Contents

What is Advanced Threat Analytics?

7/20/2020 • 3 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

Advanced Threat Analytics (ATA) is an on-premises platform that helps protect your enterprise from multiple types of advanced targeted cyber attacks and insider threats.

How ATA works

ATA leverages a proprietary network parsing engine to capture and parse network traffic of multiple protocols (such as Kerberos, DNS, RPC, NTLM, and others) for authentication, authorization, and information gathering. This information is collected by ATA via:

- Port mirroring from Domain Controllers and DNS servers to the ATA Gateway and/or
- Deploying an ATA Lightweight Gateway (LGW) directly on Domain Controllers

ATA takes information from multiple data-sources, such as logs and events in your network, to learn the behavior of users and other entities in the organization, and builds a behavioral profile about them. ATA can receive events and logs from:

- SIEM Integration
- Windows Event Forwarding (WEF)
- Directly from the Windows Event Collector (for the Lightweight Gateway)

For more information on ATA architecture, see ATA Architecture.

What does ATA do?

ATA technology detects multiple suspicious activities, focusing on several phases of the cyber-attack kill chain including:

- Reconnaissance, during which attackers gather information on how the environment is built, what the different assets are, and which entities exist. Typically, this is where attackers build plans for their next phases of attack.
- Lateral movement cycle, during which an attacker invests time and effort in spreading their attack surface inside your network.
- Domain dominance (persistence), during which an attacker captures the information that allows them to resume their campaign using various sets of entry points, credentials, and techniques.

These phases of a cyber attack are similar and predictable, no matter what type of company is under attack or what type of information is being targeted. ATA searches for three main types of attacks: Malicious attacks, abnormal behavior, and security issues and risks.

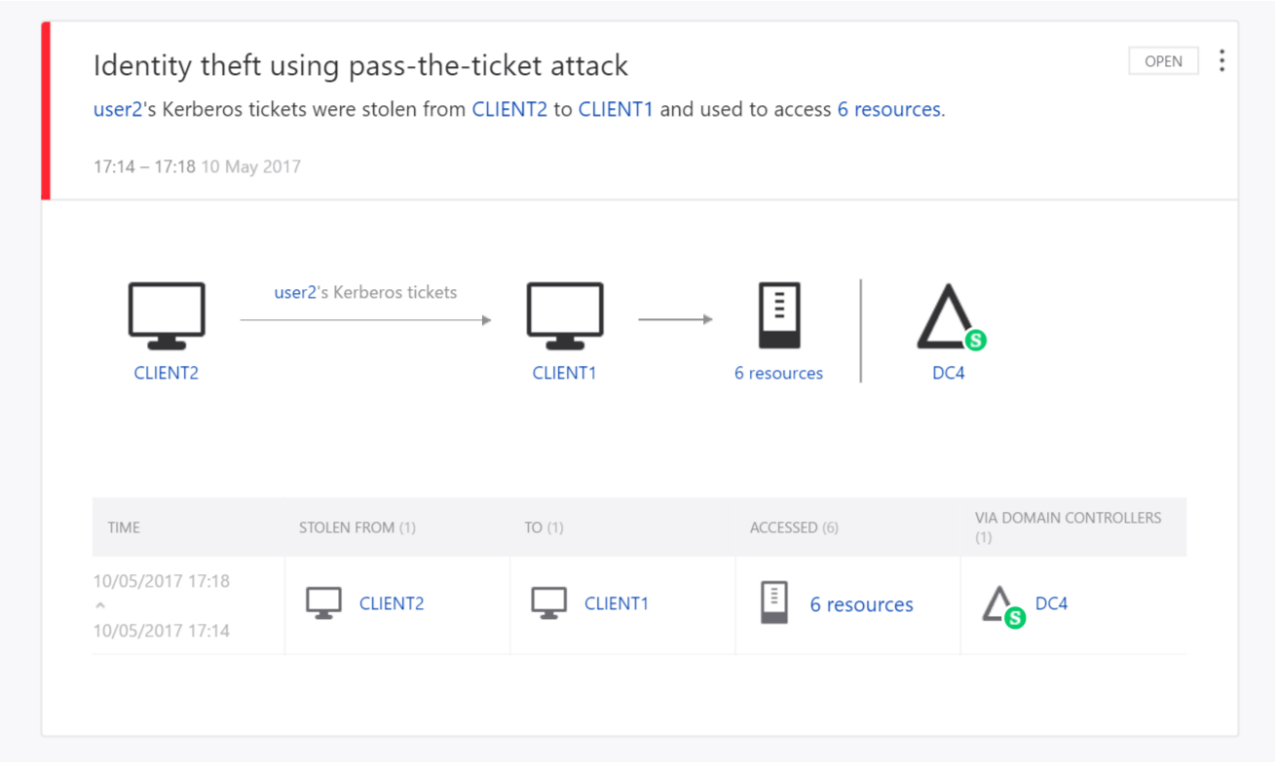
Malicious attacks are detected deterministically, by looking for the full list of known attack types including:

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Malicious replications

- Reconnaissance
- Brute Force
- Remote execution

For a complete list of the detections and their descriptions, see What Suspicious Activities Can ATA detect?.

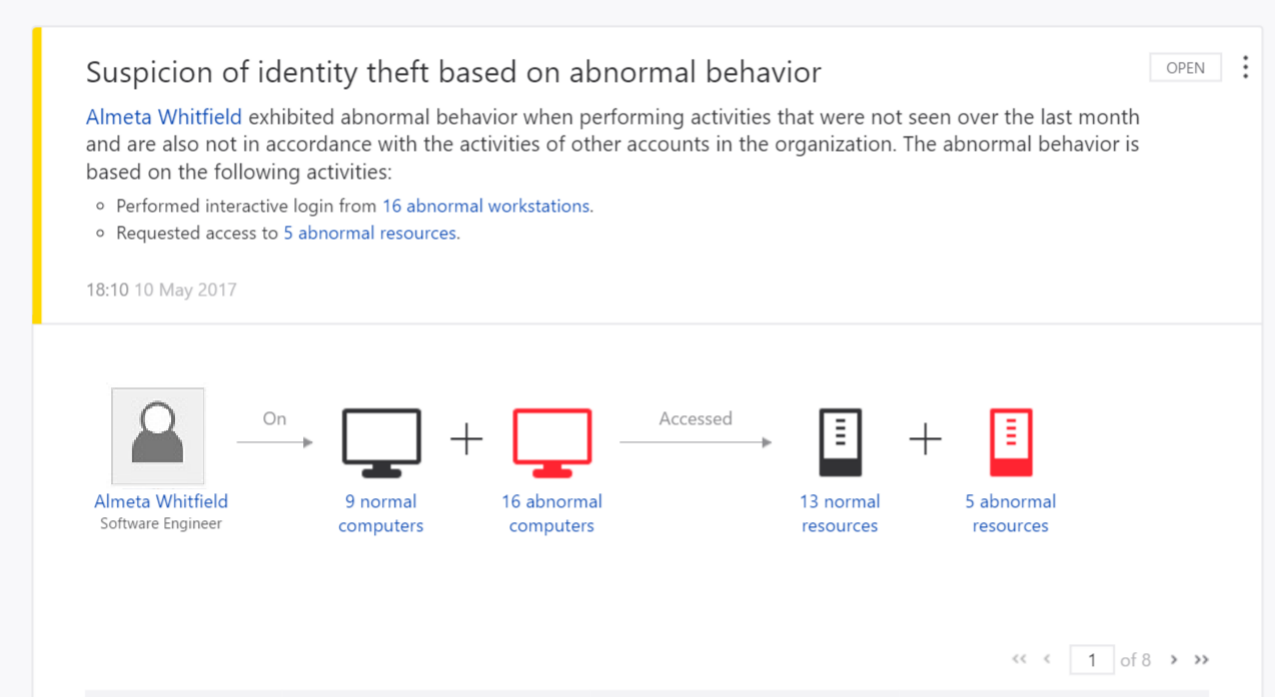
ATA detects these suspicious activities and surfaces the information in the ATA Console including a clear view of Who, What, When and How. As you can see, by monitoring this simple, user-friendly dashboard, you are alerted that ATA suspects a Pass-the-Ticket attack was attempted on Client 1 and Client 2 computers in your network.



Abnormal behavior is detected by ATA using behavioral analytics and leveraging Machine Learning to uncover questionable activities and abnormal behavior in users and devices in your network, including:

- Anomalous logins
- Unknown threats
- Password sharing
- Lateral movement
- Modification of sensitive groups

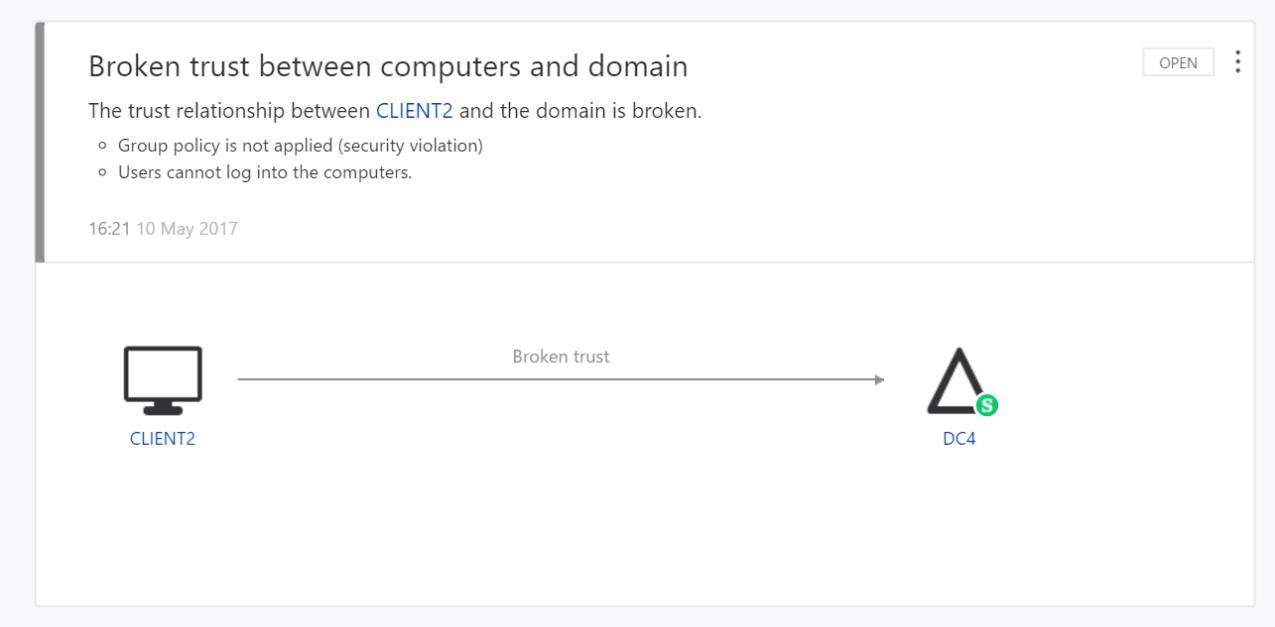
You can view suspicious activities of this type in the ATA Dashboard. In the following example, ATA alerts you when a user accesses four computers that are not ordinarily accessed by this user, which could be a cause for alarm.



ATA also detects **security issues and risks**, including:

- Broken trust
- Weak protocols
- Known protocol vulnerabilities

You can view suspicious activities of this type in the ATA Dashboard. In the following example, ATA is letting you know that there is a broken trust relationship between a computer in your network and the domain.



Known issues

- If you update to ATA 1.7 and immediately to ATA 1.8, without first updating the ATA Gateways, you cannot migrate to ATA 1.8. It is necessary to first update all of the Gateways to version 1.7.1 or 1.7.2 before updating the ATA Center to version 1.8.
- If you select the option to perform a full migration, it may take a very long time, depending on the database size. When you are selecting your migration options, the estimated time is displayed - make note of this before you decide which option to select.

What's next?

