ATAIS - Operations Guide



Advanced Threat Analytics Implementation Services

**Prepared for**

Customer Name

March 9, 2018

Version Final

**Prepared by**

**Author Name**

**Contributor**

**Add contributors' names in Document Properties**

Revision and Sign-off Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Reviewers

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

Table of Contents

[1 Operations Guide Summary 7](#_Toc508371957)

[1.1 Objectives 7](#_Toc508371958)

[1.2 Tasks Summary 7](#_Toc508371959)

[1.3 Skill Requirements 8](#_Toc508371960)

[2 Threat Detection Console 10](#_Toc508371961)

[2.1 Logging on to the Console 10](#_Toc508371962)

[2.2 Console Elements 10](#_Toc508371963)

[3 Modifying ATA Center Configuration 12](#_Toc508371964)

[3.1 The ATA Console URL 12](#_Toc508371965)

[3.2 Replacing a Certificate 13](#_Toc508371966)

[3.2.1 Procedure for Replacing the Certificate 14](#_Toc508371967)

[4 Modifying ATA Gateway Configuration 16](#_Toc508371968)

[4.1 Modifying Domain Connectivity Password 16](#_Toc508371969)

[4.1.1 Procedure for Modifying the Domain Connectivity Password 16](#_Toc508371970)

[4.2 Configuring Email Alerting 17](#_Toc508371971)

[4.3 Configuring Syslog Alerts (informational) 19](#_Toc508371972)

[5 ATA Health Center 21](#_Toc508371973)

[5.1 Managing ATA Health and Alerts 21](#_Toc508371974)

[6 Suspicious Activities 22](#_Toc508371975)

[6.1 Review Suspicious Activities on the Attack Timeline 22](#_Toc508371976)

[6.2 Filtering the Activities List 23](#_Toc508371977)

[6.2.1 Suspicious Activity Severity and Status 23](#_Toc508371978)

[6.2.2 Remediating suspicious activities 24](#_Toc508371979)

[6.3 Updating a Suspicious Activity 25](#_Toc508371980)

[7 ATA Detection Settings 27](#_Toc508371981)

[8 ATA Database 30](#_Toc508371982)

[8.1 Database Backup 30](#_Toc508371983)

[8.2 Database Restore 30](#_Toc508371984)

[8.3 Moving the ATA database to another drive 30](#_Toc508371985)

[8.4 Database Management 31](#_Toc508371986)

[9 ATA Feedback Settings to Microsoft 32](#_Toc508371987)

[9.1 Disable data collection 33](#_Toc508371988)

[10 Export and Import the ATA Configuration 34](#_Toc508371989)

[11 ATA Center Issues 35](#_Toc508371990)

[11.1 Center running out of disk space 35](#_Toc508371991)

[11.2 Failure sending mail 35](#_Toc508371992)

[11.3 Center overloaded 35](#_Toc508371993)

[11.4 Failure connecting to the SIEM server using Syslog 36](#_Toc508371994)

[11.5 Center certificate is about to expire 36](#_Toc508371995)

[11.6 ATA Center certificate expired 36](#_Toc508371996)

[12 Lightweight Gateway 37](#_Toc508371997)

[12.1 Lightweight Gateway reached a memory resource limit 37](#_Toc508371998)

[13 ATA disaster recovery 38](#_Toc508371999)

[13.1 Back up your ATA Center configuration 38](#_Toc508372000)

[13.2 Recover your ATA Center 39](#_Toc508372001)

[14 Troubleshooting ATA using the performance counters 41](#_Toc508372002)

[14.1 Retrieving performance monitor files for troubleshooting 41](#_Toc508372003)

[14.2 ATA Lightweight Gateway performance counters 42](#_Toc508372004)

[14.3 ATA Center performance counters 45](#_Toc508372005)

[15 Troubleshooting ATA using the ATA database 47](#_Toc508372006)

[15.1 Interacting with the database 47](#_Toc508372007)

[16 Appendix - ATA Gateway issues (Informational) 50](#_Toc508372008)

[16.1 Read-only user password to expire shortly 50](#_Toc508372009)

[16.2 Read-only user password expired 50](#_Toc508372010)

[16.3 Gateway certificate about to expire 50](#_Toc508372011)

[16.4 Gateway certificate expired 51](#_Toc508372012)

[16.5 Domain synchronizer not assigned 51](#_Toc508372013)

[16.6 All/Some of the capture network adapters on a Gateway are not available 51](#_Toc508372014)

[16.7 Some domain controllers are unreachable by a Gateway 51](#_Toc508372015)

[16.8 All domain controllers are unreachable by a Gateway 52](#_Toc508372016)

[16.9 Gateway stopped communicating 52](#_Toc508372017)

[16.10 No traffic received from domain controller 52](#_Toc508372018)

[16.11 Some forwarded events are not being analyzed 53](#_Toc508372019)

[16.12 Some network traffic is not being analyzed 53](#_Toc508372020)

[16.13 Gateway version outdated 54](#_Toc508372021)

[16.14 Gateway service failed to start 54](#_Toc508372022)

## Tables

[Table 1: Task Summary 7](#_Toc508372023)

[Table 2: Skill Requirements and Recommendations 8](#_Toc508372024)

[Table 3: Console Elements 10](#_Toc508372025)

[Table 4: Certificate Update—ATA Center 14](#_Toc508372026)

[Table 5: Certificate Update—ATA Center 18](#_Toc508372027)

[Table 6: Suspicious Activity Severity 23](#_Toc508372028)

[Table 7: Suspicious Activity Status 24](#_Toc508372029)

[Table 8: Detection Configuration Options 27](#_Toc508372030)

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 . 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 ’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 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

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

The following skillsets are preferred for operating the ATA solution that has been deployed in ’s environment as part of this engagement. This recommendation could apply to 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 administrate 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.
2. If the computer on which the ATA Center is installed and the computer from which you are trying to access the ATA Console are both domain joined, ATA supports single sign-on integrated with Windows authentication - if you've already logged onto your computer, ATA will use that token to log you into the ATA Console. You can also log in using a smartcard. Your permissions in ATA will correspond with your administrator role.
3. To log in using SSO, make sure the ATA console site is defined as a local intranet site in your browser and that you access it using a shortname or an localhost.
   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

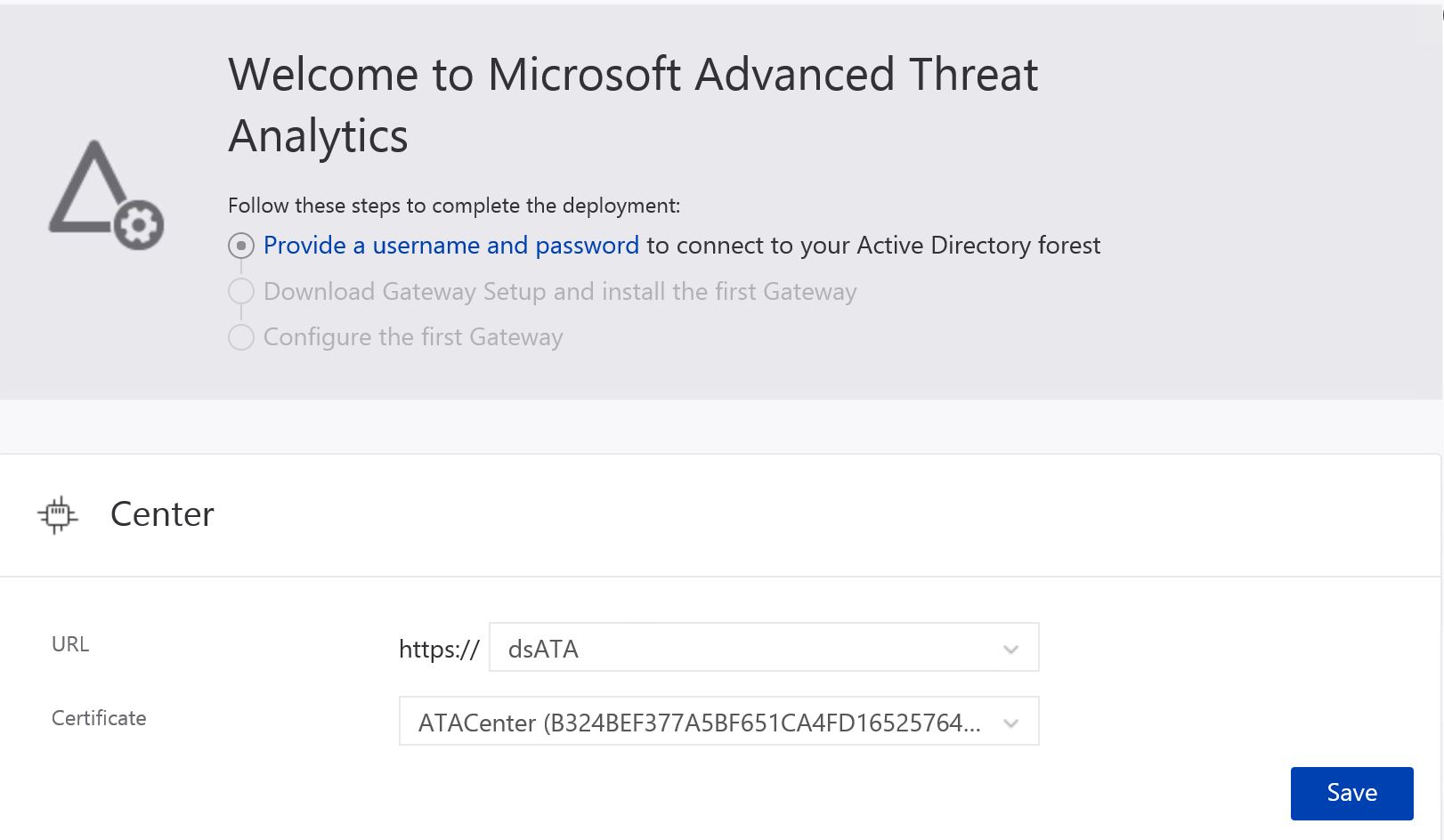
After the initial deployment, modifications to the ATA Center should be made carefully. Use the following procedures when updating the IP address and port or the certificate.

