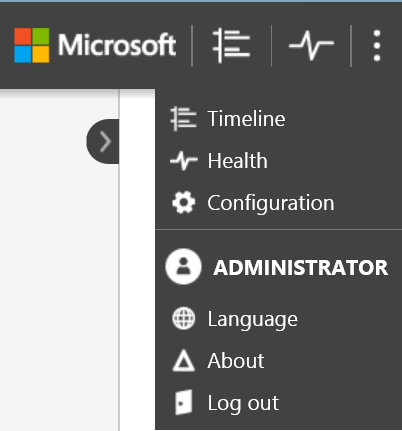
1. Under **ATA Gateways**, change the password.
2. Click **Save**.
3. After changing the password, manually check that the ATA Gateway service is running on the ATA Gateway servers.
4. ATA Alerting

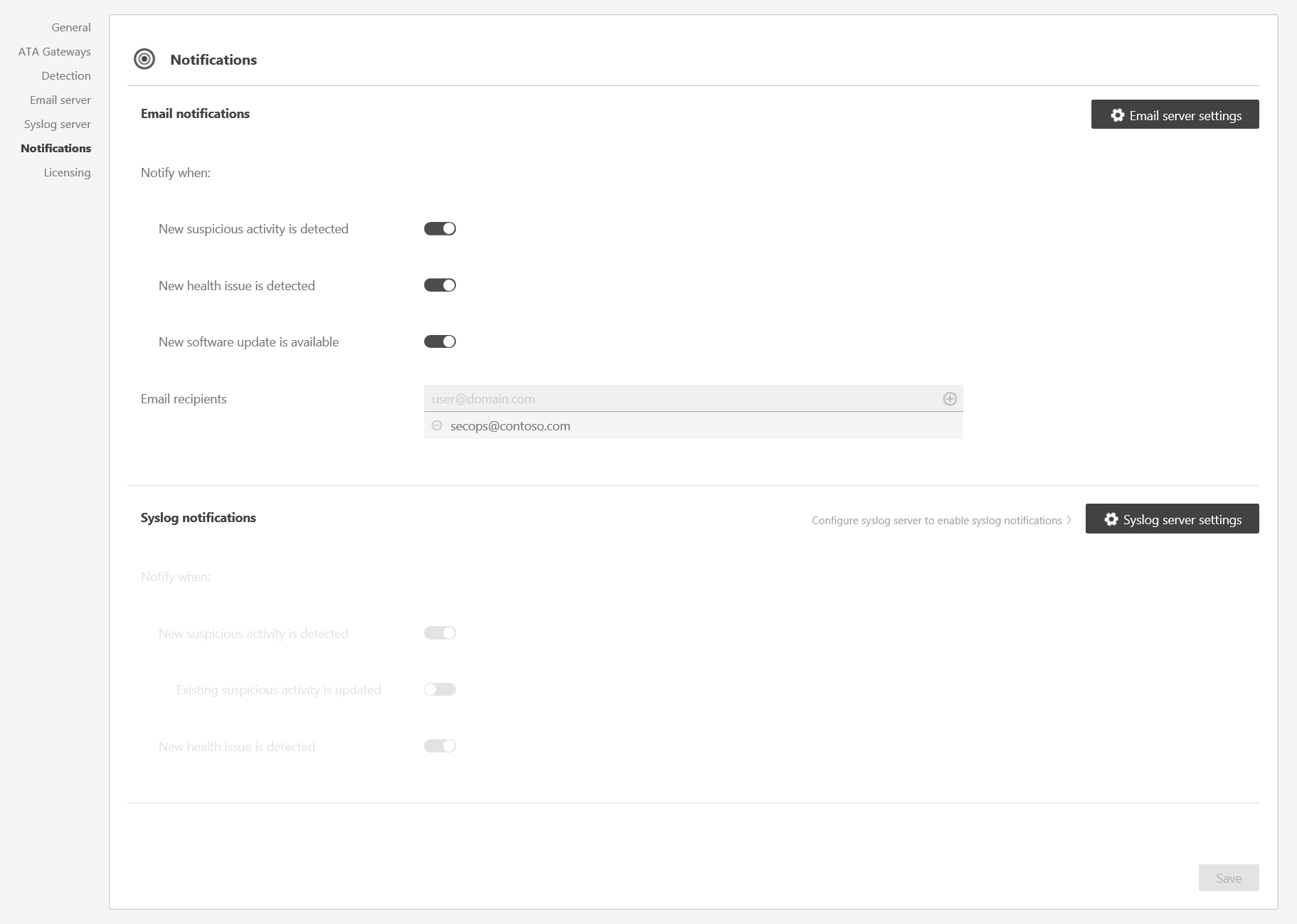
When ATA detects a suspicious activity, it can alert the administrator either via email or by sending the alert to the Syslog server. If the administrator implements either or both of these types of alerts, the administrator can set the following for them.