- For more information about how ATA fits into your network: ATA architecture
- To get started deploying ATA: Install ATA

Related Videos

- Joining the security community
- ATA Deployment Overview

See Also

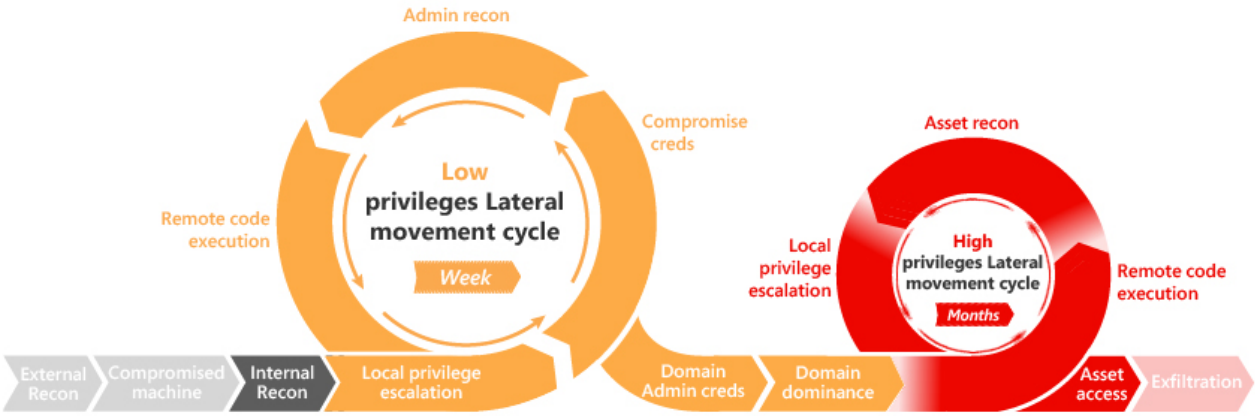
ATA suspicious activity playbook Check out the ATA forum!

What threats does ATA look for?

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

ATA provides detection for the following various phases of an advanced attack: reconnaissance, credential compromise, lateral movement, privilege escalation, domain dominance, and others. These detections are aimed at detecting advanced attacks and insider threats before they cause damage to your organization. The detection of each phase results in several suspicious activities relevant for the phase in question, where each suspicious activity correlates to different flavors of possible attacks. These phases in the kill-chain where ATA currently provides detections are highlighted in the following image:



For more information, see Working with suspicious activities and the ATA suspicious activity guide.

What's next?

- For more information about how ATA fits into your network: ATA architecture
- To get started deploying ATA: Install ATA

See Also

Check out the ATA forum!

What's new in ATA version 1.9

7/20/2020 • 2 minutes to read • Edit Online

The latest update version of ATA can be downloaded from the Download Center or the full version can be downloaded from the Eval center.

These release notes provide information about updates, new features, bug fixes, and known issues in this version of Advanced Threat Analytics.

New & updated detections

- **Suspicious service creation**: Attackers attempt to run a suspicious service on your network. ATA now raises an alert when it identifies that someone runs a new service, that seems suspicious, on a domain controller. This detection is based on events (not network traffic), for more information, see the Suspicious activity guide.

New reports to help you investigate

- The **Passwords exposed in cleartext** enables you to detect when accounts, both sensitive and non-sensitive, send account credentials in plain text. This allows you to investigate and mitigate the use of LDAP simple bind in your environment, improving your network security level. This report replaces the service and sensitive account cleartext suspicious activity alerts.
- The **Lateral movement paths to sensitive accounts** lists the sensitive accounts that are exposed via lateral movement paths. This enables you to mitigate these paths and harden your network to minimize the attack surface risk. This enables you to prevent lateral movement so that attackers can't move across your network between users and computers until they hit the virtual security jackpot: your sensitive admin account credentials.

Improved investigation

- ATA 1.9 includes a new and improved entity profile. The entity profile provides you with a dashboard designed for full deep-dive investigation of users, the resources they accessed, and their history. The entity profile also enables you to identify sensitive users who are accessible via lateral movement paths.
- ATA 1.9 enables you to manually tag groups or accounts as sensitive to enhance detections. This tagging impacts many ATA detections, such as sensitive group modification detection and lateral movement path, rely on which groups and accounts are considered sensitive.

Performance improvements

- The ATA Center infrastructure was improved for performance: the aggregated view of the traffic enables optimization of CPU and packet pipeline, and reuses sockets to the domain controllers to minimize SSL sessions to the DC.

Additional changes

- After a new version of ATA is installed, the **What's new** icon appears in the toolbar to let you know what was changed in the latest version. It also provides you with a link to the in-depth version changelog.

Removed and deprecated features

- The **Broken trust suspicious activity** alert was removed.
- The passwords exposed in clear text suspicious activity was removed. It was replaced by the **Passwords exposed in clear text report**.

See Also

Check out the ATA forum!

Update ATA to version 1.9 - migration guide

ATA version 1.9.2

7/20/2020 • 2 minutes to read • Edit Online

We're happy to announce the availability of Microsoft Advanced Threat Analytics 1.9 Update 2.

This article describes issues fixed in Update 2 of Microsoft Advanced Threat Analytics (ATA) version 1.9. The build number of this update is 1.9.7478.

Improvements included in this update

This update includes Windows Server 2019 (Including Core versions but not Nano) as a supported operating system for both the Center, Gateway and Lightweight gateway components.

This update also includes performance and stability improvements along with fixes for issues reported by customers.

Fixed issues included in this update

- Fixes an issue in which directory data display shows direct manager and recursive memberships.
- Fixes an issue in which the ATA Center URL configuration does not always show local IPs or the local machine name.
- Fixes a health alert download issue when the health alert contains a non-existent gateway.
- Fixes translation issues.
- Fixes an issue in which the MongoDB database version was not updated.
- Fixes a rare scenario in which high memory issues occurred during Active Directory sync.
- Fixes a rare scenario in which the console only allowed selection of an unsupported certificate.
- Fixes a rare scenario in which a false positive instance of the "Suspicion of identity theft based on abnormal behavior" message was received.
- Fixes a rare case in which timeline jumping occurred when alerts were auto-updated.

Get this update

To get the stand-alone package for this update, go to the Microsoft Download Center website: Download the ATA 1.9.2 package now.

Prerequisites

To install this update, you must have one of the following versions of ATA already installed:

- Update 1 for ATA 1.9 (version 1.9.7412)
- ATA 1.9 (version 1.9.7312)
- Update 1 for ATA 1.8 (version 1.8.6765)
- ATA 1.8 (version 1.8.6645)

Restart requirement

Your computer may require a restart after applying this update.

Update replacement information

This update replaces ATA version 1.9.1 (1.9.7412).

See also

- Check out the ATA forum!
- ATA versions

ATA version 1.9.1

7/20/2020 • 2 minutes to read • Edit Online

This article describes issues fixed in Update 1 for Microsoft Advanced Threat Analytics (ATA) version 1.9. The build number of this update is 1.9.7412.

Fixed issues included in this update

- Possibility of migration failures between ATA version 1.8 to version 1.9 for large databases.
- When using the latest version of the Microsoft Edge browser, and switching users, the browser may hang.
- In some scenarios, the user profile page is missing Directory Data Information.
- When adding a user to the exclusion list for abnormal behavior detection, the exclusion isn't always applied.
- Updated MongoDB database version.
- Inconsistent resync after an upgrade to version 1.9 of all Active Directory entities to ATA.
- Inconsistent exports of suspicious activities to Microsoft Excel. Occasional failure with error generation.

Improvements included in this update

- Changes required for Microsoft Accessibility Standards (MAS) certification.
- Includes additional performance and security fixes.

Get this update

Updates for Microsoft Advanced Threat Analytics version 1.9 are available from Microsoft Update or by manual download.

Microsoft Update

This update is available on Microsoft Update. For more information about how to use Microsoft Update, see How to get an update through Windows Update.

Manual download

To get the stand-alone package for this update, go to the Microsoft Download Center website: Download the ATA 1.9 package now.

Prerequisites

To install this update, you must have ATA version 1.9 (1.9.7312), Update 1 for ATA version 1.8 (1.8.6765), or ATA version 1.8 (1.8.6645) installed.

Restart requirement

Your computer may require a restart after you apply this update.

Update replacement information

This update replaces ATA version 1.9 (1.9.7312).

See also

- Check out the ATA forum!
- ATA versions

Updating ATA to version 1.9

7/20/2020 • 2 minutes to read • Edit Online

> **NOTE**
> If ATA is not installed in your environment, download the full version of ATA, which includes version 1.9 and follow the standard installation procedure described in Install ATA.

If you already have ATA version 1.8 deployed, this procedure walks you through the steps necessary to update your deployment.

> **NOTE**
> Only ATA version 1.8 (1.8.6645) and ATA 1.8 update 1 (1.8.6765) can be updated to ATA version 1.9, any earlier version of ATA can't be directly updated to ATA version 1.9.

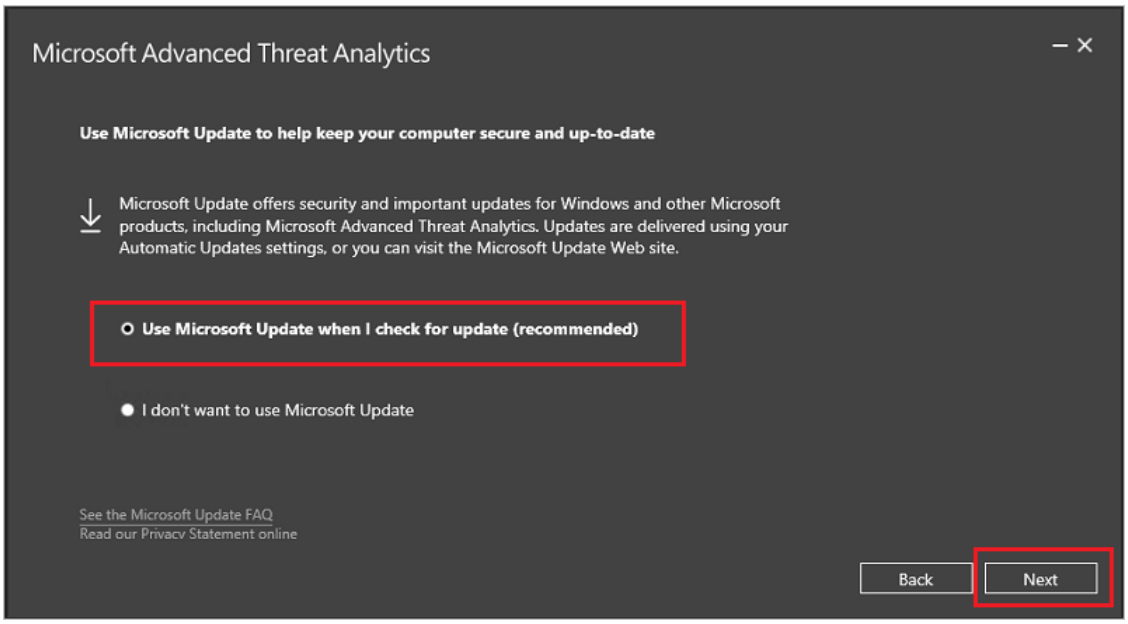
Follow these steps to update to ATA version 1.9:

1. Download the update version of ATA 1.9 from the Download Center or the full version from the Eval center. In the migration version, the file can be used only for updating from ATA 1.8. In the version from the Eval center, the same installation file (Microsoft ATA Center Setup.exe) is used for installing a new deployment of ATA and for upgrading existing deployments.
2. Update the ATA Center
3. Update the ATA Gateways

   > **IMPORTANT**
   > Update all the ATA Gateways to make sure ATA functions properly.