* 1. The ATA Console URL

The URL is used in the following scenarios:

* This is the URL used by the ATA Gateways to communicate with the ATA Center.
* 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 you enter an FQDN for the ATA Console URL, ensure that the ATA Gateway can resolve the FQDN to the IP address bound to the ATA Console.
* Alerts – When ATA sends out a 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 you installed a certificate from your internal Certification Authority (CA), match the URL to the subject name in the certificate. This prevents users from getting a warning message when connecting to the ATA Console.
* Using an FQDN for the ATA Console URL allows you to modify the IP address that is used by ATA Console without breaking previous alerts or downloading the ATA Gateway package again. You only need to update the DNS with the new IP address.

Replace the image below with a screenshot of your customer’s configuration



1. Make sure the new URL you want to use resolves to the IP address of the ATA Console.
2. In the ATA settings, under Center, enter the new URL. At this point, the ATA Center service will still use the original URL
3. Wait for the ATA Gateways to sync. They now have two potential URLs through which to access the ATA Console. As long as the ATA Gateway can connect using the original URL, it does not try the new one.
4. After all the ATA Gateways synced with the updated configuration, activate the new URL. When you activate the new URL, the ATA Gateways will now use the new URL to access the ATA Center. After connecting to the ATA Center service, the ATA Gateway will pull down the latest configuration and will have only the new URL for the ATA Console.

**Note**: If you entered a custom IP address, you cannot click Activate until you have installed the IP address on the ATA Center. If an ATA Gateway was offline during the first stage and never received the updated configuration, the administrator will need to update the configuration JavaScript Object Notation (JSON) file manually on that ATA Gateway.

* 1. Replacing a Certificate

If a certificate currently in use by ATA expires, replace the certificate by following this two-stage process.

Table 4: 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**: You cannot renew certificates within ATA. The only way to renew a certificate is by creating a new certificate and configuring ATA to use the new certificate.

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

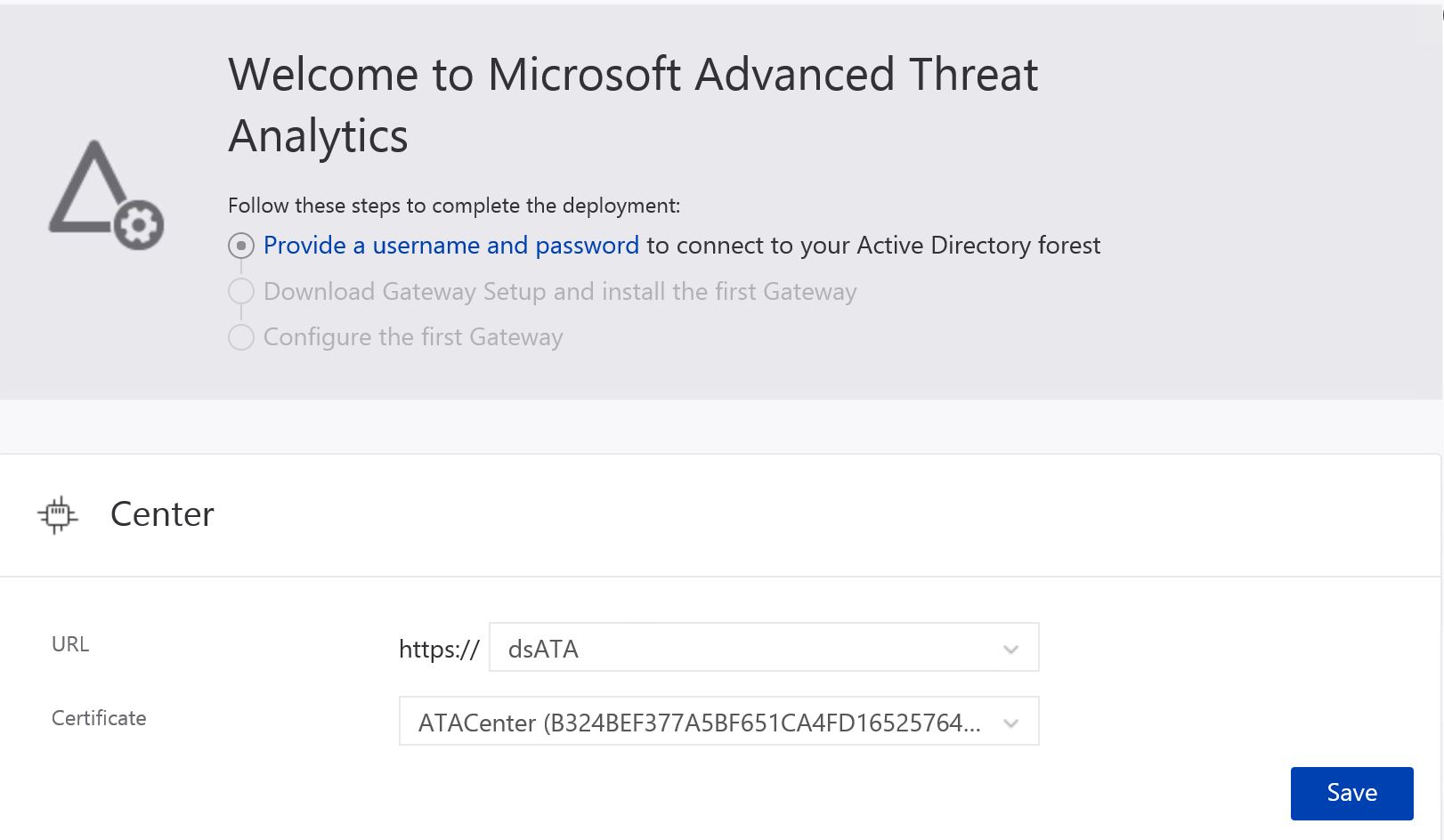
If the administrator needs to deploy a new ATA Gateway after activating the new certificate, the administrator will need to download the ATA Gateway Setup package again.

* + 1. Procedure for Replacing the Certificate

Replace the certificate by following this process:

1. Before the current certificate expires, create a new certificate and make sure it's installed on the ATA Center server. It is recommended to choose a certificate from an internal certificate authority, but it is also possible to create a new self-signed certificate. For more information see [New-SelfSignedCertificate](https://technet.microsoft.com/itpro/powershell/windows/pkiclient/new-selfsignedcertificate).
2. In the ATA settings, under Center, select this newly created certificate. At this point, the ATA Center service is still bound to the original certificate.

Replace the image below with a screenshot of your customer’s configuration



1. Wait for the ATA Gateways to sync. They now have two potential certificates that are valid for mutual authentication. As long as the ATA Gateway can connect using the original certificate, it does not try the new one.
2. After all the ATA Gateways synced with the updated configuration, activate the new certificate that ATA Center service is bound to. When you activate the new certificate, the ATA Center service binds to the new certificate. ATA Gateways will now use the new certificate to authenticate with the ATA Center. After connecting to the ATA Center service, the ATA Gateway will pull down the latest configuration and will have only the new certificate for the ATA Center.

**Note**: If an ATA Gateway was offline while you activated the new certificate, and never received the updated configuration, you must manually update the configuration JSON file on the ATA Gateway.

The certificate that you are using must be trusted by the ATA Gateways.

The certificate is also used for the ATA Console, so it should match the ATA Console address to avoid browser warnings.

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

1. Modifying ATA Gateway Configuration
   1. Modifying Domain Connectivity Password

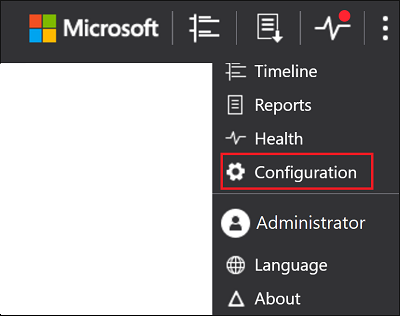
If you modify the Domain Connectivity Password, make sure that the password you enter is correct. If it is not, the ATA Gateway service will stop running on the ATA Gateways.