**Note:** the notifications will include a link that will take the user directly to the suspicious activity that was detected. The host name portion of the link is taken from the setting of the ATA Console URL on the ATA Center page. By default, the ATA Console URL is the IP address that was selected during the installation of the ATA Center. If the administrator is going to configure email or Syslog alerts, we recommend using an FQDN as the ATA Console URL.

System Health Alert alerts are sent only via email.

* 1. Configuring Language and Verbosity Alerting (brief or detailed)

1. Open the ATA Center Console.
2. On the toolbar, click the settings icon , and then click **Configuration**.
3. Click **Notifications**.
4. Under **Notify when**, slide the toggles to the right for the notifications you want to enable.



1. Click **Save**.
   1. Configuring Email Alerting

ATA can alert the administrator when it detects a suspicious activity. If the administrator implements email alerts, the administrator can set the following for them.

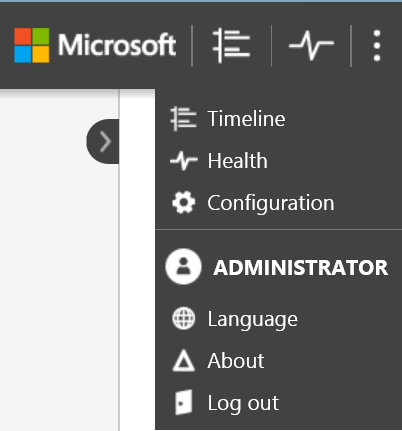
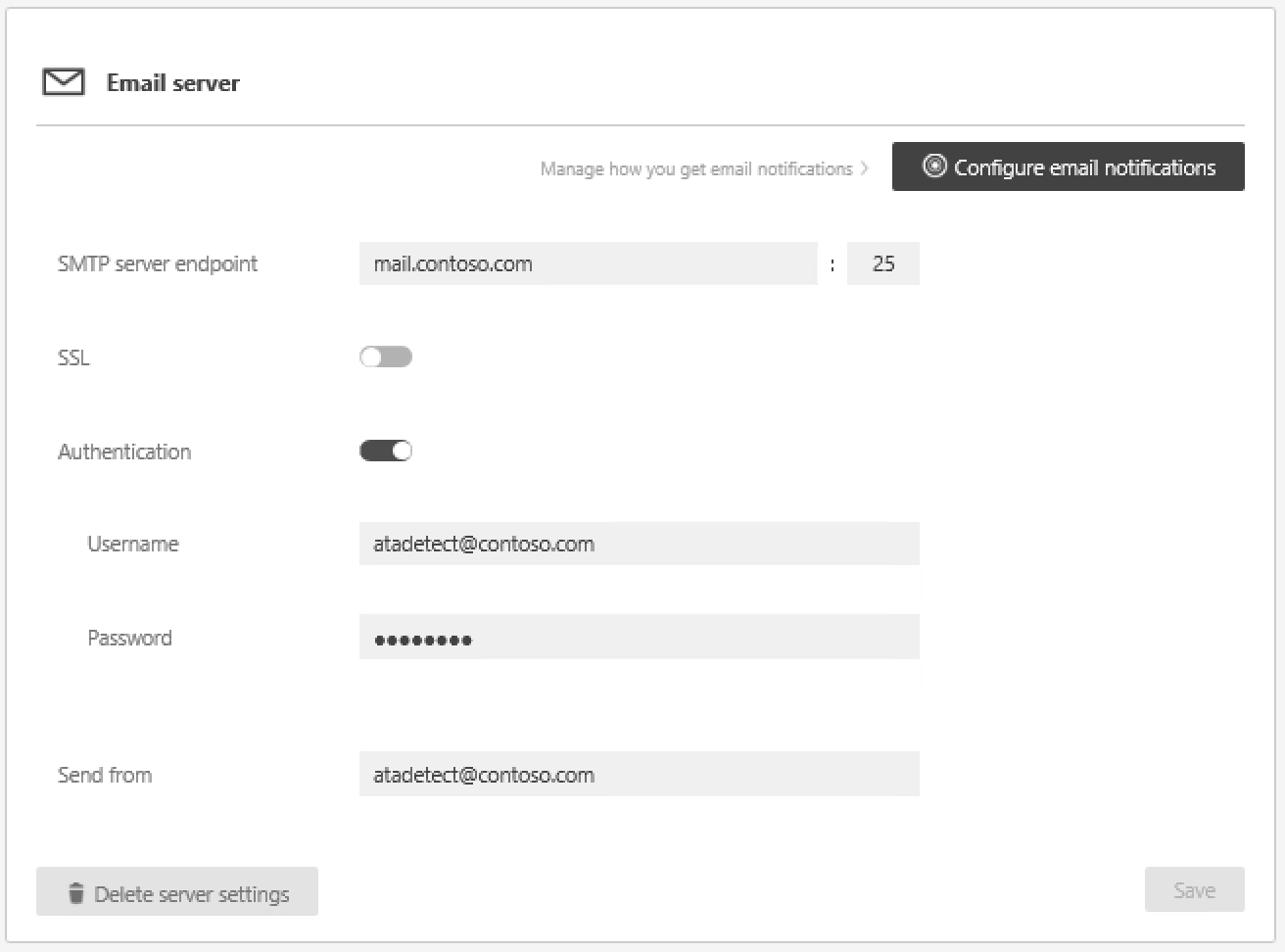
1. Open the ATA Center Console.
2. On the toolbar, click the settings icon , and then click **Configuration**.
3. Click **Email server**.
4. Enter the following information:

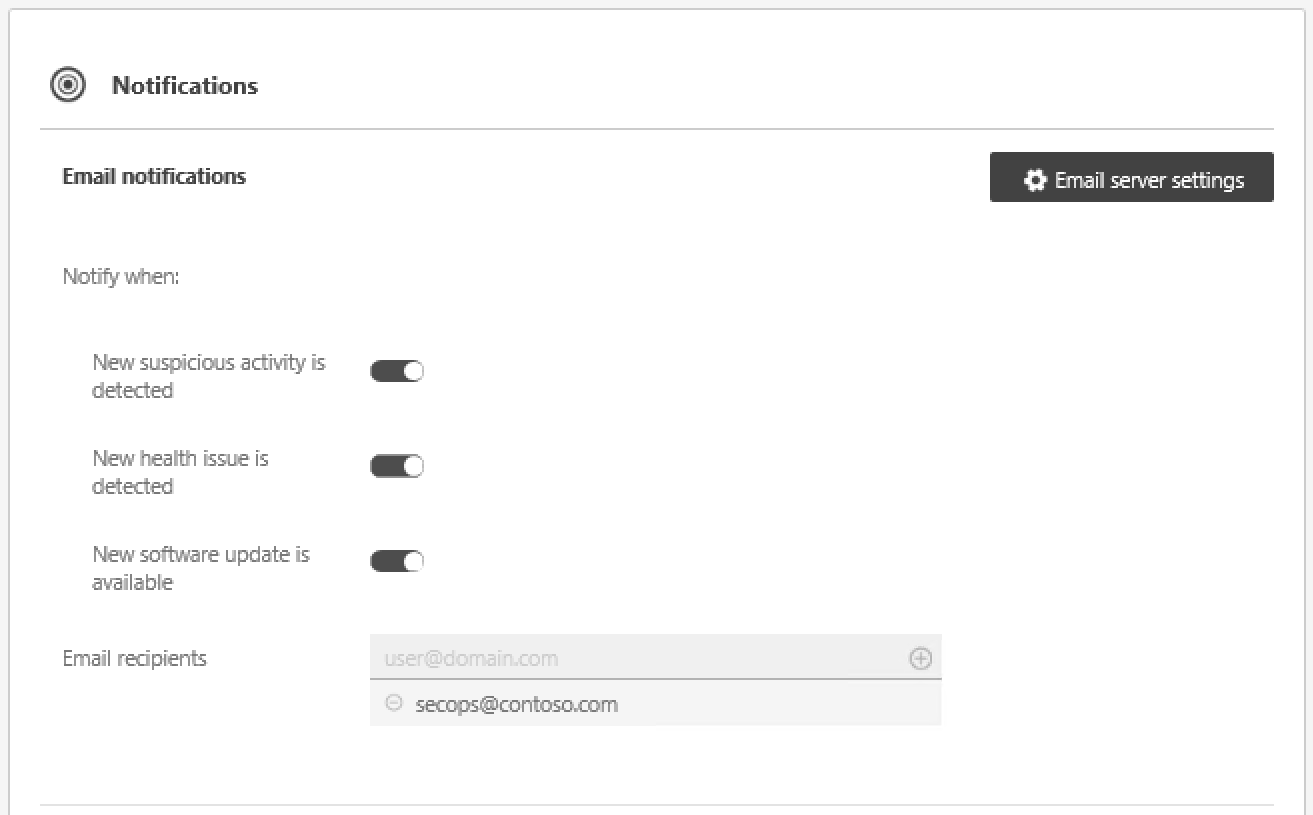
Table 6: Configuring Email Alerting

| Field | Description | Value |
| --- | --- | --- |
| SMTP server endpoint (required) | Enter the FQDN of the SMTP server. | For example: smtp.contoso.com |
| SSL | Toggle Secure Sockets Layer (SSL) if the SMTP server required SSL.   |  | | --- | | **System_CAPS_noteNote** | | If the administrator implements SSL, Customer Name will also need to change the port number. | | Default is disabled |
| Authentication | Implement if the SMTP server requires authentication.   |  | | --- | | **System_CAPS_noteNote** | | If Customer Name implements authentication, the administrator must provide a user name and password for an email account that has permission to connect to the SMTP server. | | Default is disabled |
| Send from (required) | Enter an email address from whom the email will be sent. | For example: ATA@contoso.com |



Once the e-mail settings are completed, click **Configure email notifications**. There are a 3 notifications types that can be toggled on/off:

* New suspicious activity is detected
* New health issue is detected
* New software update is available



After toggling the wanted notification types, and specifying the recipients who will receive the notifications click, Save at the bottom of the page.