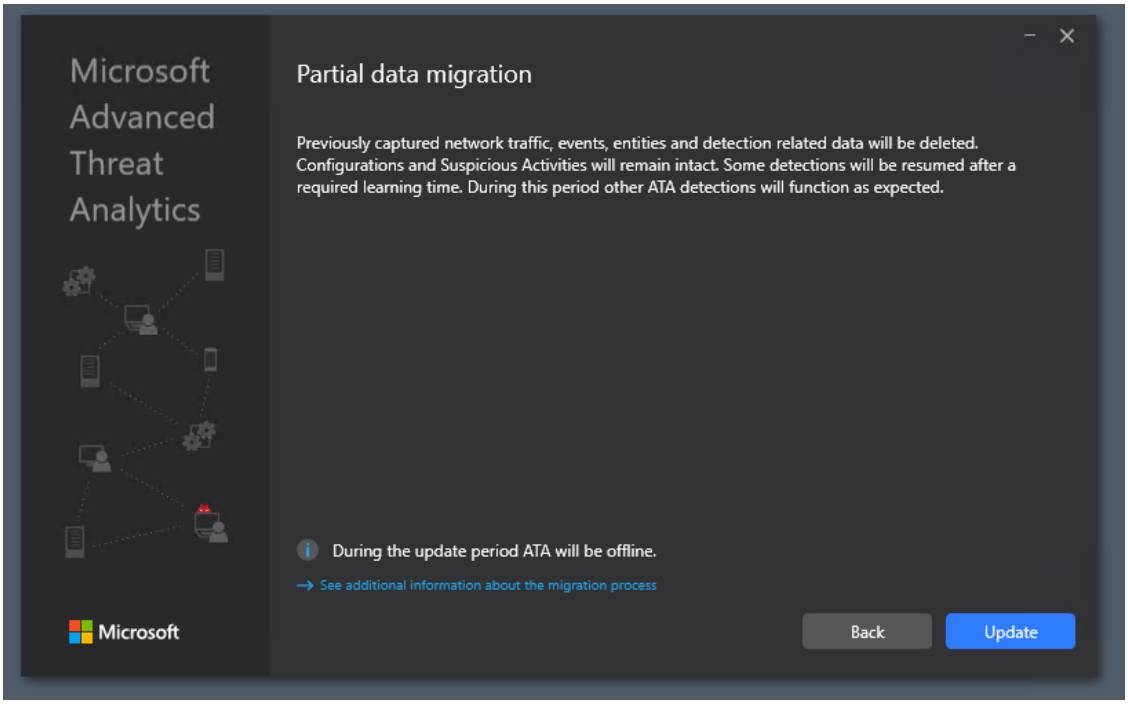
Step 1: Update the ATA Center

1. Back up your database: (optional)
   - If the ATA Center is running as a virtual machine and you want to take a checkpoint, shut down the virtual machine first.
   - If the ATA Center is running on a physical server, see the Disaster recovery article for information about backing up the database.
2. Run the installation file, **Microsoft ATA Center Setup.exe**, and follow the instructions on the screen to install the update.
   - On the **Welcome** page, choose your language and click **Next**.
   - If you didn't enable automatic updates in version 1.8, you are prompted to set ATA to use Microsoft Update for ATA to remain up-to-date. In the Microsoft Update page, select **Use Microsoft Update when I check for updates (recommended)**.



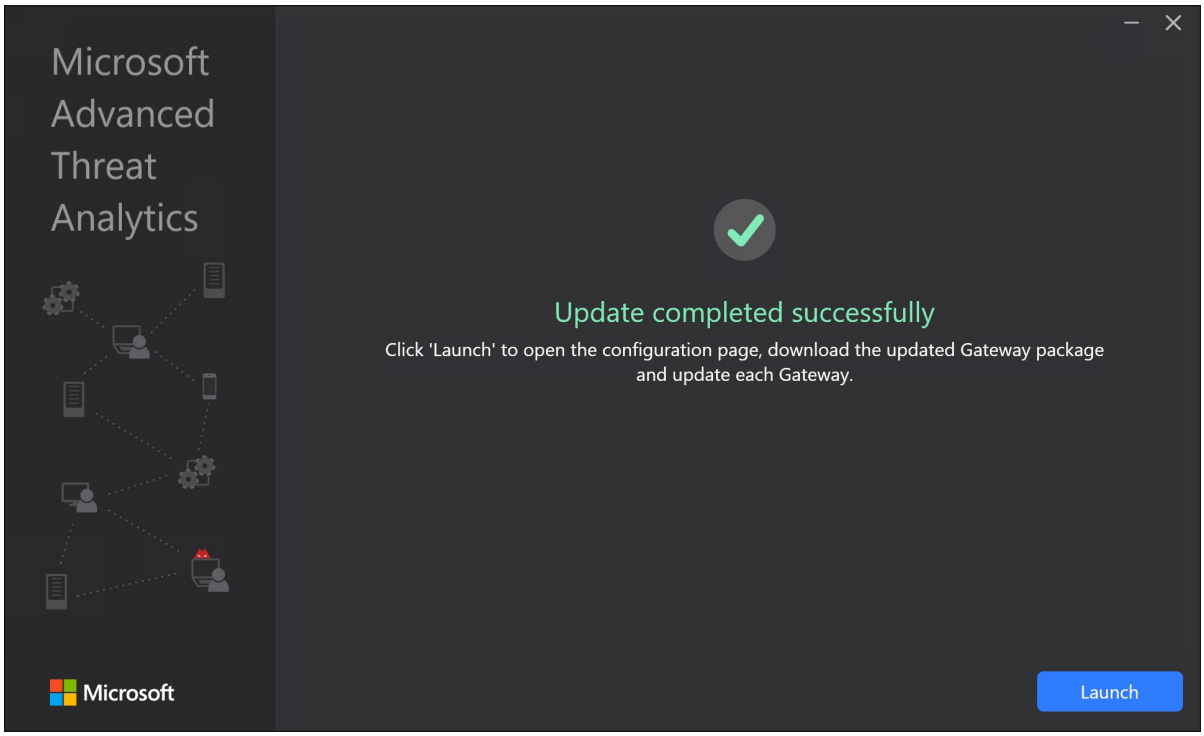
This adjusts the Windows settings to enable updates for ATA.

- The **Partial data migration** screen lets you know that previously captured network traffic, events, entities and detection related data is deleted. All detections work immediately with the exception of abnormal behavior detection, abnormal group modification, Reconnaissance using Directory Services (SAM-R), and encryption downgrade detections which take up to three weeks to build a complete profile after the required learning time.

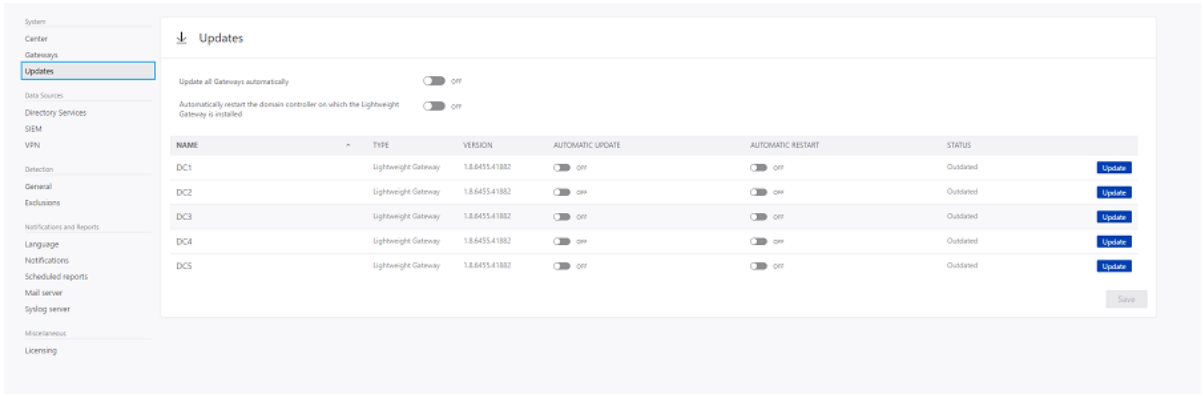


- Click **Update**. After you click Update, ATA is offline until the update procedure is complete.

3. After the ATA Center update completes successfully, click **Launch** to open the **Update** screen in the ATA console for the ATA Gateways.



4. In the **Updates** screen, if you already set your ATA Gateways to automatically update, they update at this point, if not, click **Update** next to each ATA Gateway.



> **IMPORTANT**
>
> Update all the ATA Gateways to make sure ATA functions properly.

> **NOTE**
>
> To install new ATA Gateways, go the **Gateways** screen and click **Download Gateway Setup** to get the ATA 1.9 Gateway installation package and follow the instructions for new Gateway installation as described in Step 4. Install the ATA Gateway.

See Also

- Check out the ATA forum!

What's new in ATA version 1.8

7/20/2020 • 6 minutes to read • Edit Online

The latest update version of ATA can be downloaded from the Download Center or the full version can be downloaded from the Eval center.

These release notes provide information about updates, new features, bug fixes and known issues in this version of Advanced Threat Analytics.

New & updated detections

- Unusual protocol implementation was improved to be able to detect WannaCry malware.
- NEW! **Abnormal modification of sensitive groups** – As part of the privilege escalation phase, attackers modify groups with high privileges to gain access to sensitive resources. ATA now detects when there's an abnormal change in an elevated group.
- NEW! **Suspicious authentication failures** (Behavioral brute force) – Attackers attempt to use brute force on credentials to compromise accounts. ATA now raises an alert when abnormal failed authentication behavior is detected.
- **Remote execution attempt – WMI exec** - Attackers can attempt to control your network by running code remotely on your domain controller. ATA has enhanced the remote execution detection to include detection of WMI methods to run code remotely.
- Reconnaissance using directory service queries – This detection was enhanced to be able to catch queries against a single sensitive entity and to reduce the number of false positives that were generated in the previous version. If you disabled this in version 1.7, installing version 1.8 will now automatically enable it.
- Kerberos Golden Ticket activity – ATA 1.8 includes an additional technique to detect golden ticket attacks.
    - ATA now detects suspicious activities in which the Golden ticket lifetime has expired. If a Kerberos ticket is used for more than the allowed lifetime, ATA will detect it as a suspicious activity that a Golden ticket has likely been created.
- Enhancements were made to the following detections to remove known false positives:
    - Privilege escalation detection (forged PAC)
    - Encryption downgrade activity (Skeleton Key)
    - Unusual protocol implementation
    - Broken trust

Improved triage of suspicious activities

- NEW! ATA 1.8 enables you to run the following actions suspicious activities during the triage process:
    - **Exclude entities** from raising future suspicious activities to prevent ATA from alerting when it detects benign true positives (such as an admin running remote code or detecting security scanners).
    - **Suppress recurring** suspicious activities from alerting.
    - **Delete suspicious activities** from the attack time line.
- The process for following up on suspicious activity alerts is now more efficient. The suspicious activities time line was redesigned. In ATA 1.8, you will be able to see many more suspicious activities on a single screen, containing better information for triage and investigation purposes.

New reports to help you investigate

- NEW! The **Summary report** was added to enable you to see all the summarized data from ATA, including suspicious activities, health issues and more. You can even define a customized report that is automatically generated on a recurring basis.
- NEW! The **Sensitive groups report** was added to enable you to see all the changes made in sensitive groups over a certain period.

Infrastructure improvements

- ATA Center performance was enhanced. In ATA 1.8 the ATA Center can handle more than 1M packets per second.
- The ATA Lightweight Gateway can now read events locally, without the need to configure event forwarding.
- You can now separately configure email for health alerts and suspicious activities.

Security improvements

- NEW! **Single-sign-on for ATA management**. 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. Silent installation scripts for the ATA Gateway and ATA Lightweight Gateway now use the logged on user's context, without the need to provide credentials.
- Local System privileges were removed from the ATA Gateway process, so you can now use virtual accounts (available on stand-alone ATA Gateways only), managed service accounts and group managed service accounts to run the ATA Gateway process.
- Auditing logs for ATA Center and Gateways were added and all actions are now logged in the Windows Event Log.
- Support was added for KSP Certificates for the ATA Center.