If you suspect that this happened, on the ATA Gateway, look at the Microsoft.Tri.GatewayErrors.log file for the following: *The supplied credential is invalid.*

To correct this, follow this procedure to update the Domain Connectivity password on the ATA Center:

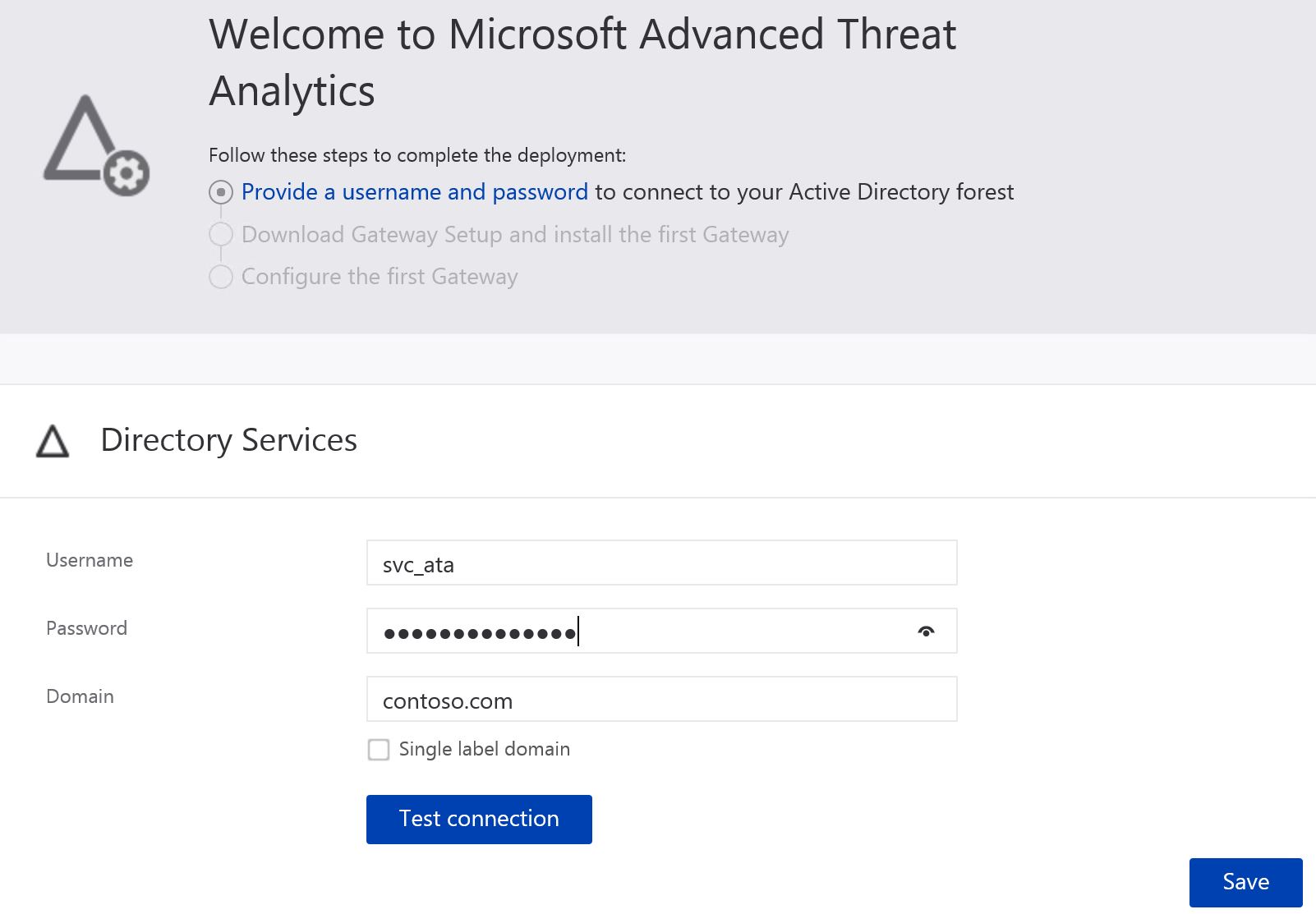
* + 1. Procedure for Modifying the Domain Connectivity Password

1. Open the ATA Console on the ATA Center.
2. Select the settings option on the toolbar and select **Configuration**.



1. Select **Directory Services.**

Replace the image below with a screenshot of your customer’s configuration



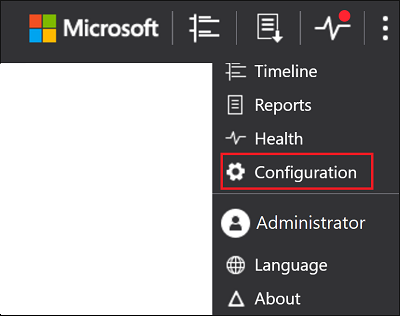
1. Under **Password**, change the password.

If the ATA Center have connectivity to the domain, use the **Test Connection** button to validate the credentials

1. Click **Save**.
2. After changing the password, manually check that the ATA Gateway service is running on the ATA Gateway servers.
   1. Configuring Email Alerting

ATA can notify you when it detects a suspicious activity. For ATA to be able to send email notifications, you must first configure the **Email server settings**.

1. On the ATA Center server, click the **Microsoft Advanced Threat Analytics Management** icon on the desktop.
2. Enter your user name and password and click **Log in**.
3. Select the settings option on the toolbar and select **Configuration**.



1. Under Mail server, enter the following information:

Enter the appropriate information for the values in the table below (the right hand column)

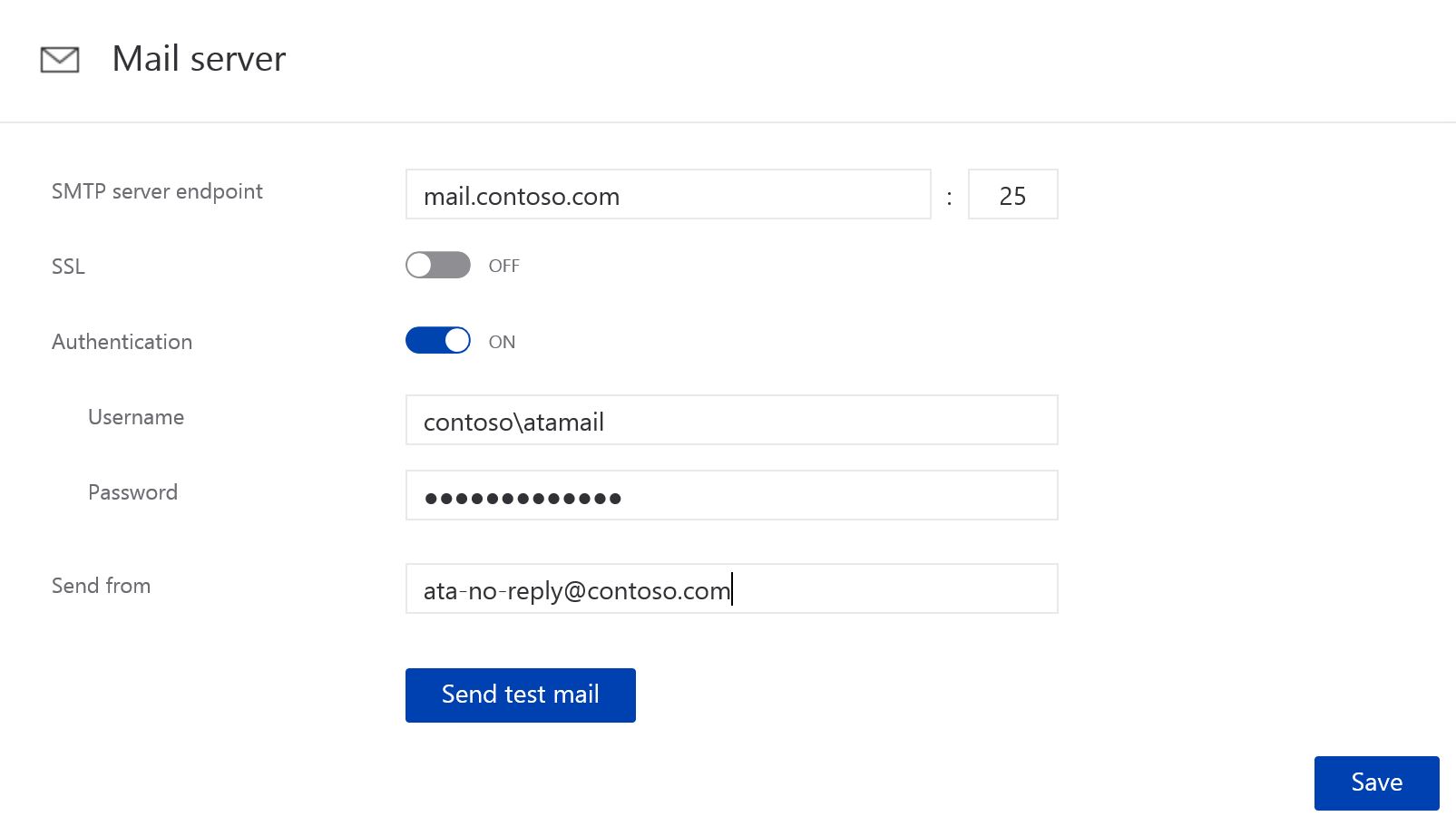
Table 5: Certificate Update—ATA Center

|  |  |  |
| --- | --- | --- |
| Field | Description | Value |
| SMTP server endpoint (required) | Enter the FQDN of the SMTP server. | Mail.domain.com |
| SSL | Toggle Secure Sockets Layer (SSL) if the SMTP server requires SSL.  **Note**: 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.  **Note**: 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. | Enabled |
| Send from (required) | Enter an email address from whom the email will be sent. | not-reply-ata@contoso.com |

**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.

Suspicious activities and health alerts can be alerted via email.