* 1. Configuring Syslog Alerts (informational)

Syslog configuration is out of scope for this engagement. This section is informational for Customer Name to be able to configure Syslog forwarding.

ATA can alert Customer Name when it detects a suspicious activity by sending the alert to the Syslog server. ATA can also receive Syslog events from selected vendors. See the list of vendors at <https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/configure-event-collection> (Configure Event Collection).

Also see <https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/setting-ata-alerts> on working with alerts and configuring ATA to push to a Syslog server.

Customer Name should work with the documentation and guidance that is offered by the SIEM or Syslog service vendor in conjunction with the guidance that is offered in this section.

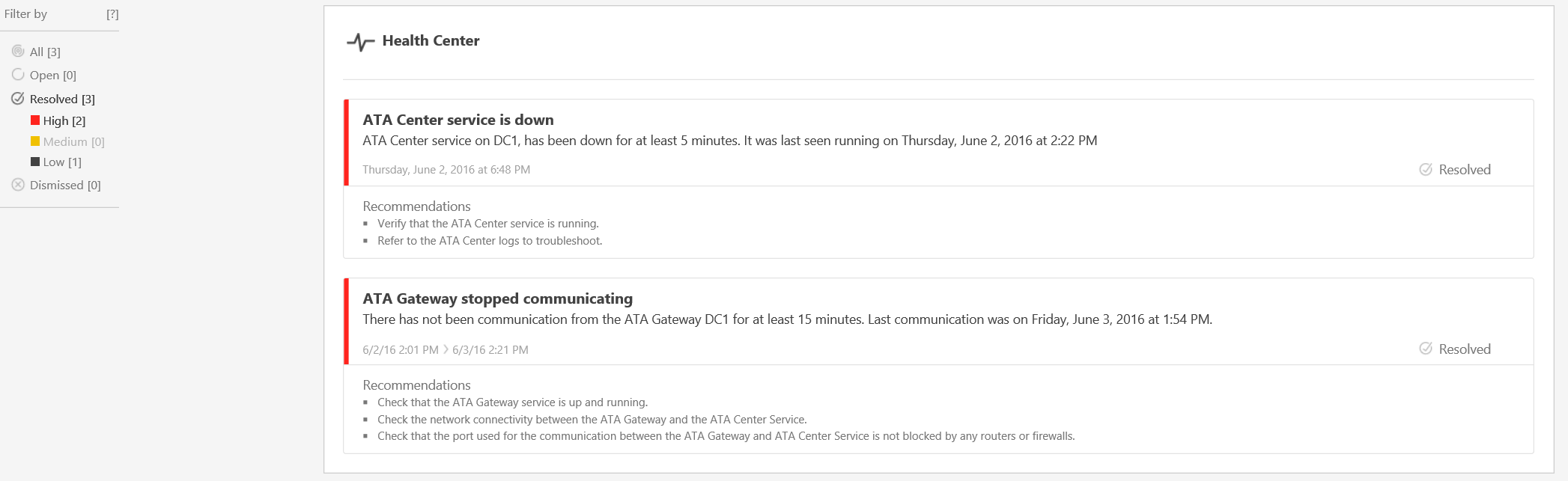
1. ATA Health Center

The ATA Health Center notifies Customer Name about a problem by raising an alert (a red dot) above the Health Center icon in the menu bar.

* 1. Managing ATA Health and Alerts

ATA red dotTo check on the system's overall health, click the **Health Center** icon in the menu bar.

* All open alerts can be managed by setting them to **Resolved** or **Dismissed**. In the alert, click **Open,** and then scroll down to either **Resolved** or **Dismissed**.
* If the administrator resolves an issue and ATA detects that the issue persists, the issue will automatically be moved back to the **Open** issues list. If ATA detects that an open issue is resolved, it will automatically be moved to the **Resolved** issues list.
* **The Dismissed** list includes issues that the administrator does not want ATA to continue to check—for example, if the administrator is alerted to an issue that the administrator knows exists, does not plan to resolve, does not want to be notified about, and does not want to see on the **Open** issues list, the administrator can set it to **Dismissed**.



1. Suspicious Activities

This section explains how to work with suspicious activities. This section does not cover how to respond to suspicious activities but rather how to work with them in the console, add comments, and filter these activities.