Additional changes

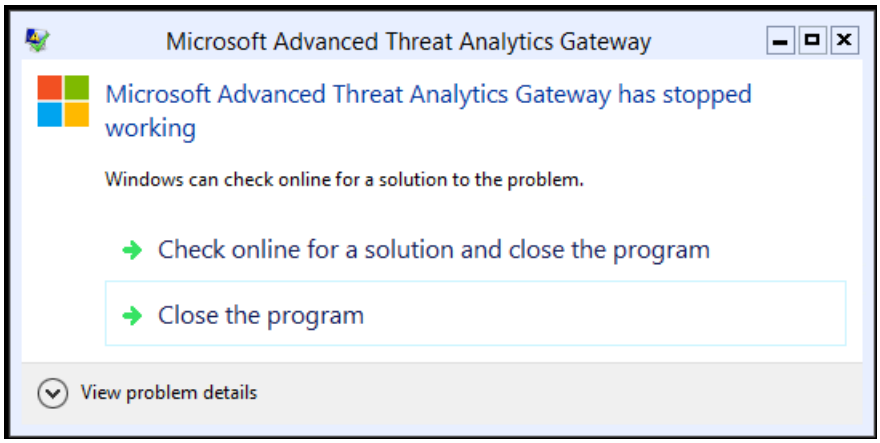
- The option to add notes was removed from Suspicious Activities
- Recommendations for mitigating Suspicious Activities were removed from the Suspicious Activities time line.
- Starting with ATA version 1.8 the ATA Gateways and Lightweight Gateways are managing their own certificates and need no administrator interaction to manage them.

Known issues

> **WARNING**
> In order to avoid these known issues please update or deploy using the 1.8 update 1.

ATA Gateway on Windows Server Core

Symptoms: Upgrading an ATA Gateway to 1.8 on Windows Server 2012R2 Core with .Net framework 4.7 may fail with the error: *Microsoft Advanced Threat Analytics Gateway has stopped working*.



On Windows Server 2016 Core you may not see the error, but the process will fail when you try to install, and events 1000 and 1001 (process crash) will be logged in the application Event Log on the server.

Description: There is a problem with the .NET framework 4.7 that causes applications that uses WPF technology (such as ATA) to fail to load. See KB 4034015 for more information.

Workaround: Uninstall .Net 4.7 See KB 3186497 to revert the .NET version to .NET 4.6.2 and then update your ATA Gateway to version 1.8. After the upgrade of ATA you can reinstall .NET 4.7. There will be an update to correct this problem in a future release.

Lightweight Gateway event log permissions

Symptoms: When you upgrade ATA to version 1.8, apps or services that were previously granted permissions to access the Security Event Log may lose the permissions.

Description: In order to make ATA easier to deploy, ATA 1.8 accesses your Security Event Log directly, without necessitating Windows Event Forwarding configuration. At the same time, ATA runs as a low-permission local service to maintain tighter security. In order to provide access for ATA to read the events, the ATA service grants itself permissions to the Security Event Log. When this happens, permissions previously set for other services may be disabled.

Workaround: Run the following Windows PowerShell script. This removes the incorrectly added permissions in the registry from ATA, and adds them via a different API. This may restore permissions for other apps. If it does not, they will need to be restored manually. There will be an update to correct this problem in a future release.

```
   $ATADaclEntry = "(A;;0x1;;;S-1-5-80-1717699148-1527177629-2874996750-2971184233-2178472682)"
    try {
  $SecurityDescriptor = Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\Eventlog\Security -Name
CustomSD
  $ATASddl = "O:BAG:SYD:" + $ATADaclEntry
  if($SecurityDescriptor.CustomSD -eq $ATASddl) {
Remove-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\Eventlog\Security -Name CustomSD
  }
}
catch
{
# registry key does not exist
}

$EventLogConfiguration = New-Object -TypeName
System.Diagnostics.Eventing.Reader.EventLogConfiguration("Security")
$EventLogConfiguration.SecurityDescriptor = $EventLogConfiguration.SecurityDescriptor + $ATADaclEntry
```

Proxy interference

Symptoms: After upgrading to ATA 1.8 the ATA Gateway service may fail to start. In the ATA error log you may see the following exception: *System.Net.Http.HttpRequestException: An error occurred while sending the request. --->*

System.Net.WebException: The remote server returned an error: (407) Proxy Authentication Required.

Description: Starting from ATA 1.8, the ATA Gateway communicates with the ATA Center using the http protocol. If the machine on which you installed the ATA Gateway uses a proxy server to connect to the ATA Center, it can break this communication.

Workaround: Disable the use of a proxy server on the ATA Gateway service account. There will be an update to correct this problem in a future release.

Report settings reset

Symptoms: Any settings that were made to the scheduled reports are cleared when you update to 1.8 update 1.

Description: Updating to 1.8 update 1 from 1.8 resets the reports schedule settings.

Workaround: Before updating to 1.8 update 1, make a copy of the report settings and reenter them, this can also be done via a script, for more information, see Export and Import the ATA Configuration.

See Also

Check out the ATA forum!

Update ATA to version 1.8 - migration guide

Updating ATA to version 1.8

7/20/2020 • 2 minutes to read • Edit Online

> **NOTE**
> If ATA is not installed in your environment, download the full version of ATA, which includes version 1.8 and follow the standard installation procedure described in Install ATA.

If you already have ATA version 1.7 deployed, this procedure walks you through the steps necessary to update your deployment.

> **NOTE**
> Only ATA version 1.7 Update 1 and 1.7 Update 2 can be updated to ATA version 1.8, any earlier version of ATA can't be directly updated to ATA version 1.8.

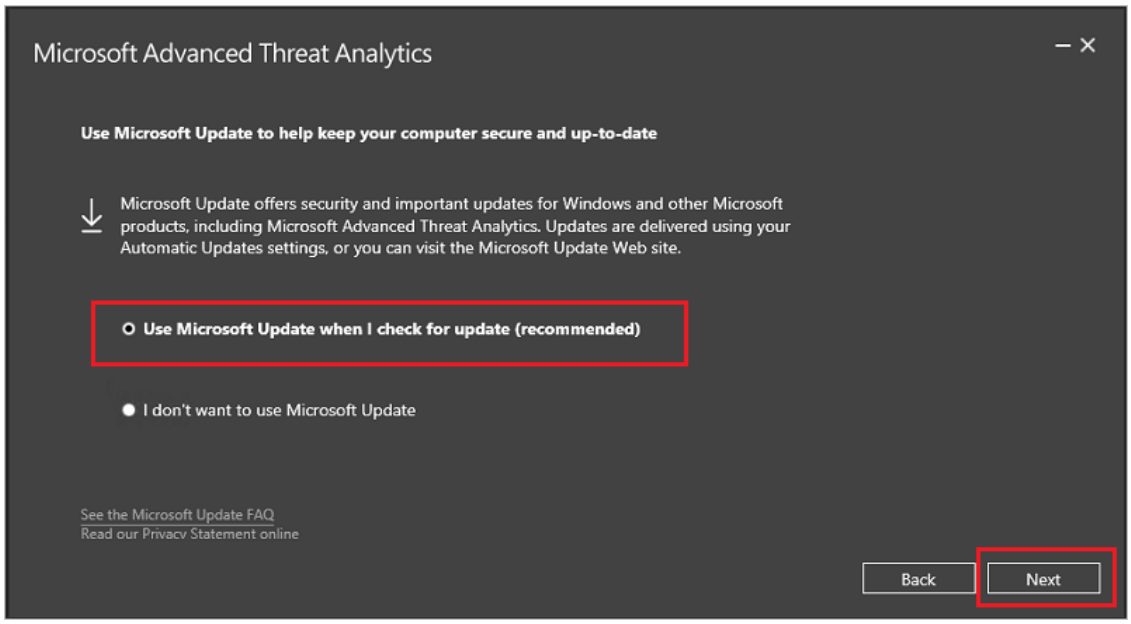
Follow these steps to update to ATA version 1.8:

1. Download the update version of ATA 1.8 from the Download Center or the full version from the Eval center. In the migration version, the file can be used only for updating from ATA 1.7. In the version from the Eval center, the same installation file (Microsoft ATA Center Setup.exe) is used for installing a new deployment of ATA and for upgrading existing deployments.
2. Update the ATA Center
3. Update the ATA Gateways

> **IMPORTANT**
> Update all the ATA Gateways to make sure ATA functions properly.

Step 1: Update the ATA Center

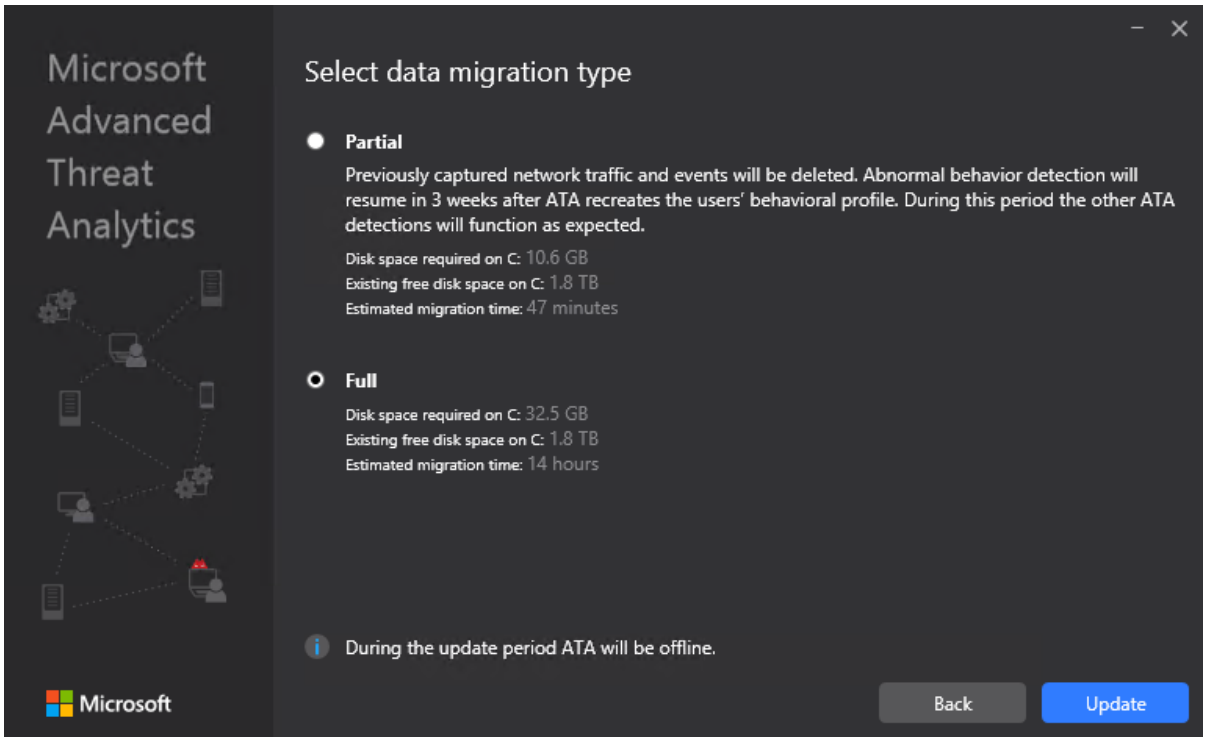
1. Back up your database: (optional)
   - If the ATA Center is running as a virtual machine and you want to take a checkpoint, shut down the virtual machine first.
   - If the ATA Center is running on a physical server, see the Disaster recovery article for information about backing up the database.
2. Run the installation file, **Microsoft ATA Center Setup.exe**, and follow the instructions on the screen to install the update.
   - On the **Welcome** page, choose your language and click **Next**.
   - If you didn't enable automatic updates in version 1.7, you are prompted to set ATA to use Microsoft Update for ATA to remain up-to-date. In the Microsoft Update page, select **Use Microsoft Update when I check for updates (recommended)**.



This adjusts the Windows settings to enable updates for ATA.