Replace the image below with a screenshot from your customer’s environment with the relevant settings (which should be the same as those entered in the table above)



* 1. Configuring Syslog Alerts (informational)

ATA can notify you when it detects a suspicious activity, update a suspicious activity or if there is a health alert by sending the notification to your Syslog server. If you enable Syslog notifications, you can set the following for them.

1. Before configuring Syslog notifications, work with your SIEM admin to find out the following information:

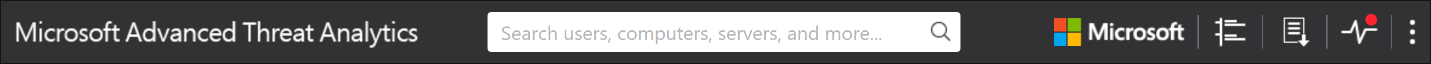
* FQDN or IP address of the SIEM server
* Port on which the SIEM server is listening
* What transport to use: UDP, TCP or TLS (Secured Syslog)
* Format in which to send the data RFC 3164 or 5424

1. On the ATA Center server, click the Microsoft Advanced Threat Analytics Management icon on the desktop.
2. Enter your user name and password and click Log in.
3. Select the settings option on the toolbar and select Configuration.
4. Under **Notifications** section, Select **Syslog** server and enter the following information:

|  |  |
| --- | --- |
| Field | Description |
| Syslog server endpoint | FQDN of the Syslog server and optionally change the port number (default 514) |
| Transport | Can be UDP, TCP or TLS (Secured Syslog) |
| Format | This is the format that ATA uses to send events to the SIEM server - either RFC 5424 or RFC 3164. |

1. ATA Health Center

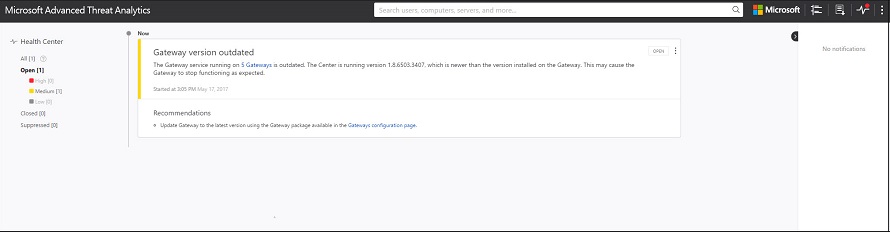
The ATA Health Center alerts Customer Name to performance, stability, or availability issues in the ATA infrastructure by placing a red dot above the Health Center icon in the menu bar, as shown below:



* 1. Managing ATA Health and Alerts

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

* All open alerts can be managed by setting them to **Close** or **Suppress**. In the alert, click **Open,** and then scroll down to either **Close** or **Suppress**.
* 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 **Close** issues list.
* **The Suppress** list includes issues that the administrator wants to ignore ongoing activity but alerted if it resumes after a day—for example, if the administrator is alerted to an issue that the administrator knows exists, does not plan to close, does not want to be notified about, and does not want to see on the **Open** issues list, the administrator can set it to **Suppress**.



1. Suspicious Activities

This topic explains the basics of how to work with ATA. This section does not cover how to respond to suspicious activities but rather how to work with them in the console and filter these activities.

* 1. Review Suspicious Activities on the Attack Timeline

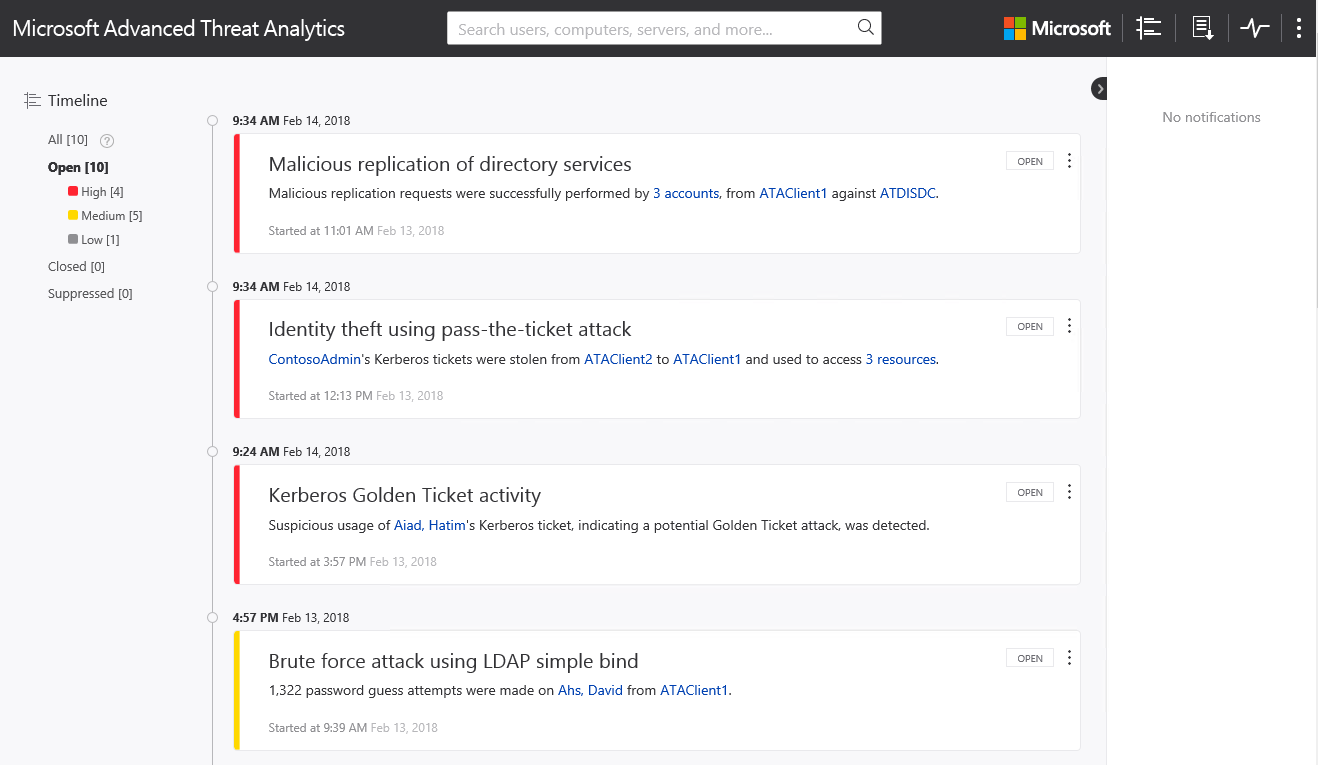
After logging on to the ATA Console, the administrator is taken automatically to the open **Suspicious Activities Timeline**. Suspicious activities are listed in chronological order with the newest suspicious activities at the top of the timeline. Each suspicious activity has the following information:

* 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, Close, Suppress, Close and exclude, Delete

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.
* Download the suspicious activity to Excel.

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



**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**, **Closed**, or **Suppressed**.
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 6: 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.

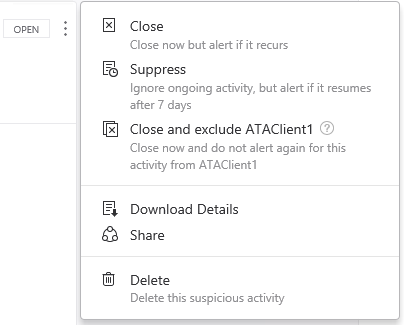
Table 7: Suspicious Activity Status

|  |  |
| --- | --- |
| Status | Description |
| Open | All new suspicious activities appear in this list. |
| Closed | Used to track suspicious activities that Customer Name identified, researched, and fixed or mitigated. |
| Suppressed | Activities that Customer Name dismissed manually. If ATA detects a similar suspicious activity after 7 days, a new detection will be created. |

**Note:** ATA may re-open a Closed activity if the same activity is detected again within a short period of time.

* + 1. Remediating suspicious activities

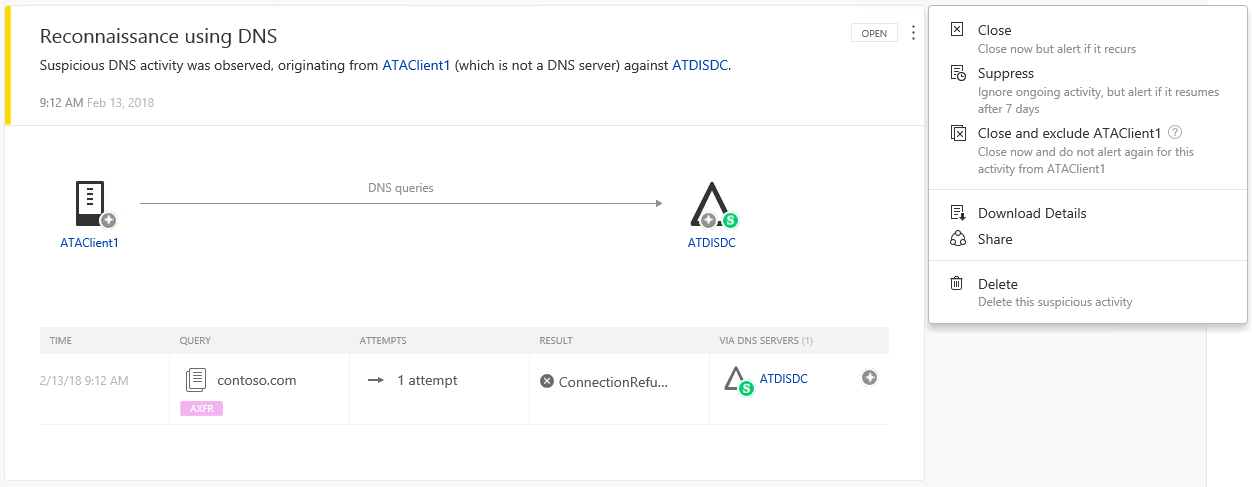
You can change the status of a suspicious activity by clicking the current status of the suspicious activity and selecting one of the following **Open**, **Suppressed**, **Closed** or **Deleted**. To do this, click the three dots at the top right corner of a specific suspicious activity to reveal the list of available actions.