* 1. Review Suspicious Activities on the Attack Timeline

After logging on to the ATA Console, the administrator is taken automatically to the open **Suspicious Activities Timeline**. Suspicious activities are listed in chronological order with the newest suspicious activities at the top of the timeline. Each suspicious activity has the following information:

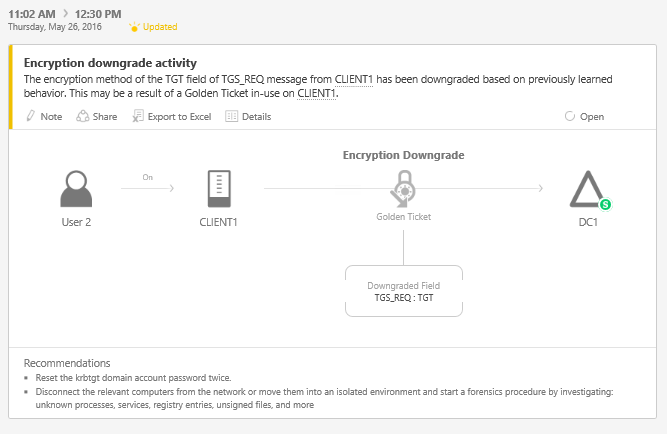
* Entities involved, including users, computers, servers, domain controllers, and resources
* Times and time frame of the suspicious activities
* Severity of the suspicious activity, High, Medium, or Low
* Status: Open, Resolved, or Dismissed

The attack timeline also has the ability to:

* Send the suspicious activity to other people in Customer Name via email. Sending these notifications requires an email client to be installed on the computer from which the administrator is browsing.
* Export the suspicious activity to Excel.
* Add a note to the suspicious activity.
* Provide input on the suspicious activity.

**Note:** When the administrator hovers a mouse cursor over a user or computer, an entity mini profile is displayed that provides additional information about the entity and includes the number of suspicious activities to which the entity is linked.

If the administrator clicks an entity, the administrator sees the entity profile of the user or computer.



**Caution Note:** the threat console provides recommendations on how to respond to the suspicious activity. This high-level guidance requires an effective response plan as part of this engagement (see ATAIS—Response Plan). Each activity requires unique attention and response processes depending on severity and status.

* 1. Filtering the Activities List

To filter the suspicious activities list:

1. In the **Filter by** pane on the left side of the screen, click one of the following: **All**, **Open**, **Resolved**, or **Dismissed**.
2. To filter the list further, click **High**, **Medium,** or **Low**.
   * 1. Suspicious Activity Severity and Status

The following table outlines the severity under which each suspect activity can be classified.

Table 7: Suspicious Activity Severity

| Severity Level | Description |
| --- | --- |
| LOW | Indicates suspicious activities including individual attacks by malicious users or through software that can be used to gain access to organizational data. |
| MEDIUM | Indicates suspicious activities that can put specific identities at risk for more severe attacks that can result in identity theft or privilege escalation. |
| HIGH | Indicates suspicious activities that can lead to identity theft, privilege escalation, or other high-impact attacks. |

The following table shows the current status of the activity that is updated and modified by the ATA administrator.