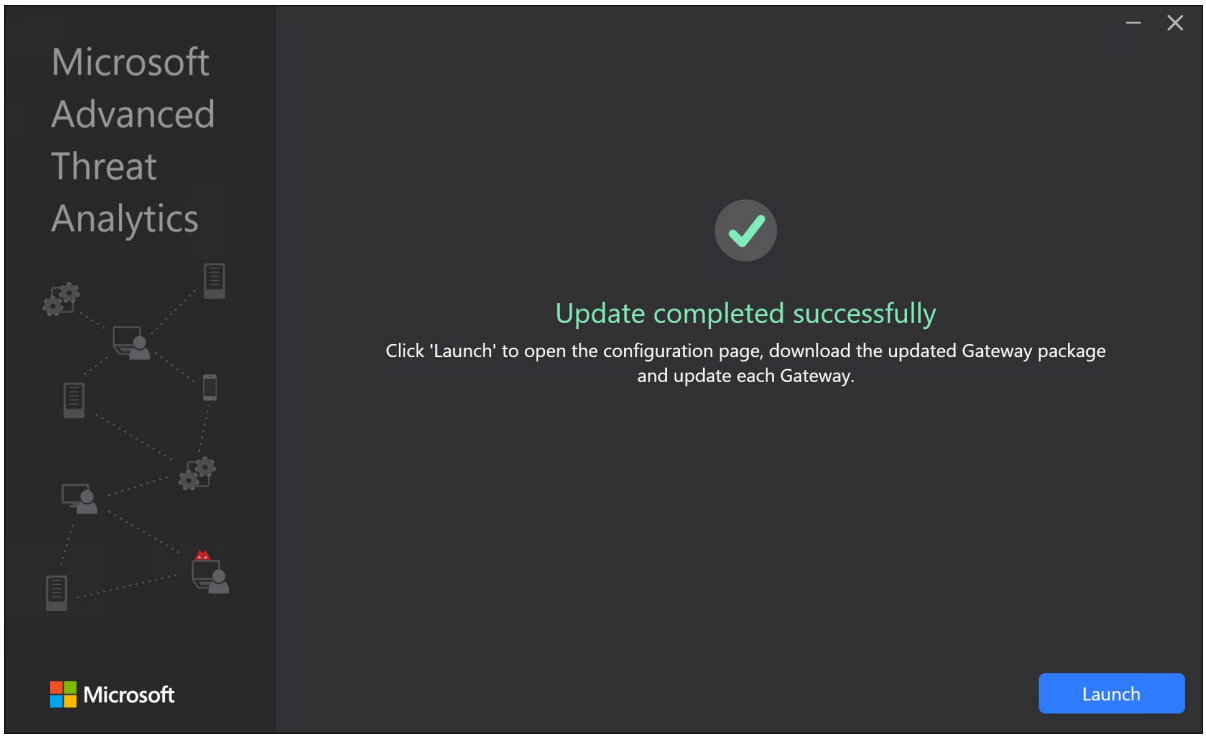
- In the **Data migration** screen, select whether you want to migrate all or partial data. If you choose to migrate only partial data, all detections work immediately with the exception of abnormal behavior detection, which takes three weeks to build a complete profile.

Partial data migration takes much less time to install. If you select **Full** data migration, it may take a significant amount of time for the installation to complete. Make sure you look at the estimated amount of time and the required disk space, which are listed on the **Data Migration** screen. These figures depend on the amount of previously captured network traffic you had saved in previous versions of ATA. For example, in the screen below you can see a data migration from a large database:

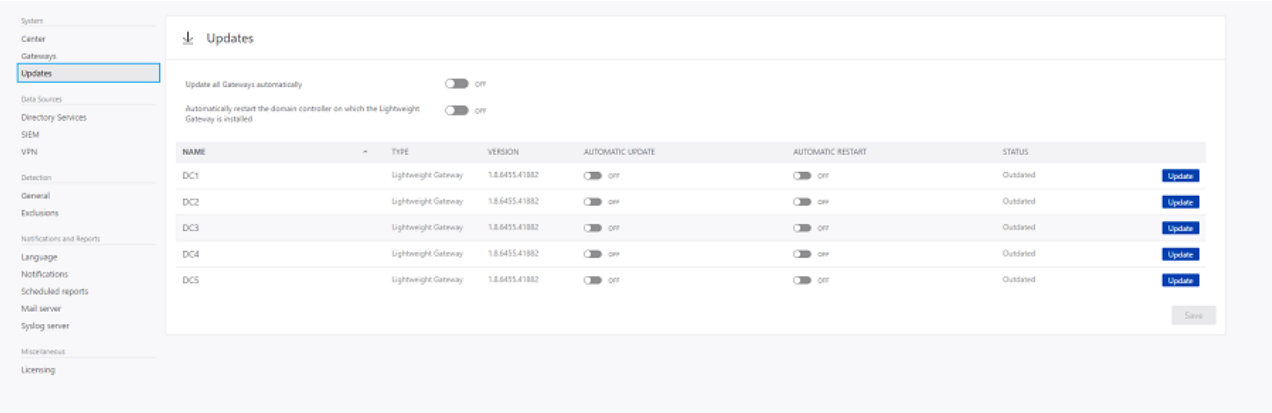


- Click **Update**. After you click Update, ATA is offline until the update procedure is complete.

3. After the ATA Center update completes successfully, click **Launch** to open the **Update** screen in the ATA console for the ATA Gateways.



4. In the **Updates** screen, if you already set your ATA Gateways to automatically update, they update at this point, if not, click **Update** next to each ATA Gateway.



IMPORTANT

Update all the ATA Gateways to make sure ATA functions properly.

NOTE

To install new ATA Gateways, go the **Gateways** screen and click **Download Gateway Setup** to get the ATA 1.8 Gateway installation package and follow the instructions for new Gateway installation as described in Step 4. Install the ATA Gateway.

See Also

- Check out the ATA forum!

What's new in ATA version 1.7

7/20/2020 • 4 minutes to read • Edit Online

These release notes provide information about known issues in this version of Advanced Threat Analytics.

What's new in the ATA 1.7 update?

The update to ATA 1.7 provides improvements in the following areas:

- New & updated detections
- Role-based access control
- Support for Windows Server 2016 and Windows Server 2016 Core
- User experience improvements
- Minor changes

New & updated detections

- **Reconnaissance using Directory Services Enumeration** As part of the reconnaissance phase, attackers gather information about the entities in the network using different methods. Directory services enumeration using the SAM-R protocol enables attackers to obtain the list of users and groups in a domain and understand the interaction between the different entities.
- **Pass-the-Hash Enhancements** To enhance Pass-the-Hash detection, we added additional behavioral models for the authentication patterns of entities. These models enable ATA to correlate entity behavior with suspicious NTLM authentications, and differentiate real Pass-the-Hash attacks from the behavior of false positive scenarios.
- **Pass-the-Ticket Enhancements** To successfully detect advanced attacks in general and Pass-the-Ticket in particular, the correlation between an IP address and the computer account must be accurate. This is a challenge in environments where IP addresses change rapidly by design (for example Wi-Fi networks and multiple virtual machines sharing the same host). To overcome this challenge and improve the accuracy of the Pass-the-Ticket detection, ATA's Network Name Resolution (NNR) mechanism was improved significantly to reduce false-positives.
- **Abnormal Behavior Enhancements** In ATA 1.7, NTLM authentication data was added as a data source for the abnormal behavior detections, providing the algorithms with broader coverage of entity behavior in the network.
- **Unusual Protocol Implementation Enhancements** ATA now detects unusual protocol implementation in the Kerberos protocol, along with additional anomalies in the NTLM protocol. Specifically, these new anomalies for Kerberos are commonly used in Over-pass-the-Hash attacks.

Infrastructure

- **Role based access control** Role-Based Access Control (RBAC) capability. ATA 1.7 includes three roles: ATA Administrator, ATA Analyst and ATA Executive.
- **Support for Windows Server 2016 and Windows Server Core** ATA 1.7 supports the deployment of Lightweight Gateways on domain controllers running Windows Server 2008 R2 SP1 (not including Server Core), Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 (including Core but not Nano). Additionally, this release supports Windows Server 2016 both for the ATA Center and ATA Gateway

components.

User Experience

- **Configuration Experience** In this release, the ATA configuration experience was redesigned for a better user experience and to better support of environments with multiple ATA Gateways. This release also introduces the ATA Gateway update page for simpler, better management of automatic updates for the various Gateways.

Known issues

The following known issues exist in this version.

Gateway automatic update may fail

Symptoms: In environments with slow WAN links, the ATA Gateway update may reach the timeout for the update (100 seconds) and fail to complete successfully. In the ATA Console, the ATA Gateway will have the status of "Updating (downloading package)" for a long amount of time and it eventually fails. **Workaround:** To work around this issue, download the latest ATA Gateway package from the ATA Console, and update the ATA Gateway manually.

> **IMPORTANT**
> Automatic certificate renewal for the certificates used by ATA is not supported. The use of these certificates may cause ATA to stop functioning when the certificate is automatically renewed.

No browser support for JIS encoding

Symptoms: The ATA Console may not function as expected on browsers using JIS encoding **Workaround:** Change the browser's encoding to Unicode UTF-8.

Dropped port mirror traffic when using VMware

Dropped port mirror traffic alerts when using lightweight gateway on VMware.

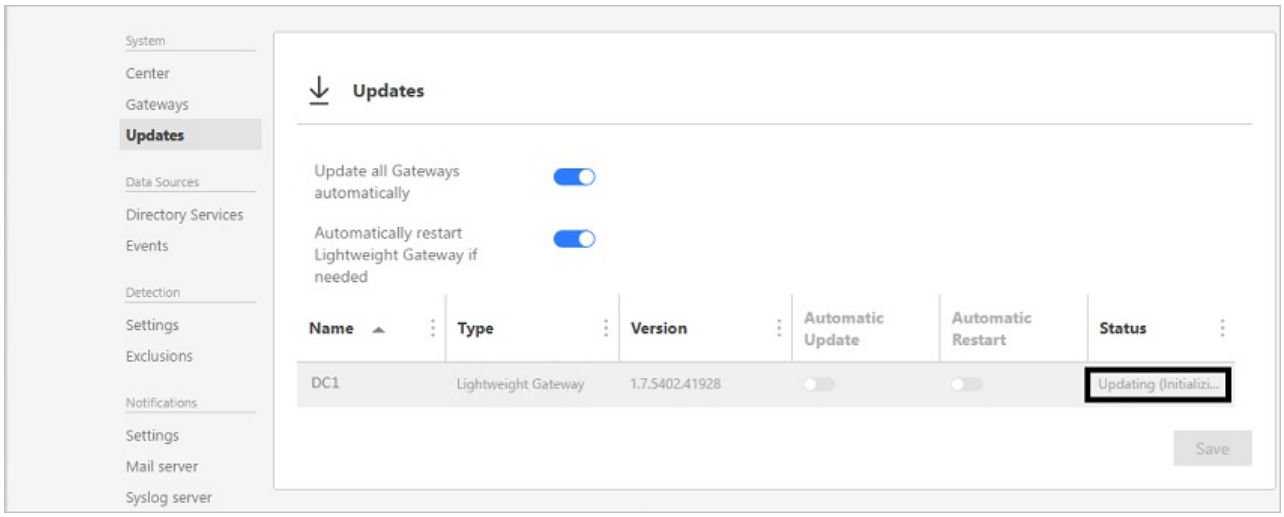
If you are using domain controllers on VMware virtual machines, you might receive alerts about **Dropped port mirrored network traffic**. This might happens because of a configuration mismatch in VMware. To avoid these alerts, you can check that the following settings are set to 0 or Disabled in the virtual machine:

- TsoEnable
- LargeSendOffload(IPv4)
- IPv4 TSO Offload

Also, consider disabling IPv4 Giant TSO Offload. For more information consult your VMware documentation.