* 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. Customer Name can provide inputs to ATA to exclude entities while considering if the activity is suspicious or not. In the following example, the administrator is being asked if running scanning tools is allowed from a specific computer.



1. However, if the administrator chose to close and exclude, the suspicious activity might be closed, and future activities of this type from this computer might not generate a suspicious activity alert.
2. If Customer Name’s ATA administrator is not sure, click **Cancel,** and follow up with the entity owner.
3. Customer Name can change the status of a closed suspicious activity by clicking the current status of the suspicious activity and selecting **Re-Open**
4. 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 8: Detection Configuration Options

|  |  |
| --- | --- |
| Item | Description |
| Honeytoken account security identifiers | This is a user account which 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 to add those accounts under General section. |
| Detection exclusions | Customer Name can exclude IP addresses or users from the following detections. If Customer Name enters an IP address or users in one of these lists, ATA will exclude that IP address from this specific type of detected activity.   * Abnormal modification of sensitive groups * Identitiy theft using pass the ticket attack * Kerberos Golden ticket activity * Malicious data protection private request * Malicious replication of directory services * Reconnaissance using account enumeration * Reconnaissance using directory services queries * Reconnaisance using DNS * Reconnaisance using SMB Session Enumeration * Remote execution attempt detected * Suspicion of identitiy theft on abnormal behavior * Unusual protocol implementation |

This topic explains how to exclude entities from triggering alerts in order to minimize true benign positives while still alerting for malign positives.

**Note**: A benign positive is an occurrence which matches attacker behavior but is under the control or direction of Customer Name. For example, a “Remote execution attempt detected” alert generated by an administrator using PsExec to run code remotely against a domain controller would be considered a benign positive, because code was indeed executed remotely, but the impact is benign. It is important to distinguish between benign positives and false negatives. False negatives are flaws in the detection engine which should be resolved by code updates in future. Benign positives should be addressed by setting exclusions for the known entities.

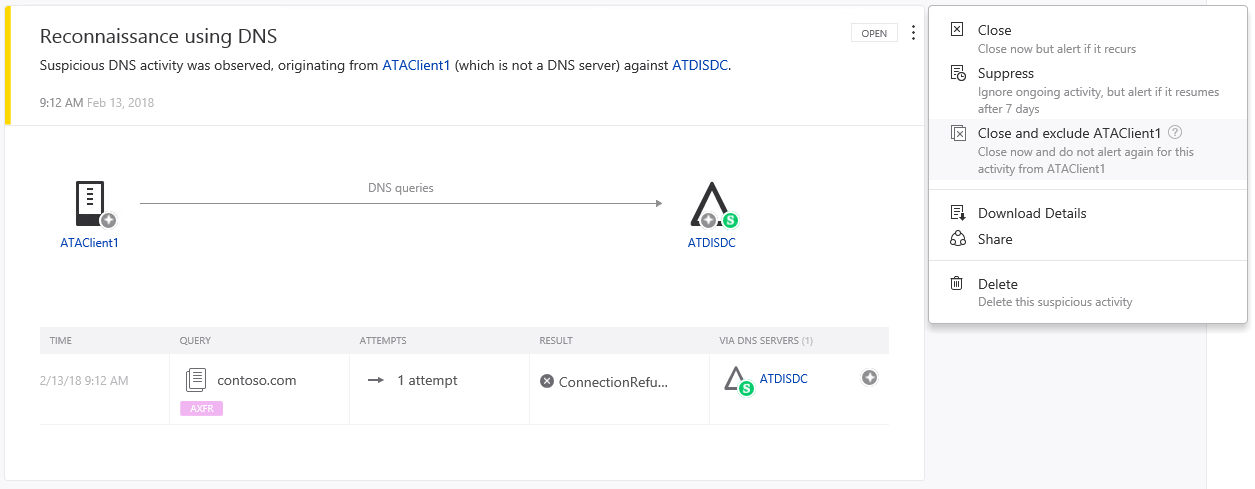
In order to keep ATA from generating alerts about activities that, from specific users, may be part of your normal rhythm of business, you can exclude specific entities from raising alerts.

For example, you may wish to exclude a security scanner which performs DNS reconnaissance or an administrator who remotely executes scripts on a domain controller from a specific workstation (sanctioned activities which form a part of the normal IT operations in your organization).

To exclude entities from raising alerts in ATA:

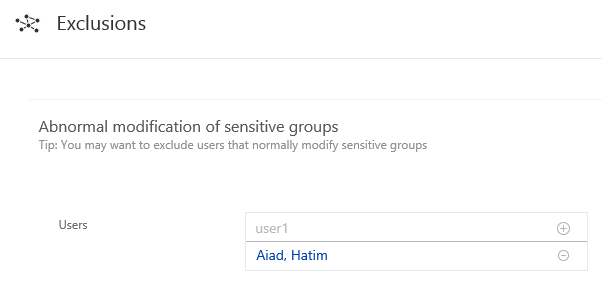
There are two ways in which you can exclude entities, from the suspicious activity itself, or from the **Exclusions** tab on the **Configuration** page.

* **From the suspicious activity**: In the Suspicious activity timeline, when you receive an alert on an activity for a user or computer or IP address that is allowed to perform the particular activity and may do so frequently, left click the three dots at the end of the row for the suspicious activity on that entity, and select **Close and exclude**.   
  This will add the user, computer or IP address to the exclusions list for that suspicious activity. It will also close the suspicious activity and it will no longer be listed in the **Open** events list in the **Suspicious activity timeline**.



* **From the Configuration page**: under the **Detection** section on the left pane, click **Exclusions** and then select the suspicious activity you want to exclude, such as **Abnormal modification of sensitive group**.

**Enter the entity to be excluded from the type of suspicious activity selected. Click the plus sign then save** at the bottom of the page.



To remove an entity from the **Exclusions** configuration, click the minus next to the entity name and then click **Save** at the bottom of the page. It is recommended that you add exclusions to detections only after you get alerts of the type and determine that they are true benign positives.

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/).

For example, the following command was used during the test case:

mongodump.exe /d ATA /o "target backup folder"

* 1. Database Restore

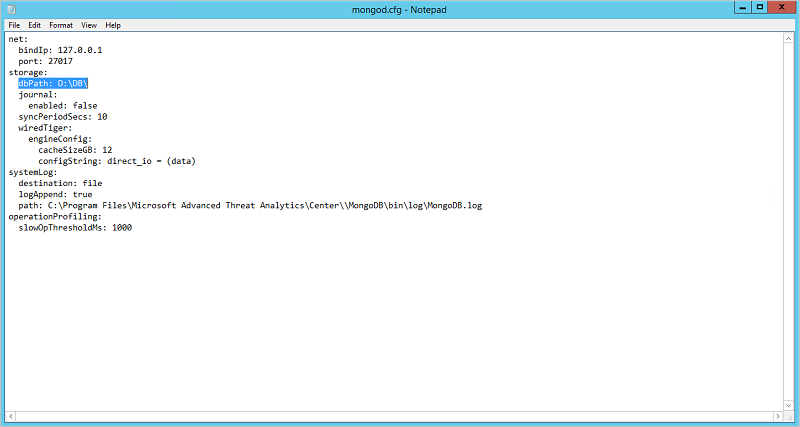
Refer to the [relevant MongoDB documentation](http://docs.mongodb.org/manual/administration/backup/).

For example, the following command was used during the test case:

mongorestore.exe /d ATA /dir: "Target backup folder\ATA" /objcheck

* 1. Moving the ATA database to another drive

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/).

**Important Note**: Microsoft does not support the modification of the ATA database.

1. ATA Feedback Settings to Microsoft

Advanced Threat Analytics (ATA) collects anonymized telemetry data about ATA and transmits the data over an HTTPS connection to Microsoft servers. This data is used by Microsoft to help improve future versions of ATA. 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 whose name would be the first domain when sorted alphabetically
* Number of domain controllers
* Number of domain controllers 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.)