Table 8: Suspicious Activity Status

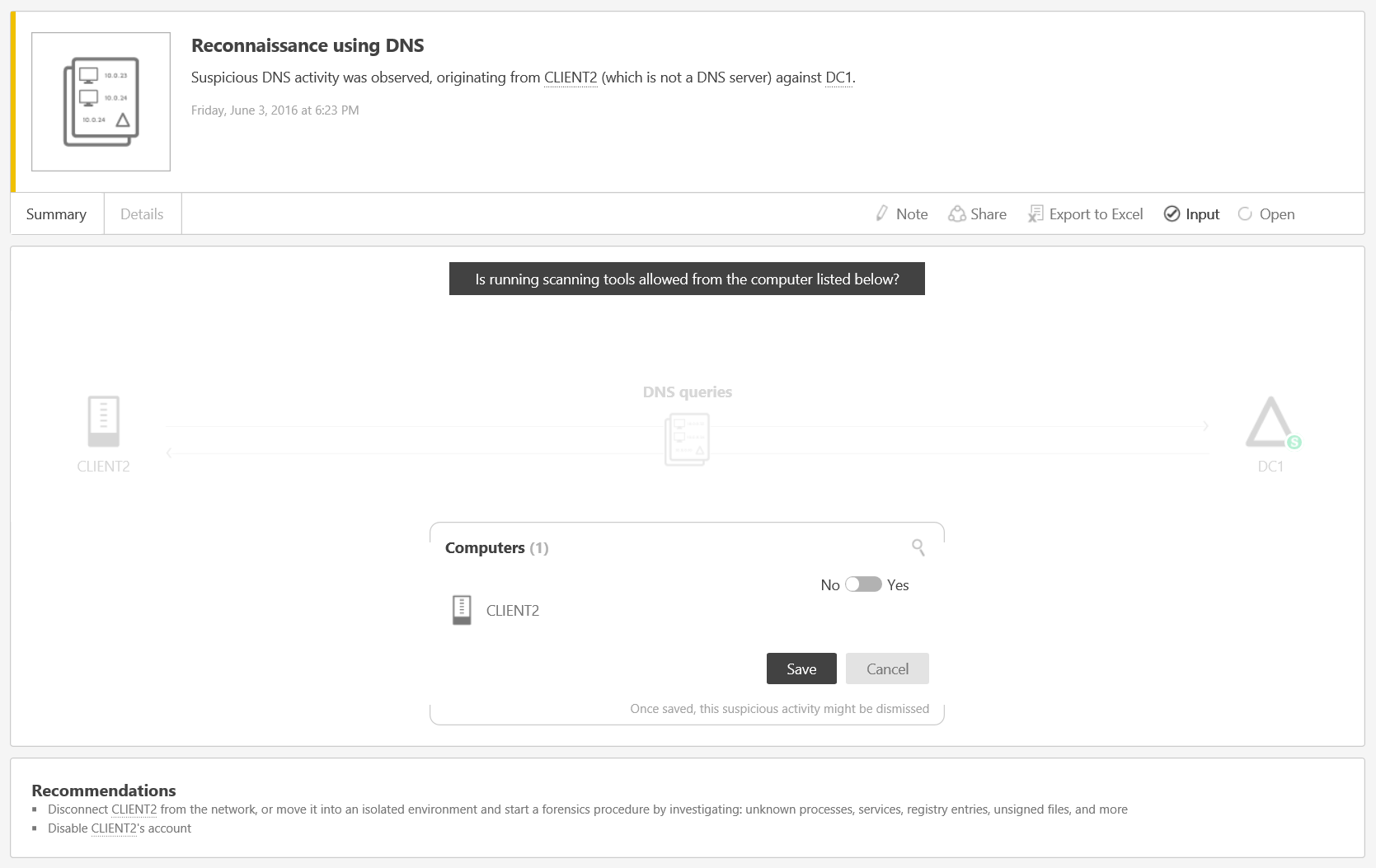
|  |  |
| --- | --- |
| Status | Description |
| Open | All new suspicious activities appear in this list. |
| Resolved | Used to track suspicious activities that Customer Name identified, researched, and fixed or mitigated. |
| Dismissed | Activities that Customer Name dismissed manually. If ATA detects a similar suspicious activity, a new detection will be created. |

**Note:** ATA can reopen a Resolved activity if the same activity is detected again within a short period of time.

* 1. Updating a Suspicious Activity

To empower ATA to learn about Customer Name’s network, some suspicious activities (DNS reconnaissance, pass the ticket, abnormal behavior, and remote execution) request input to enhance the detection of suspicious activities.

1. For suspicious activities that empower Customer Name to provide input, the input question opens automatically. Customer Name will be asked to answer questions about activities on their network and whether they should be considered suspicious. In the following example, the administrator is being asked if running scanning tools is allowed from a specific computer.



1. If the administrator answers **No**, this activity will be considered suspicious, and any time ATA encounters this activity from this computer, Customer Name will be alerted.
2. 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 dismissed automatically.
3. If Customer Name’s ATA administrator is not sure, click **Cancel,** and follow up with the entity owner.
4. Customer Name 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**.
5. ATA Detection Settings

On the Detection configuration page, Customer Name can create a list of IP addresses and subnets that have unusual circumstances and should be handled slightly differently than other entities on the network.

On the **Detection** page the administrator can define the items in the following table.

Table 9: Detection Configuration Options

|  |  |
| --- | --- |
| Item | Description |
| Short-term lease subnets | If Customer Name has any subnets on which the IP addresses are very short-term, such as virtual private network IP address subnets or Wi-Fi subnets, it is important to input these IP addresses and subnets into ATA so that ATA stores the association between a computer and an IP address from these ranges for a shorter period of time than it would for other IP addresses. |
| Honeytoken account security identifiers (SIDs) | This is a user account that should have no network activities. This account will be configured as the ATA Honeytoken user. If someone attempts to use this user account, ATA will create a suspicious activity and flag this as an indication of malicious activity. To configure the Honeytoken user, the administrator will need the SID of the user account, not the user name.  To find the SID for a user, run the following Windows PowerShell cmdlet: **Get-ADUser UserName-Properties**. |
| Detection exclusions | Customer Name can exclude IP addresses from the following detections. If Customer Name enters an IP address in one of these lists, ATA will exclude that IP address from this specific type of detected activity.   * DNS Reconnaissance IP address exclusions * Pass-the-Ticket IP address exclusions |

1. ATA Database

ATA uses an open source database with the relevant agreements in place as part of the ATA installation. This database is called MongoDB. The latest version of ATA uses *wiredtiger* versus the older mmapv1 storage engine.

The following sources and procedures will help Customer Name to back up, restore, move, and manage the database if required.