Automatic Gateway update fail when updating to 1.7 update 1

When updating from ATA 1.7 to ATA 1.7 update 1, both the automatic ATA Gateway update process and the manual installation of Gateways using the Gateway package may not work as expected. This issue will occur if the certificate used by the ATA Center was changed prior to updating ATA. To verify this issue, review the **Microsoft.Tri.Gateway.Updater.log** on the ATA Gateway and look for the following exceptions: **System.Net.Http.HttpRequestException: An error occurred while sending the request. ---> System.Net.WebException: The underlying connection was closed: An unexpected error occurred on a send. ---> System.IdentityModel.Tokens.SecurityTokenValidationException: Failed to validate certificate thumbprint**



In order to resolve this issue, after changing the certificate, from an elevated command prompt, browse to the following location: **%ProgramFiles%\Microsoft Advanced Threat Analytics\Center\MongoDB\bin** and run the following:

1. Mongo.exe ATA (ATA must be capitalized)
2. CenterThumbprint=db.SystemProfile.find({_t:"CenterSystemProfile"}).toArray()[0].Configuration.SecretManagerConfiguration.CertificateThumbprint;
3. db.SystemProfile.update({_t:"ServiceSystemProfile"},{$set:{"Configuration.ManagementClientConfiguration.ServerCertificateThumbprint":CenterThumbprint}}, {multi: true})

Export suspicious activity details to Excel may fail

When trying to export suspicious activity details to an Excel file, the operation may fail with the following error: *Error [BsonClassMapSerializer`1] System.FormatException: An error occurred while deserializing the Activity property of class Microsoft.Tri.Common.Data.NetworkActivities.SuspiciousActivityActivity: Element 'ResourceIdentifier' does not match any field or property of class Microsoft.Tri.Common.Data.EventActivities.NtlmEvent. ---> System.FormatException: Element 'ResourceIdentifier' does not match any field or property of class Microsoft.Tri.Common.Data.EventActivities.NtlmEvent.*

To resolve this issue, from an elevated command prompt, browse to the following location: **%ProgramFiles%\Microsoft Advanced Threat Analytics\Center\MongoDB\bin** and run the following commands:

1. `Mongo.exe ATA` (ATA must be capitalized)
2. `db.SuspiciousActivityActivity.update({ "Activity._t": "NtlmEvent" },{$unset: {"Activity.ResourceIdentifier": ""}}, {multi: true});`

Minor changes

- ATA is now using OWIN instead of IIS for the ATA Console.
- If the ATA Center service is down, you cannot access the ATA Console.
- Short-term Lease subnets are no longer necessary due to changes in the ATA NNR.

See Also

Check out the ATA forum!

Update ATA to version 1.7 - migration guide

ATA update to 1.7 migration guide

7/20/2020 • 2 minutes to read • Edit Online

The update to ATA 1.7 provides improvements in the following areas:

- New detections
- Improvements to existing detections

Updating ATA to version 1.7

> **NOTE**
> If ATA is not installed in your environment, download the full version of ATA, which includes version 1.7 and follow the standard installation procedure described in Install ATA.

If you already have ATA version 1.6 deployed, this procedure walks you through the steps necessary to update your deployment.

> **NOTE**
> You cannot install ATA version 1.7 directly on top of ATA version 1.4 or 1.5. You must install ATA version 1.6 first.

Follow these steps to update to ATA version 1.7:

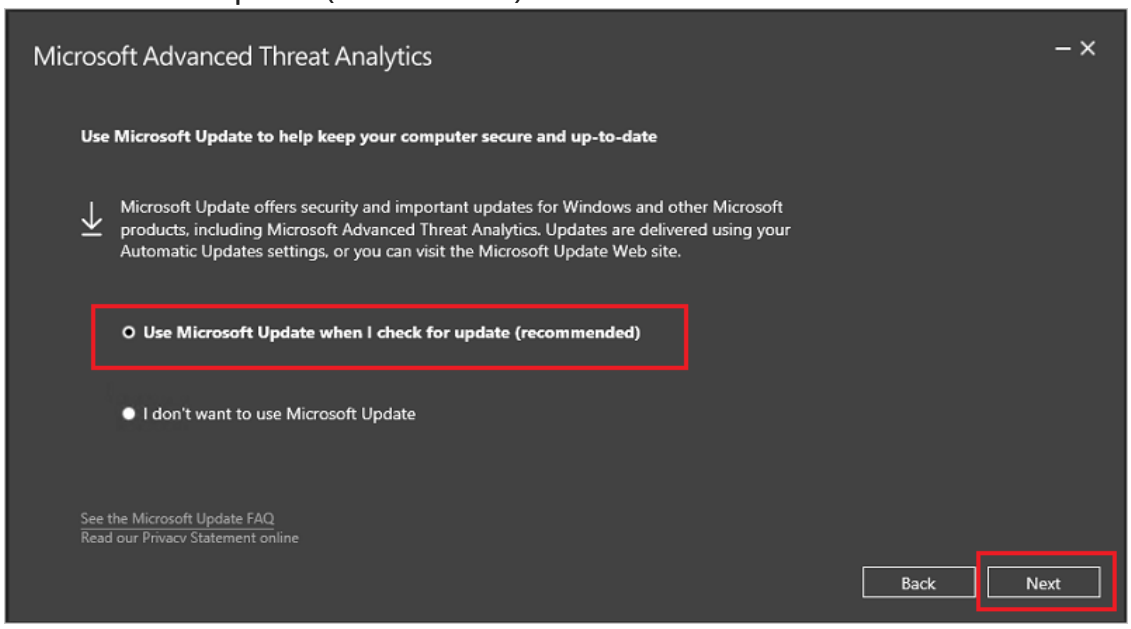
1. Download update 1.7
   In this version of, the same installation file (Microsoft ATA Center Setup.exe) is used for installing a new deployment of ATA and for upgrading existing deployments.
2. Update the ATA Center
3. Update the ATA Gateways

   > **IMPORTANT**
   > Update all the ATA Gateways to make sure ATA functions properly.

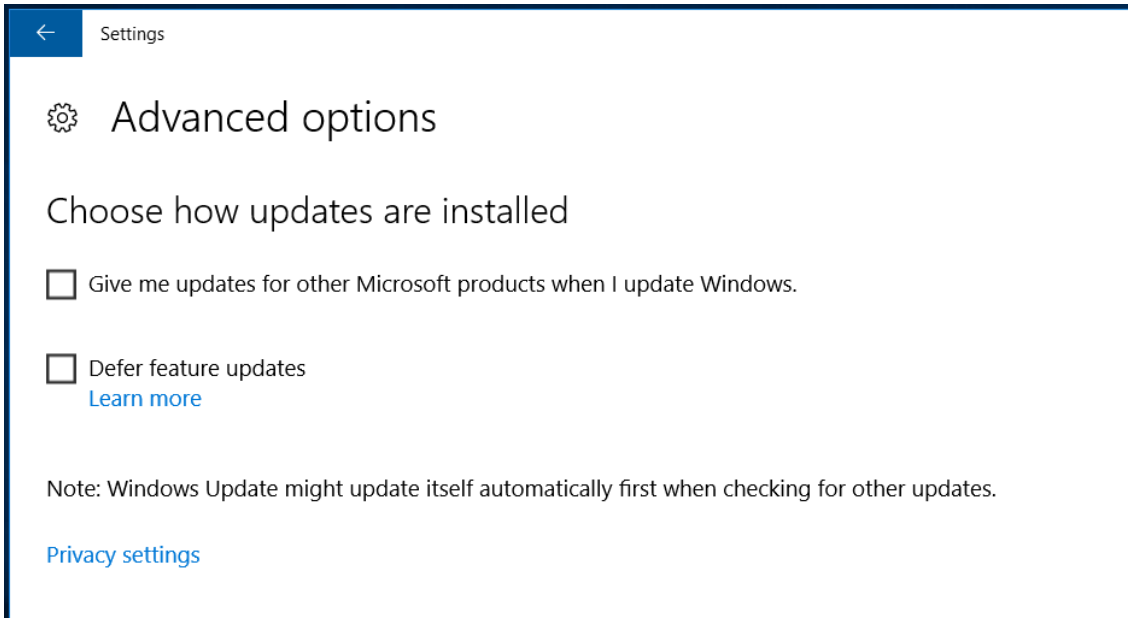
Step 1: Update the ATA Center

1. Back up your database: (optional)
   - If the ATA Center is running as a virtual machine and you want to take a checkpoint, shut down the virtual machine first.
   - If the ATA Center is running on a physical server, follow the recommended procedure to back up MongoDB.
2. Run the installation file, **Microsoft ATA Center Setup.exe**, and follow the instructions on the screen to install the update.
   - On the **Welcome** page, select your language and click **Next**.
   - If you didn't enable automatic updates in version 1.6, you are prompted to set ATA to use Microsoft

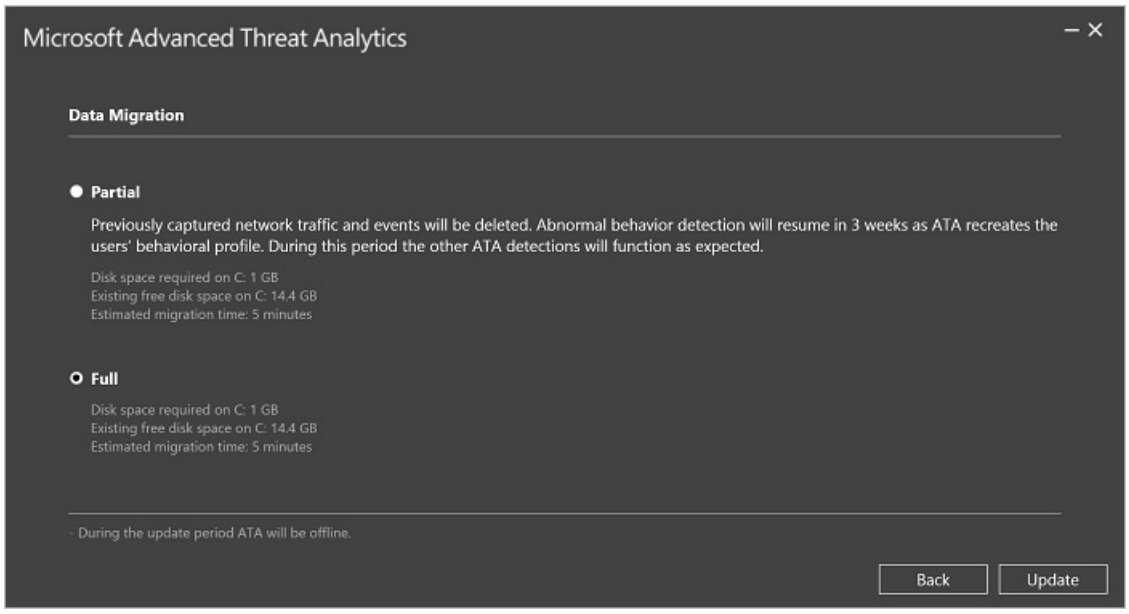
Update for ATA to remain up-to-date. In the Microsoft Update page, select **Use Microsoft Update when I check for updates (recommended)**.



This adjusts the Windows settings to enable updates for other Microsoft products (including ATA), as seen here.

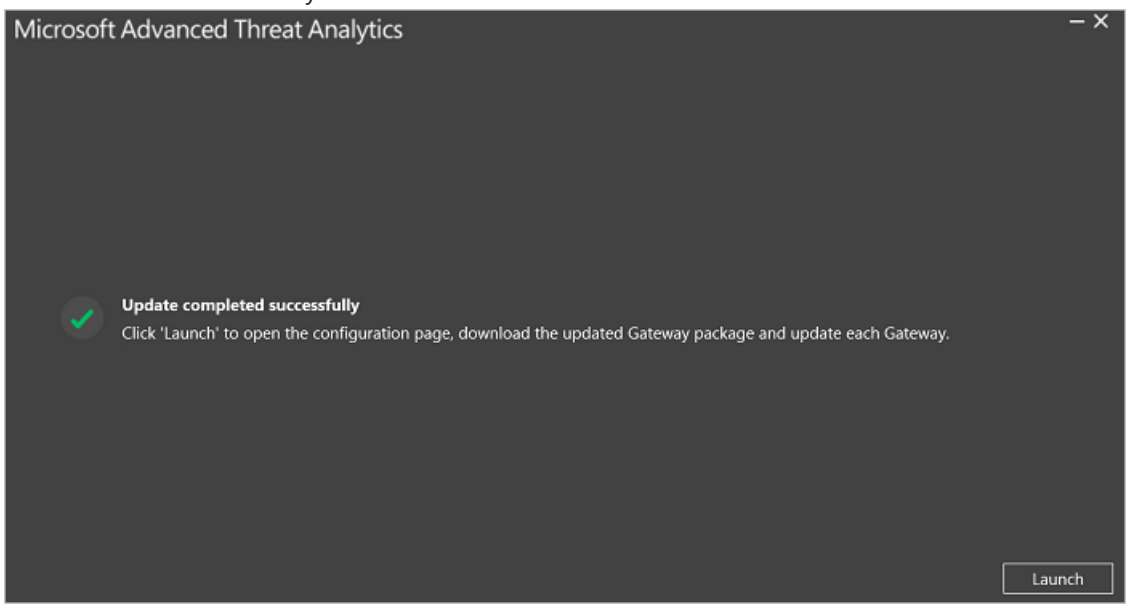


- In the **Data migration** screen, select whether you want to migrate all or partial data. If you choose to migrate only partial data, your previously captured network traffic and behavior profiles will not be migrated. This means that it takes three weeks before the abnormal behavior detection has a complete profile to enable anomalous activity detection. During those three weeks, all other ATA detections function properly. The **Partial** data migration takes much less time to install. If you select **Full** data migration, it may take a significant amount of time for the installation to complete. The estimated amount of time and the required disk space, which are listed on the **Data Migration** screen, depend on the amount of previously captured network traffic you had saved in previous versions of ATA. Before selecting **Partial** or **Full**, make sure to check these requirements.