* Health issues – The following anonymized data is collected for each health issue:

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

* + Health issue type
  + Health issue ID
  + Status
  + Start and End Time
* ATA Console URL addresses - URL addresses when using the ATA Console i.e. which pages in the ATA Console are visited.
  1. Disable data collection

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

1. Log in to the ATA Console, click the three dots in the toolbar and select **About**.
2. Uncheck the box for **Send us usage information to help improve your customer experience in the future**.
3. Export and Import the ATA Configuration

The configuration of ATA is stored in the "SystemProfile" collection in the database. This collection is backed up every hour by the ATA Center service to files called SystemProfile\_timestamp.json. The most recent ten versions are stored. This is located in a subfolder called "Backup". In a default ATA installation, the file is located in C:\Program Files\Microsoft Advanced Threat Analytics\Center\Backup\.

**Note:** It is recommended that you back up this file to a safe location when making major changes to ATA.

It is possible to restore all the settings by running the following command:

mongoimport.exe --db ATA --collection SystemProfile --file "<SystemProfile.json backup file>" –upsert

1. ATA Center Issues
   1. Center running out of disk space

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The free space on the ATA Center machine drive that is used for storing the ATA database is getting low. | This means that the hard drive has less than 200 GB of free space or that there is less than 20% free space, whichever is smaller. When ATA recognizes that the drive is running low on space, it starts to delete old data from the database. If it cannot delete old data because it still needs the data for the detection engine, you will receive this alert. When you receive this alert, ATA stops keeping track of new activities. | Increase the drive size or free up space from that drive. | High |

* 1. Failure sending mail

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| ATA Failed to send an email notification to the specified mail server. | No email messages will be sent from ATA. | Verify the SMTP server configuration. | Low |

* 1. Center overloaded

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Center is not able to handle the amount of data being transferred from the ATA Gateways. | The ATA Center will stop analyzing new network traffic and events. This means that the accuracy of the detections and profiles is reduced while this monitoring alert is active. | Make sure that you provided enough resources for the ATA Center. See [ATA capacity planning](https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-capacity-planning) for more details on how to properly plan for ATA Center capacity. Investigate the performance of the ATA Center using [Troubleshooting ATA using the performance counters](https://docs.microsoft.com/en-us/advanced-threat-analytics/troubleshooting-ata-using-perf-counters). | High |

* 1. Failure connecting to the SIEM server using Syslog

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| ATA failed to send events to the specified SIEM. | This means the ATA Center cannot send suspicious activities and monitoring alerts to your SIEM. | Make sure that your [Syslog server settings are configured correctly](https://docs.microsoft.com/en-us/advanced-threat-analytics/setting-syslog-email-server-settings). | Low |

* 1. Center certificate is about to expire

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Center certificate will expire in less than 3 weeks. | After the certificate expires: Connectivity from ATA Gateways to ATA Center will fail. The ATA Center process will crash and all ATA functionality will stop. | [Replace the ATA Center certificate](https://docs.microsoft.com/en-us/advanced-threat-analytics/modifying-ata-center-configuration) | Medium |

* 1. ATA Center certificate expired

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Center certificate expired. | After the certificate expires: Connectivity from the ATA Gateways to the ATA Center will fail. The ATA Center process will crash and all ATA functionality will stop. | [Replace the ATA Center certificate](https://docs.microsoft.com/en-us/advanced-threat-analytics/modifying-ata-center-configuration) | High |

1. Lightweight Gateway
   1. Lightweight Gateway reached a memory resource limit

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The Lightweight ATA Gateway stopped itself and will restart automatically to protect the domain controller from a low memory condition. | The Lightweight ATA Gateway enforces memory limitations upon itself to prevent the domain controller from experiencing resource limitations. This happens when memory usage on the domain controller is high. Data from this domain controller is only partly monitored. | Increase the amount of memory (RAM) on the domain controller or add more domain controllers in this site to better distribute the load of this domain controller. | Medium |

1. ATA disaster recovery

This section provides Customer Name with guidance to quickly recover an ATA Center and restore ATA functionality in the event that the ATA Center has become permanently unavailable but the ATA Gateways are still working.

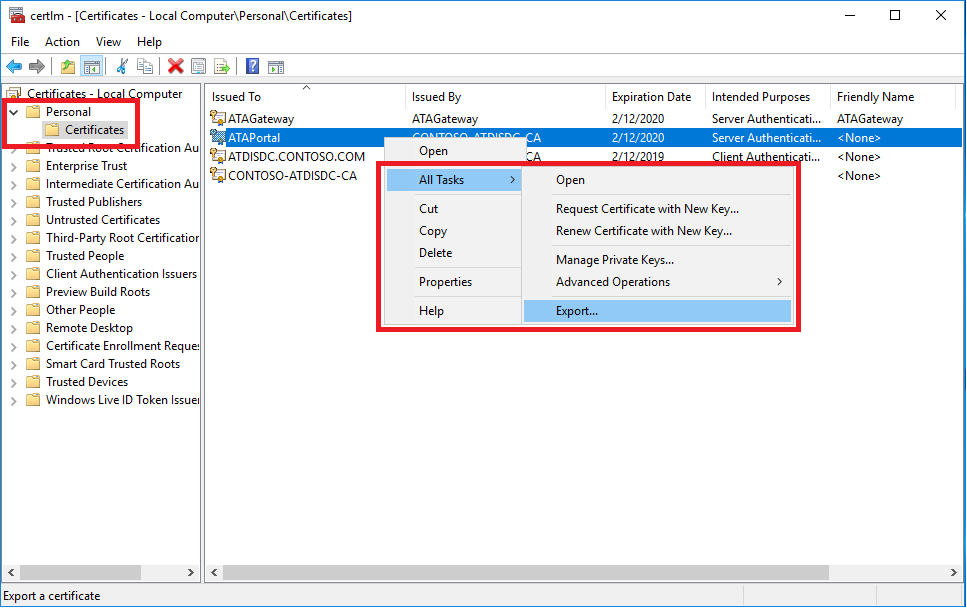
**Note:** The process described does not recover previously detected suspicious activities but does return the ATA Center to full functionality. Additionally, the learning period needed for some behavioral detections will restart, but most of the detection that ATA offers is operational after the ATA Center is restored.

* 1. Back up your ATA Center configuration

1. The ATA Center configuration is backed up to a file every hour. Locate the latest backup copy of the ATA Center configuration and save it on a separate computer. For a full explanation of how to locate these files, see [Export and import the ATA configuration](https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/ata-configuration-file).
2. Export the ATA Center certificate.
3. In the certificate manager, navigate to **Certificates (Local Computer)** -> **Personal** ->**Certificates**, and select **ATA Center**.

**Note**: If you use a certificate managed by your organization’s Certificate Authority, select the appropriate certificate name.

1. Right click the certificate name and select **All Tasks** followed by **Export**.



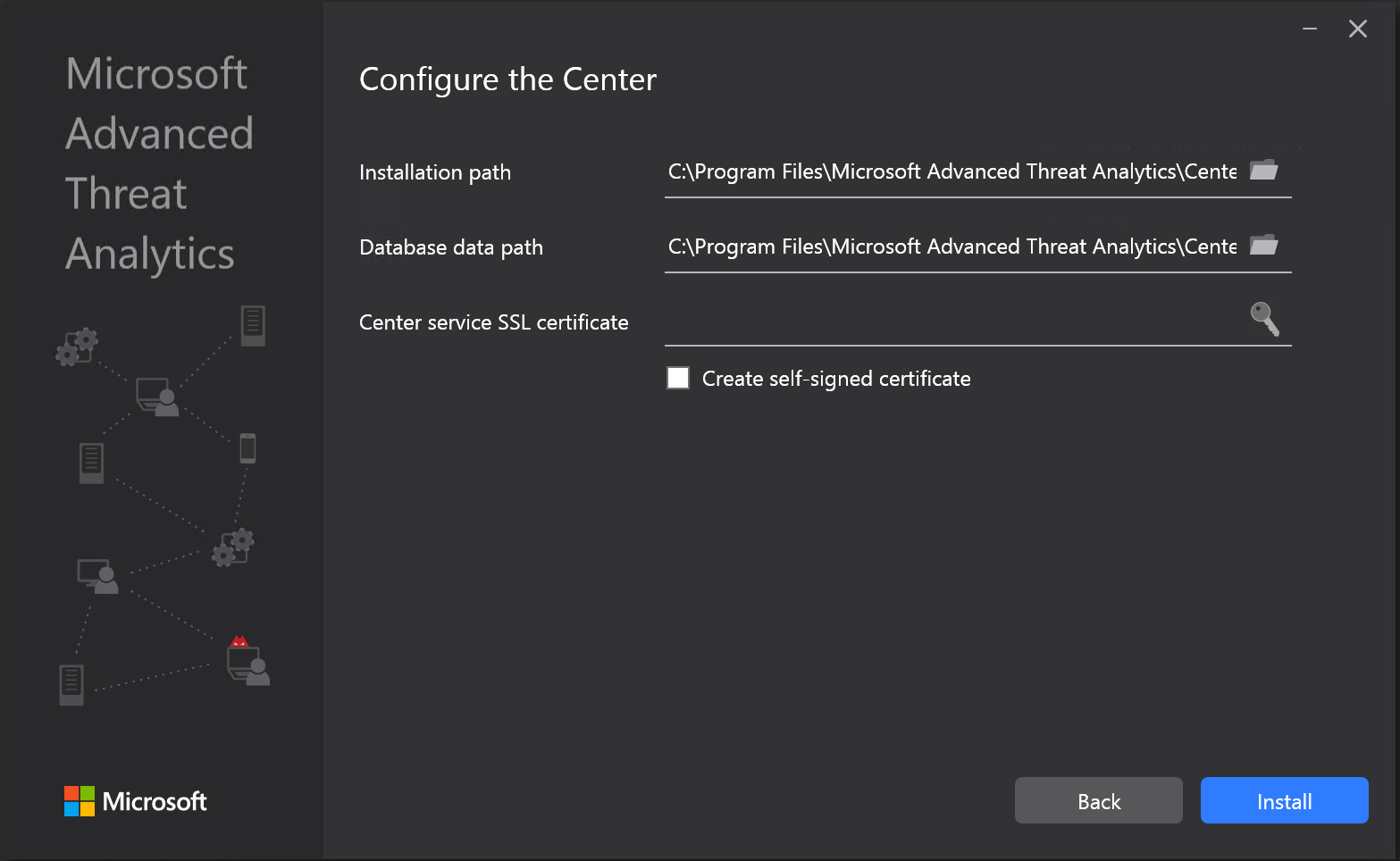
**Note**: In this example screenshot, the ATA Center uses a custom certificate called ATAPortal, rather than a self-signed certificate.