* 1. Database Backup

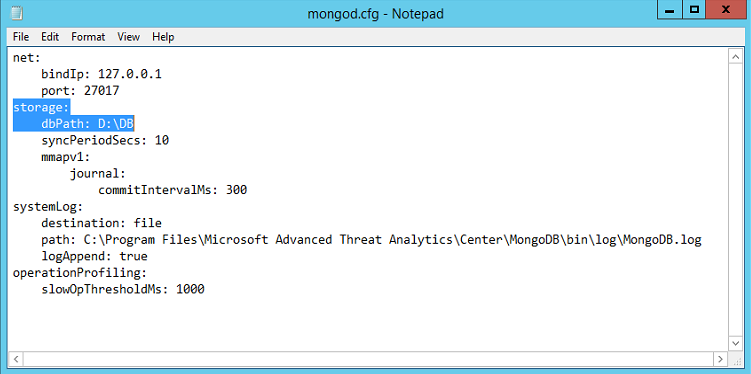
Refer to the [relevant MongoDB documentation](http://docs.mongodb.org/manual/administration/backup/).

* 1. Database Restore

Refer to the [relevant MongoDB documentation](http://docs.mongodb.org/manual/administration/backup/).

* 1. Database Move

1. Stop the **Microsoft Advanced Threat Analytics Center** service.
2. Stop the **MongoDB** service.
3. Open the Mongo configuration file, which by default is located at: C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\mongod.cfg.
4. Find the parameter *storage: dbPath*.
5. Move the folder that is listed in the *dbPath* parameter to the new location.
6. Change the *dbPath* parameter that is inside the Mongo configuration file to the new folder path, and then save and close the file.



1. Start the **MongoDB** service.
2. Open a command prompt, and run the Mongo shell by running **mongo.exe ATA**.

By default, the mongo.exe will be located in: C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin

1. Run the following command:

**db.SystemProfiles.update( {\_t: "CenterSystemProfile"} , {$set:{"Configuration.CenterDatabaseClientConfiguration.DataPath" : "<*New DB Location*>"}})** where <*New DB Location*> is the new folder path.

1. Start the **Microsoft Advanced Threat Analytics Center** service.
   1. Database Management

Refer to the [relevant Robomongo documentation](https://robomongo.org/). ***Microsoft does not support the modification of the ATA database***.

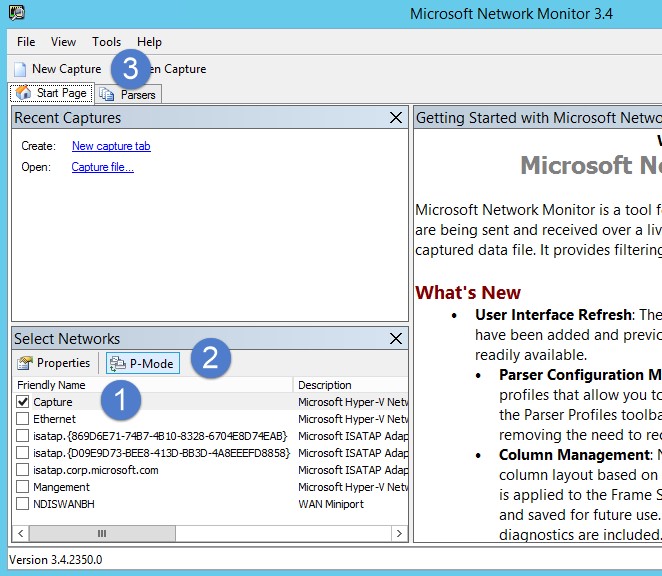
1. Port Mirroring Validation

The following steps walk the administrator through the process for validating that port mirroring is properly configured and operational if Port Mirroring was used in lieu of the ATA Lightweight Gateway.

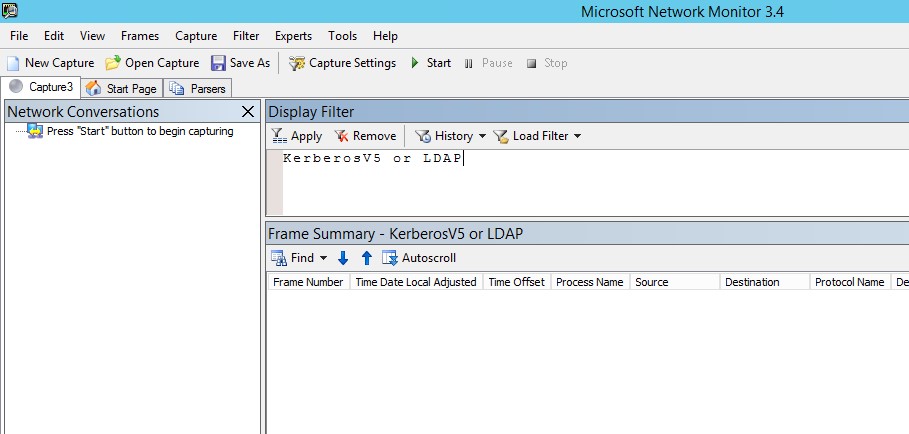
Install [Microsoft Network Monitor 3.4](https://www.microsoft.com/download/details.aspx?id=4865) or another network sniffing tool. Do not install Microsoft Message Analyzer or any other traffic capture software on the ATA Gateway.