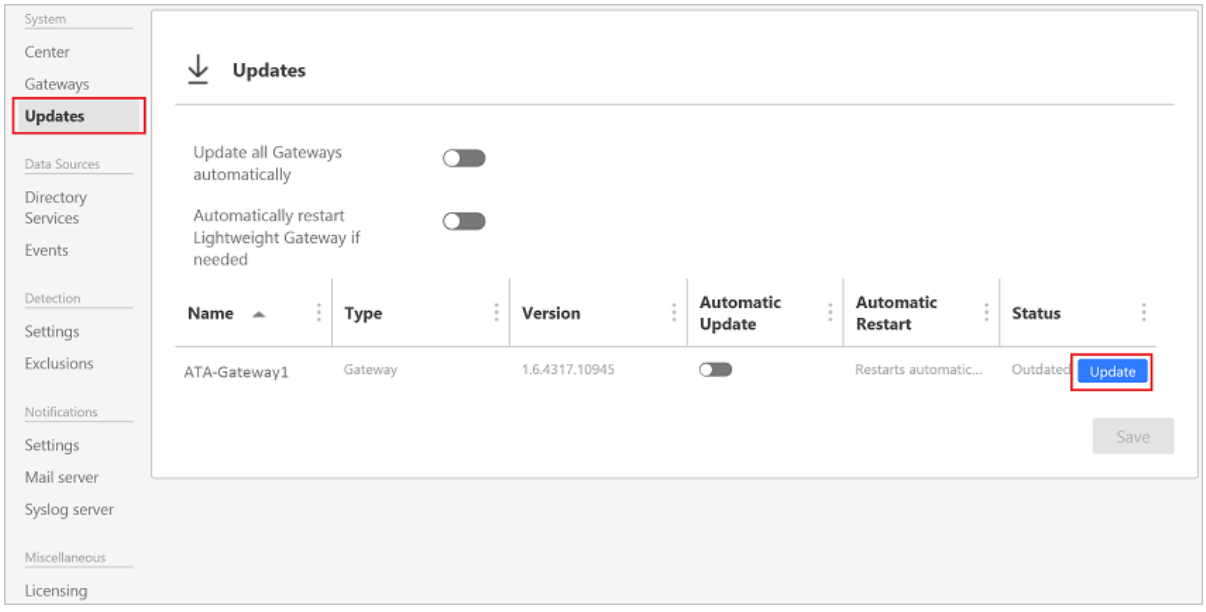


- Click **Update**. After you click Update, ATA is offline until the update procedure is complete.

3. After the ATA Center update completes successfully, click **Launch** to open the **Update** screen in the ATA console for the ATA Gateways.



4. In the **Updates** screen, if you already set your ATA Gateways to automatically update, they update at this point, if not, click **Update** next to each ATA Gateway.



IMPORTANT

Update all the ATA Gateways to make sure ATA functions properly. The configured Syslog listener port on all Gateways will be changed to 514.

NOTE

To install new ATA Gateways, go the **Gateways** screen and click **Download Gateway Setup** to get the ATA 1.7 installation package and follow the instructions for new Gateway installation as described in Step 4. Install the ATA Gateway.

See Also

- Check out the ATA forum!

What's new in ATA version 1.6

7/20/2020 • 6 minutes to read • Edit Online

These release notes provide information about known issues in this version of Advanced Threat Analytics.

What's new in the ATA 1.6 update?

The update to ATA 1.6 provides improvements in the following areas:

- New detections
- Improvements to existing detections
- The ATA Lightweight Gateway
- Automatic updates
- Improved ATA Center performance
- Lower storage requirements
- Support for IBM QRadar

New detections

- **Malicious Data Protection Private Information Request** Data Protection API (DPAPI) is a password-based data protection service. This protection service is used by various applications that store user's secrets, such as website passwords and file-share credentials. In order to support password-loss scenarios, users can decrypt protected data by using a recovery key, which doesn't involve their password. In a domain environment, attackers can remotely steal the recovery key and use it to decrypt protected data on all domain joined computers.

- **Net Session Enumeration** Reconnaissance is a key stage within the advanced attack kill chain. Domain Controllers (DCs) function as file servers for the purpose of Group Policy Object distribution, using the Server Message Block (SMB) protocol. As part of the reconnaissance phase, attackers can query the DC for all active SMB sessions on the server. It allow them to gain access to all users and IP addresses associated with those SMB sessions. SMB session enumeration can be used by attackers for targeting sensitive accounts, helping them move laterally across the network.

- **Malicious replication requests** In Active Directory environments, replication happens regularly between Domain Controllers. An attacker can spoof an Active Directory replication request (sometimes impersonating a Domain Controller). This spoof allows the attacker to retrieve the data stored in Active Directory, including password hashes, without utilizing more intrusive techniques like Volume Shadow Copy.

- **Detection of MS11-013 vulnerability**
  There is an elevation of privilege vulnerability in Kerberos, which allows for certain aspects of a Kerberos service ticket to be forged. A malicious user or attacker who successfully exploits this vulnerability can obtain a token with elevated privileges on the Domain Controller.

- **Unusual protocol implementation** Authentication requests (Kerberos or NTLM) are usually performed using a standard set of methods and protocols. However, in order to successfully authenticate, the request must meet only a specific set of requirements. Attackers might implement these protocols with minor deviations from the standard implementation in the environment. These deviations might indicate the presence of an attacker attempting to execute attacks such as Pass-The-Hash, Brute Force, and others.

Improvements to existing detections

ATA 1.6 includes improved detection logic that reduces false-positive and false-negative scenarios for existing detections such as Golden Ticket, Honey Token, Brute Force, and Remote Execution.

The ATA Lightweight Gateway

This version of ATA introduces a new deployment option for the ATA Gateway, which allows an ATA Gateway to be installed directly on the Domain Controller. This deployment option removes non-critical functionality of the ATA Gateway and introduces dynamic resource management based on available resources on the DC, which makes sure the existing operations of the DC are not affected. The ATA Lightweight Gateway reduces the cost of ATA deployment. At the same time, it makes deployment easier in branch sites, in which there is limited hardware resource capacity or inability to set up port-mirroring support. For more information about the ATA Lightweight Gateway, see ATA architecture

For more information about deployment considerations and choosing the right type of gateways for you, see ATA capacity planning

Automatic updates

Starting with version 1.6, it is possible to update the ATA Center using Microsoft Update. In addition, the ATA Gateways can now be automatically updated using their standard communication channel to the ATA Center.

Improved ATA Center performance

With this version, a lighter database load and a more efficient way of running all detection enables many more domain controllers to be monitored with a single ATA Center.

Lower storage requirements

ATA 1.6 necessitates ignificantly less storage space to run the ATA Database, now requiring only 20% of the storage space used in previous versions.

Support for IBM QRadar

ATA can now receive events from IBM's QRadar SIEM solution, in addition to the previously supported SIEM solutions.

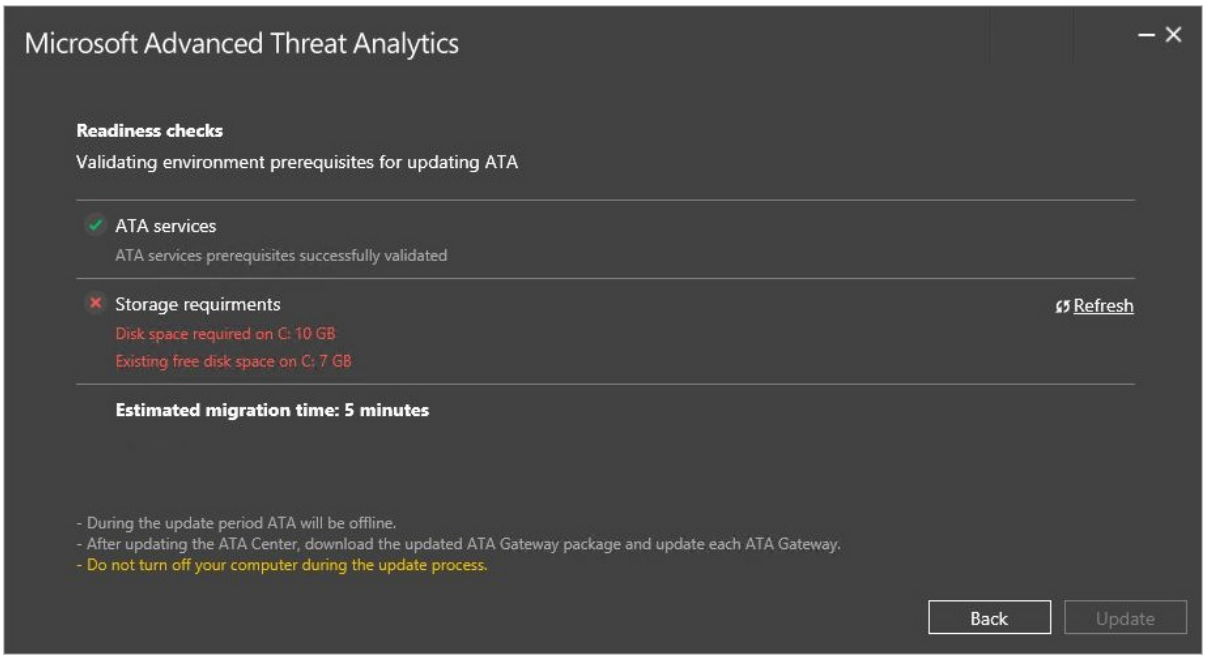
Known issues

The following known issues exist in this version.

Failure to recognize new path in manually moved databases

In deployments in which the database path is manually moved, ATA deployment does not use the new database path for the update. This manually moved database path may cause the following issues:

- ATA may use all the free space in the system drive of the ATA Center, without circularly deleting old network activities.
- Updating ATA to version 1.6 may fail the pre-update Readiness Checks, as shown in the image below.