1. Follow the instructions to export the certificate, making sure to export the private key as well.
2. Back up the exported certificate file on a separate computer.

**Note:** If you cannot export the private key, you must create a new certificate and deploy it to ATA, as described in [Change the ATA Center certificate](https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/modifying-ata-config-centercert), and then export it.

* 1. Recover your ATA Center

1. Create a new Windows Server machine using the same IP address and computer name as the previous ATA Center machine.
2. Import the certificate you backed up, above, to the new server.
3. Follow the instructions to [Deploy the ATA Center](https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/install-ata-step1) on the newly created Windows Server. There is no need to deploy the ATA Gateways again. When prompted for a certificate, provide the certificate you exported when backing up the ATA Center configuration.



1. Import the backed up ATA Center configuration:
2. Remove the default ATA Center System Profile document from the MongoDB:
3. Go to C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin.
4. Run mongo.exe ATA

**Note**: The database name is case-sensitive and must be entered as ATA in all capital letters.

1. Run this command to remove the default system profile: db.SystemProfile.remove({})
2. Using an ATA backup file (see section 13.1), run the following command (substituting the appropriate name for <SystemProfile.json backup file>):

mongoimport.exe --db ATA --collection SystemProfile --file "<SystemProfile.json backup file>" --upsert.

For a full explanation of how to locate and import backup files, see [Export and import the ATA configuration.](https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/ata-configuration-file)

1. Open the ATA Console. You should see all the ATA Gateways linked under the Configuration/System/Gateways tab.
2. Make sure to define a [Directory Services user](https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/install-ata-step2) and to choose a [Domain controller synchronizer](https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/install-ata-step5).
3. Troubleshooting ATA using the performance counters

The ATA performance counters provide insight into how well each component of ATA is performing. The components in ATA process data sequentially, so that when there's a problem, it might cause partial dropped traffic somewhere along the chain of components. In order to fix the problem, you have to figure out which component is backfiring and fix the problem at the beginning of the chain. Use the data found in the performance counters to understand how each component is functioning. Refer to [ATA architecture](https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-architecture) to understand the flow of internal ATA components.

**ATA component process**:

1. When a component reaches its maximum size, it blocks the previous component from sending more entities to it.
2. Then, eventually the previous component will start to increase **its** own size until it blocks the component before it, from sending more entities.
3. This happens all the way back to the **NetworkListener** component which will drop traffic when it can no longer forward entities.
   1. Retrieving performance monitor files for troubleshooting

To retrieve the performance monitor files (BLG) from the various ATA components:

1. Open Performance Monitor.
2. Stop the data collector set named: "Microsoft ATA Gateway " or “Microsoft ATA Center”.
3. Go to the data collector set folder (by default, this is C:\Program Files\Microsoft Advanced Threat Analytics\Gateway\Logs\DataCollectorSets or C:\Program Files\Microsoft Advanced Threat Analytics\Center\Logs\DataCollectorSets).
4. Copy the BLG file that was most recently modified.
5. Restart the data collector set named: "Microsoft ATA Gateway" or “Microsoft ATA Center”.
   1. ATA Lightweight Gateway performance counters

The performance counters can be used for quota management in the Lightweight Gateway, to make sure that ATA doesn't drain too many resources from the domain controllers on which it is installed. To measure the resource limitations that ATA enforces on the Lightweight Gateway, add these counters.

This is done by opening "Performance Monitor" and adding all counters for the ATA Lightweight Gateway. The name of the performance counter objects are: "Microsoft ATA Gateway" and "Microsoft ATA Gateway Updater".

|  |  |  |  |
| --- | --- | --- | --- |
| **Counter** | **Description** | **Threshold** | **Troubleshooting** |
| Microsoft ATA Gateway Updater\GatewayUpdaterResourceManager CPU Time Max % | The maximum amount of CPU time (in percentage) that the Lightweight Gateway process can consume. | No threshold. | This is the limitation that protects the domain controller resources from being used up by the ATA Lightweight Gateway. If you see that the process reaches the maximum limit often over a period of time (the process reaches the limit and then starts to drop traffic) it means that you need to add more resources to the server running the domain controller.. |
| Microsoft ATA Gateway Updater\GatewayUpdaterResourceManager Commit Memory Max Size | The maximum amount of committed memory (in bytes) that the Lightweight Gateway process can consume. | No threshold. | This is the limitation that protects the domain controller resources from being used up by the ATA Lightweight Gateway. If you see that the process reaches the maximum limit often over a period of time (the process reaches the limit and then starts to drop traffic) it means that you need to add more resources to the server running the domain controller. |
| Microsoft ATA Gateway Updater\GatewayUpdaterResourceManager Working Set Limit Size | The Maximum amount of physical memory (in bytes) that the Lightweight Gateway process can consume. | No threshold. | This is the limitation that protects the domain controller resources from being used up by the ATA Lightweight Gateway. If you see that the process reaches the maximum limit often over a period of time (the process reaches the limit and then starts to drop traffic) it means that you need to add more resources to the server running the domain controller. |

In order to see your actual consumption, refer to the following counters:

|  |  |  |  |
| --- | --- | --- | --- |
| **Counter** | **Description** | **Threshold** | **Troubleshooting** |
| Process(Microsoft.Tri.Gateway)\%Processor Time | The amount of CPU time (in percentage) that the Lightweight Gateway process is actually consuming. | No threshold. | Compare the results of this counter to the limit found in GatewayUpdaterResourceManager CPU Time Max %. If you see that the process reaches the maximum limit often over a period of time (the process reaches the limit and then starts to drop traffic) it means that you need to dedicate more resources to the Lightweight Gateway. |
| Process(Microsoft.Tri.Gateway)\Private Bytes | The amount of committed memory (in bytes) that the Lightweight Gateway process is actually consuming. | No threshold. | Compare the results of this counter to the limit found in GatewayUpdaterResourceManager Commit Memory Max Size. If you see that the process reaches the maximum limit often over a period of time (the process reaches the limit and then starts to drop traffic) it means that you need to dedicate more resources to the Lightweight Gateway. |
| Process(Microsoft.Tri.Gateway)\Working Set | The amount of physical memory (in bytes) that the Lightweight Gateway process is actually consuming. | No threshold. | Compare the results of this counter to the limit found in GatewayUpdaterResourceManager Working Set Limit Size. If you see that the process reaches the maximum limit often over a period of time (the process reaches the limit and then starts to drop traffic) it means that you need to dedicate more resources to the Lightweight Gateway. |

* 1. ATA Center performance counters

You can observe the real-time performance status of the ATA Center by adding the ATA Center's performance counters.

This is done by opening "Performance Monitor" and adding all counters for the ATA Center. The name of the performance counter object is: "Microsoft ATA Center".

Here is the list of the main ATA Center counters to pay attention to:

|  |  |  |  |
| --- | --- | --- | --- |
| **Counter** | **Description** | **Threshold** | **Troubleshooting** |
| Microsoft ATA Center\EntityReceiver Entity Batch Block Size | The number of entity batches queued by the ATA Center. | Should be less than the maximum-1 (default maximum: 10,000) | Check if there is any component that reached its maximum size and is blocking previous components all the way to the NetworkListener. Refer to the **ATA Component Process** above.  Check that there is no issue with the CPU or memory. |
| Microsoft ATA Center\NetworkActivityProcessor Network Activity Block Size | The number of Network Activities (NAs) queued for processing. | Should be less than the maximum-1 (default maximum: 50,000) | Check if there is any component that reached its maximum size and is blocking previous components all the way to the NetworkListener. Refer to the **ATA Component Process** above.  Check that there is no issue with the CPU or memory. |
| Microsoft ATA Center\EntityProfiler Network Activity Block Size | The number of Network Activities (NAs) queued for profiling. | Should be less than the maximum-1 (default maximum: 10,000) | Check if there is any component that reached its maximum size and is blocking previous components all the way to the NetworkListener. Refer to the **ATA Component Process** above.  Check that there is no issue with the CPU or memory. |
| Microsoft ATA Center\Database \* Block Size | The number of Network Activities (NAs), of a specific type, queued to be written to the database. | Should be less than the maximum-1 (default maximum: 50,000) | Check if there is any component that reached its maximum size and is blocking previous components all the way to the NetworkListener. Refer to the **ATA Component Process** above.  Check that there is no issue with the CPU or memory. |

1. Troubleshooting ATA using the ATA database

ATA uses MongoDB as its database. You can interact with the database using the default command line or using a user interface tool to perform advanced tasks and troubleshooting.