Open Network Monitor and create a new capture tab.

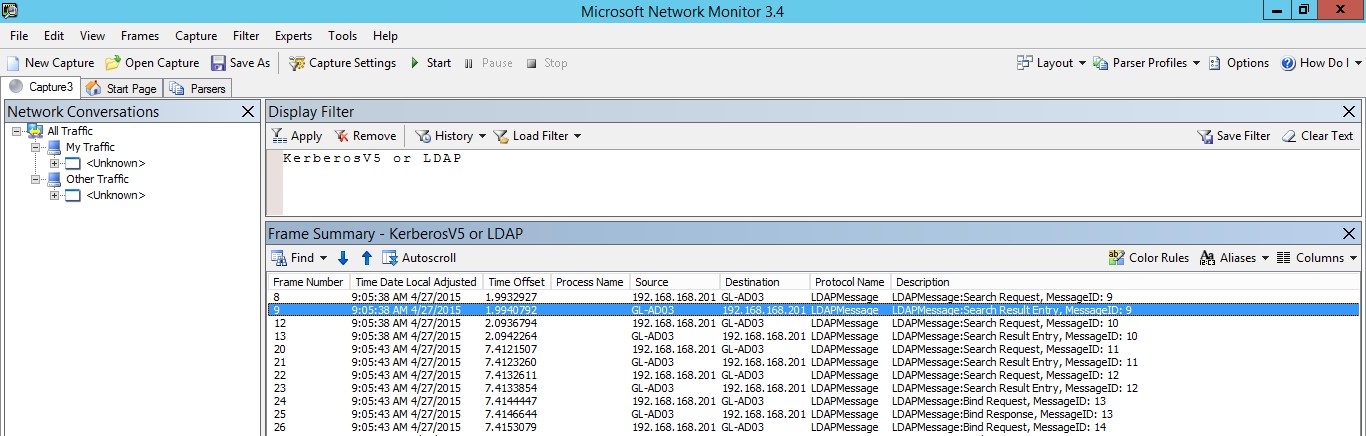
1. Select only the **Capture** network adapter or the network adapter that is connected to the switch port that is configured as the port mirroring destination.
2. If ATA has not yet been installed, verify that P-Mode is enabled. If you have already installed the ATA Gateway role, do not click **P-Mode**. Because the ATA Gateway service automatically places the NIC into promiscuous mode, selecting this option might cause issues.
3. Click **New Capture**.



1. In the **Display Filter** window, enter the following filter: **KerberosV5 or LDAP,** and then click **Apply**.



1. Click **Start** to start the capture session. If the administrator does not see traffic to and from the domain controller, review the port mirroring configuration.
2. It is important to make sure the administrator sees traffic to and from the domain controllers as shown in the following screen capture.



1. ATA Feedback Settings to Microsoft

Advanced Threat Analytics (ATA) has the ability to collect anonymized telemetry data about ATA and if enabled, will transfer the data over an HTTPS connection to Microsoft servers. This data is used by Microsoft to help improve future versions of ATA. This setting is disabled by default. If you choose to enable this, ATA will share the following:

* Performance counters from both the ATA Center and the ATA Gateway
* Product ID from licensed copies of ATA
* Deployment date of the ATA Center
* Number of deployed ATA Gateways
* The following anonymized Active Directory information:
  + Domain ID for the domain that is listed first when sorted alphabetically
  + Number of domain controllers
  + Number of domain controllers that are monitored by ATA via port mirroring
  + Number of Sites
  + Number of Computers
  + Number of Groups
  + Number of Users
* Suspicious activities—the following anonymized data is collected for each suspicious activity:
  + Suspicious activity type
  + Suspicious activity ID
  + Status
  + Start and end time
  + Input provided

(Computer names, user names, and IP addresses are not collected.)

Perform the following steps to start collecting and sending telemetry data to Microsoft:

1. Log on to the ATA Console.
2. On the toolbar, click the three dots, and then click **About**.
3. Check the box for **Send us usage information to help improve your customer experience in the future**.

1. Like suspicious activities, Health Center alerts can be dismissed or resolved and are categorized High, Medium, or Low depending on their severity. If you resolve an alert that the ATA service detects as still active, it will automatically be moved to the Open list of alerts. If the system detects that there is no longer cause for an alert (the situation has been fixed), it will automatically be moved to the Resolved list. [↑](#footnote-ref-2)