* 1. Interacting with the database

The default and most basic way to query the database is using the Mongo shell. Perform these steps from the ATA Center server.

1. Open a command prompt and change the path to the MongoDB bin folder. The default path is C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin.
2. Run the following command:

mongo.exe ATA

**Note**: The database name is case-sensitive and must be entered as ATA in all capital letters.

1. Within the Mongo shell, run the desired command. A number of useful command strings are provided below.

|  |  |  |
| --- | --- | --- |
| **How to...** | **Syntax** | **Notes** |
| Check for collections in the database. | show collections | Useful as an end-to-end test to see that traffic is being written to the database and that event 4776 is being received by ATA. |
| Get the details of a user/computer/group (UniqueEntity), such as user ID. | db.UniqueEntity.find({SearchNames: "<name of entity in lower case>"}) |  |
| Find Kerberos authentication traffic originating from a specific computer on a specific day. | db.KerberosAs\_<datetime>.find({SourceComputerId: "<Id of the source computer>"}) | To get the <ID of the source computer> you can query the UniqueEntity collections, as shown in the example.  Each network activity type, for example Kerberos authentications, has its own collection per UTC date. |
| Find NTLM traffic originating from a specific computer related to a specific account on a specific day. | db.Ntlm\_<datetime>.find({SourceComputerId: "<Id of the source computer>", SourceAccountId: "<Id of the account>"}) | To get the <ID of the source computer> and <ID of the account> you can query the UniqueEntity collections, as shown in the example.  Each network activity type, for example NTLM authentications, has its own collection per UTC date. |
| Search for advanced properties such as the active dates of an account. | db.UniqueEntityProfile.find({UniqueEntityId: "<Id of the account>") | To get the <ID of the account> you can query the UniqueEntity collections, as shown in the example. The property name that shows the dates in which the account has been active is called: "ActiveDates". For example you may want to know if an account has at least 21 days of activity for the abnormal behavior machine learning algorithm to be able to run on it. |
| Make advanced configuration changes. In this example we change the send queue size for all ATA Gateways to 10,000. | db.SystemProfile.update( {\_t: "GatewaySystemProfile"} , {$set:{"Configuration.EntitySenderConfiguration.EntityBatchBlockMaxSize" : "10000"}}) | ` |

1. Appendix - ATA Gateway issues (Informational)

Update the language below if the customer has deployed ATA Gateways.

At the time of writing, Customer Name does not have a plan to implement ATA Gateway. This section is for informational only for ATA Gateway troubleshooting reference.

* 1. Read-only user password to expire shortly

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The read-only user password, used to perform resolution of entities against Active Directory, is about to expire in less than 30 days. | If the password for this user expires, all the ATA Gateways will stop running and no new data will be collected. | [Change the domain connectivity password](https://docs.microsoft.com/en-us/advanced-threat-analytics/modifying-ata-config-dcpassword) and then update the password in the ATA Console. | Medium |

* 1. Read-only user password expired

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The read-only user password, used to get directory data, expired. | All the ATA Gateways will stop running (or will top running soon) and no new data will be collected. | [Change the domain connectivity password](https://docs.microsoft.com/en-us/advanced-threat-analytics/modifying-ata-config-dcpassword) and then update the password in the ATA Console. | High |

* 1. Gateway certificate about to expire

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Gateway certificate will expire in less than 3 weeks. | Connectivity from the specific ATA Gateway to the ATA Center will fail. No data from that ATA Gateway will be sent. | The ATA Gateway certificate should have been renewed automatically. Read the ATA Gateway and ATA Center logs to understand why that Certificate did not renew automatically. | Medium |

* 1. Gateway certificate expired

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Gateway certificate expired. | There is no connectivity from this ATA Gateway to the ATA Center. No data from that ATA Gateway will be sent. | [Uninstall and reinstall the ATA Gateway](https://docs.microsoft.com/en-us/advanced-threat-analytics/install-ata-step3). | High |

* 1. Domain synchronizer not assigned

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| No domain synchronizer is assigned to any ATA Gateway. This may happen if there is no ATA Gateway configured as domain synchronizer candidate. | When the domain is not synchronized, changes to entities might cause entity information in ATA to become out of date or missing but will not affect any detection. | Make sure that at least one ATA Gateway is set as a [Domain synchronizer](https://docs.microsoft.com/en-us/advanced-threat-analytics/install-ata-step5). | Low |

* 1. All/Some of the capture network adapters on a Gateway are not available

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| All/Some of the selected capture network adapters on the ATA Gateway are disabled or disconnected. | Network traffic for some/all of the domain controllers is no longer captured by the ATA Gateway. This will impact the ability to detect suspicious activities, related to those domain controllers. | Make sure these selected capture network adapters on the ATA Gateway are enabled and connected. | Medium |

* 1. Some domain controllers are unreachable by a Gateway

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| An ATA Gateway has limited functionality due to connectivity issues to some of the configured domain controllers. | Pass the Hash detection might be less accurate when some domain controllers can't be queried by the ATA Gateway. | Make sure the domain controllers are up and running and that this ATA Gateway can open LDAP connections to them. | Medium |

* 1. All domain controllers are unreachable by a Gateway

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Gateway is currently offline due to connectivity issues to all the configured domain controllers. | This will impact ATA’s ability to detect suspicious activities related to domain controllers monitored by this ATA Gateway. | Make sure the domain controllers are up and running and that this ATA Gateway can open LDAP connections to them. | Medium |

* 1. Gateway stopped communicating

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| There has been no communication from the ATA Gateway. The default time span for this alert is 5 minutes. | Network traffic is no longer captured by the network adapter on the ATA Gateway. This will impact ATA’s ability to detect suspicious activities, since network traffic will not be able to reach the ATA Center. | Check that the port used for the communication between the ATA Gateway and ATA Center service is not blocked by any routers or firewalls. | Medium |

* 1. No traffic received from domain controller

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| No traffic was received from the domain controller via this ATA Gateway. | This might indicate that port mirroring from the domain controllers to the ATA Gateway is not configured yet or not working. | Verify that [port mirroring is configured properly on your network devices](https://docs.microsoft.com/en-us/advanced-threat-analytics/configure-port-mirroring). On the ATA Gateway capture NIC, disable these features in Advanced Settings: Receive Segment Coalescing (IPv4) Receive Segment Coalescing (IPv6) | Medium |

* 1. Some forwarded events are not being analyzed

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Gateway is receiving more events than it can process. | Some forwarded events are not being analyzed, which can impact the ability to detect suspicious activities originating from domain controllers being monitored by this ATA Gateway. | Verify that only required events are forwarded to the ATA Gateway or try to forward some of the events to another ATA Gateway. | Medium |

* 1. Some network traffic is not being analyzed

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Gateway is receiving more network traffic than it can process. | Some network traffic is not being analyzed, which can impact the ability to detect suspicious activities originating from domain controllers being monitored by this ATA Gateway. | Consider [adding additional processors and memory](https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-capacity-planning) as required. If this is a standalone ATA Gateway, reduce the number of domain controllers being monitored. This can also happen if you are using domain controllers on VMware virtual machines. To avoid these alerts, you can check that the following settings are set to 0 or Disabled in the virtual machine: - TsoEnable - LargeSendOffload(IPv4) - IPv4 TSO Offload Also, consider disabling IPv4 Giant TSO Offload. For more information consult your VMware documentation. | Medium |

* 1. Gateway version outdated

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Center is newer than the version installed on the ATA Gateway. This is causing the ATA Gateway to stop functioning as expected. | This can impact the ability to detect suspicious activities originating from domain controllers being monitored by this ATA Gateway. | Update the ATA Gateway to the latest version automatically by enabling [automatic update](https://docs.microsoft.com/en-us/advanced-threat-analytics/install-ata-step1) in the ATA Console or by downloading the latest ATA Gateway package available in the ATA Console. | High |

* 1. Gateway service failed to start

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Description** | **Resolution** | **Severity** |
| The ATA Gateway service failed to start for at least 30 minutes. | This can impact the ability to detect suspicious activities originating from domain controllers being monitored by this ATA Gateway. | Monitor ATA Gateway logs to [understand the root cause for ATA Gateway service failure](https://docs.microsoft.com/en-us/advanced-threat-analytics/troubleshooting-ata-using-logs). | High |

1. Like suspicious activities, Health Center alerts can be closed or suppressed and are categorized High, Medium, or Low depending on their severity. If you close 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 close list. [↑](#footnote-ref-2)