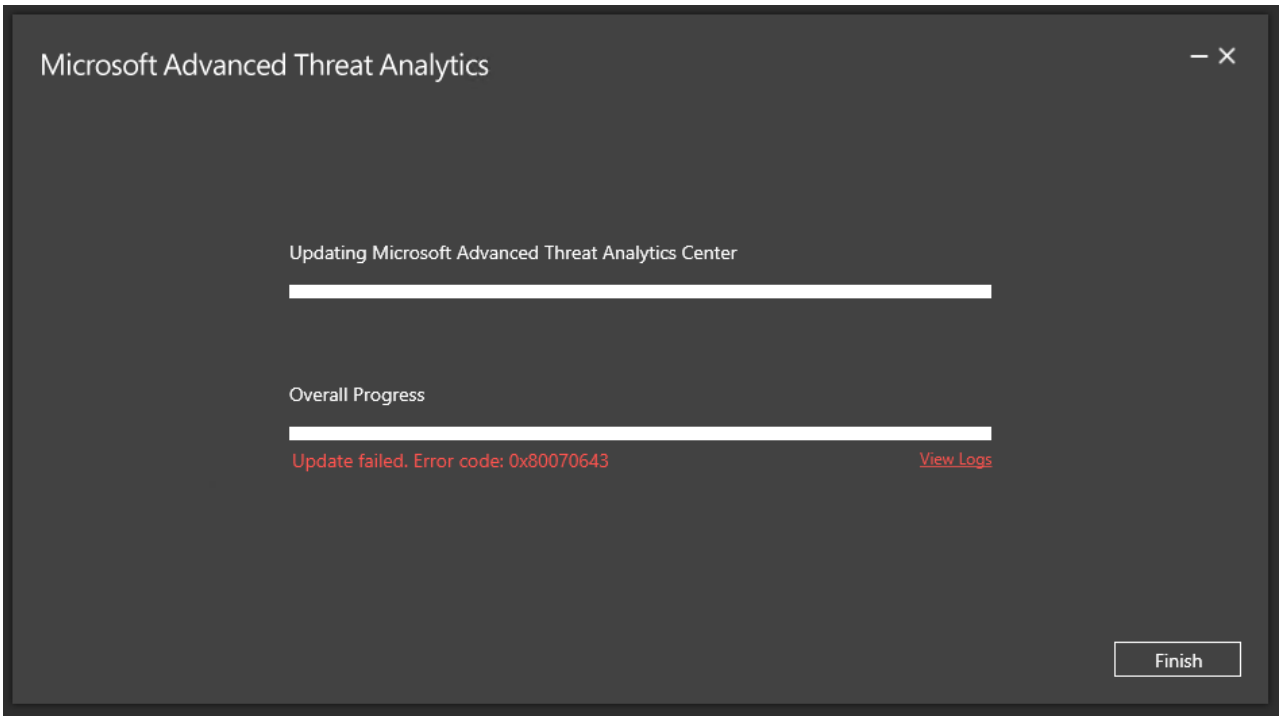
IMPORTANT

Before updating ATA to version 1.6, update the following registry key with the correct database path:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Advanced Threat Analytics\Center\DatabaseDataPath`

Migration failure when updating from ATA 1.5

When updating to ATA 1.6, the update process may fail with the following error code:



If you see this error, review the deployment log in: **C:\Users<User>\AppData\Local\Temp**, and look for the following exception:

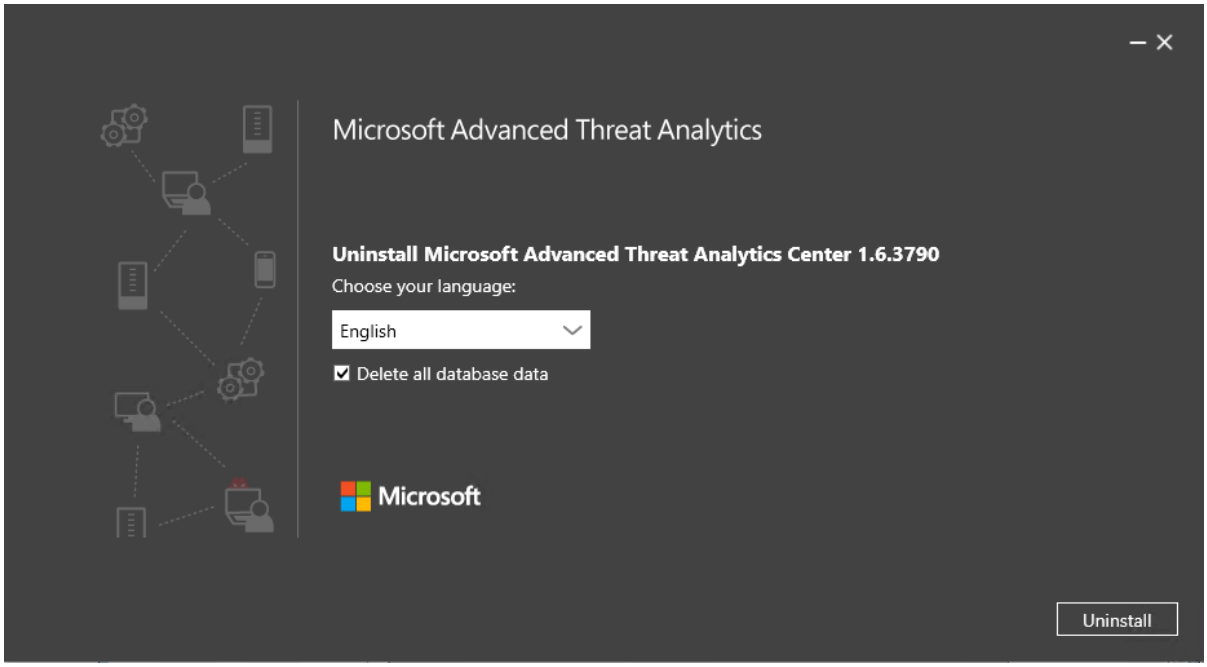
```
System.Reflection.TargetInvocationException: Exception has been thrown by the target of an invocation. --->
MongoDB.Driver.MongoWriteException: A write operation resulted in an error. E11000 duplicate key error index:
ATA.UniqueEntityProfile.$_id_ dup key: { : "<guid>" } ---> MongoDB.Driver.MongoBulkWriteException`1: A bulk
write operation resulted in one or more errors.  E11000 duplicate key error index:
ATA.UniqueEntityProfile.$_id_ dup key: { : " <guid> " }
```

You may also see this error: System.ArgumentNullException: Value cannot be null.

If you see either of these errors, run the following workaround:

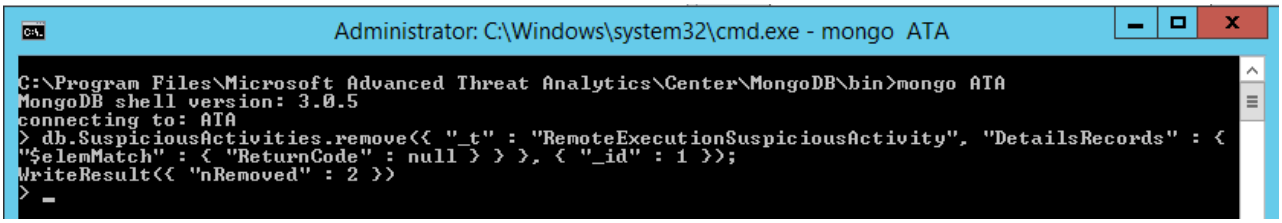
Workaround:

1. Move the folder "data_old" to a temporary folder (usually located in %ProgramFiles%\Microsoft Advanced Threat Analytics\Center\MongoDB\bin).
2. Uninstall the ATA Center v1.5, and delete all database data.



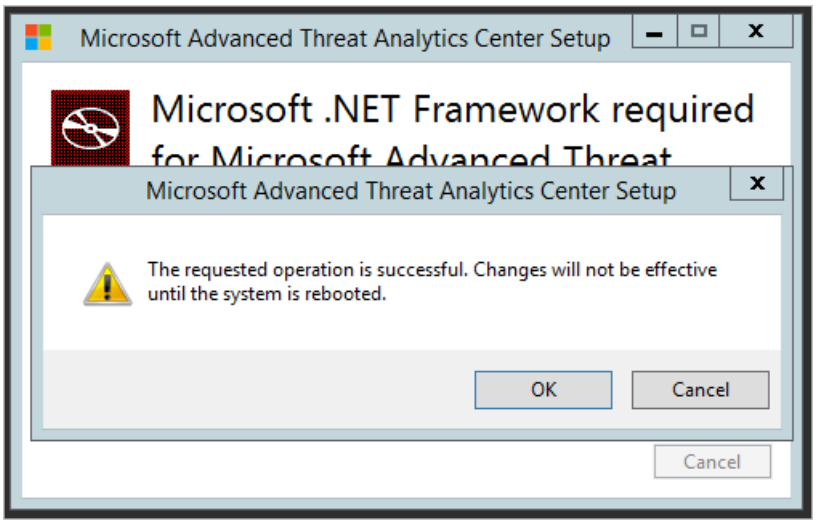
3. Reinstall ATA Center v1.5. Make sure to use the same configuration as the previous ATA 1.5 installation (Certificates, IP addresses, DB path, etc.).
4. Stop these services in the following order:
   a. Microsoft Advanced Threat Analytics Center
   b. MongoDB
5. Replace the MongoDB database files with the files in the "data_old" folder.
6. Start these services in the following order:
   a. MongoDB
   b. Microsoft Advanced Threat Analytics Center
7. Review the logs to verify that the product is running without errors.
8. Download the "RemoveDuplicateProfiles.exe" tool and copy it to the main installation path (%ProgramFiles%\Microsoft Advanced Threat Analytics\Center)
9. From an elevated command prompt, run `RemoveDuplicateProfiles.exe` and wait until it completes successfully.
10. From here: ...\Microsoft Advanced Threat Analytics\Center\MongoDB\bin directory: **Mongo ATA**, type the following command:

```
  db.SuspiciousActivities.remove({ "_t" : "RemoteExecutionSuspiciousActivity", "DetailsRecords" : {
"$elemMatch" : { "ReturnCode" : null } } }, { "_id" : 1 });
```



This should return a `WriteResult({ "nRemoved" : XX })` where "XX" is the number of Suspicious Activities that were deleted. If the number is greater than 0, exit the command prompt, and continue with the update process.

Net Framework 4.6.1 requires restarting the server



Historical network activities no longer migrated

This version of ATA delivers an improved detection engine, which provides more accurate detection and reduces many false positive scenarios, especially for Pass-the-Hash. The new and improved detection engine utilizes inline detection technology that enables detection without accessing historical network activity, to increase significantly the performance of the ATA Center. This also means that is unnecessary to migrate historical network activity during the update procedure. The ATA update procedure exports the data, in case you want it for future investigation, to `<Center Installation Path>\Migration` as a JSON file.

See Also

Check out the ATA forum!

Update ATA to version 1.6 - migration guide

ATA update to 1.6 migration guide

7/20/2020 • 4 minutes to read • Edit Online

The update to ATA 1.6 provides improvements in the following areas:

- New detections
- Improvements to existing detections
- The ATA Lightweight Gateway
- Automatic updates
- Improved ATA Center performance
- Lower storage requirements
- Support for IBM QRadar

Updating ATA to version 1.6

> **NOTE**
> If ATA is not installed in your environment, download the full version of ATA, which includes version 1.6 and follow the standard installation procedure described in Install ATA.

If you already have ATA version 1.5 deployed, this procedure walks you through the steps necessary to update your deployment.

> **NOTE**
> You cannot install ATA version 1.6 directly on top of ATA version 1.4. You must install ATA version 1.5 first. If you accidentally attempted to install ATA 1.6 without installing ATA 1.5, you get an error telling you that **A newer version is already installed on your machine.** You must uninstall the remnants of ATA 1.6 that remain on your computer - even though the installation failed - before you install ATA version 1.5.

Follow these steps to update to ATA version 1.6:

1. To avoid upgrade issues, make sure you follow steps 8 to 10 of **Migration failure when updating to ATA version 1.6** described in What's new in ATA version 1.6.
2. Make sure you have the necessary free space to complete the upgrade. You can perform the installation up to the readiness check to get an estimate of how much free space is needed, and then restart the upgrade after allocating the necessary disk space.
3. Download update 1.6
   In this version of, the same installation file (Microsoft ATA Center Setup.exe) is used for installing a new deployment of ATA and for upgrading existing deployments.
4. Update the ATA Center
5. Download the updated ATA Gateway package
6. Update the ATA Gateways

> **IMPORTANT**
>
> Update all the ATA Gateways to make sure ATA functions properly.

Step 1: Update the ATA Center

1. Back up your database: (optional)

   - If the ATA Center is running as a virtual machine and you want to take a checkpoint, shut down the virtual machine first.
   - If the ATA Center is running on a physical server, follow the recommended procedure to back up MongoDB.

2. Run the installation file, Microsoft ATA Center Setup.exe, and follow the instructions on the screen to install the update.

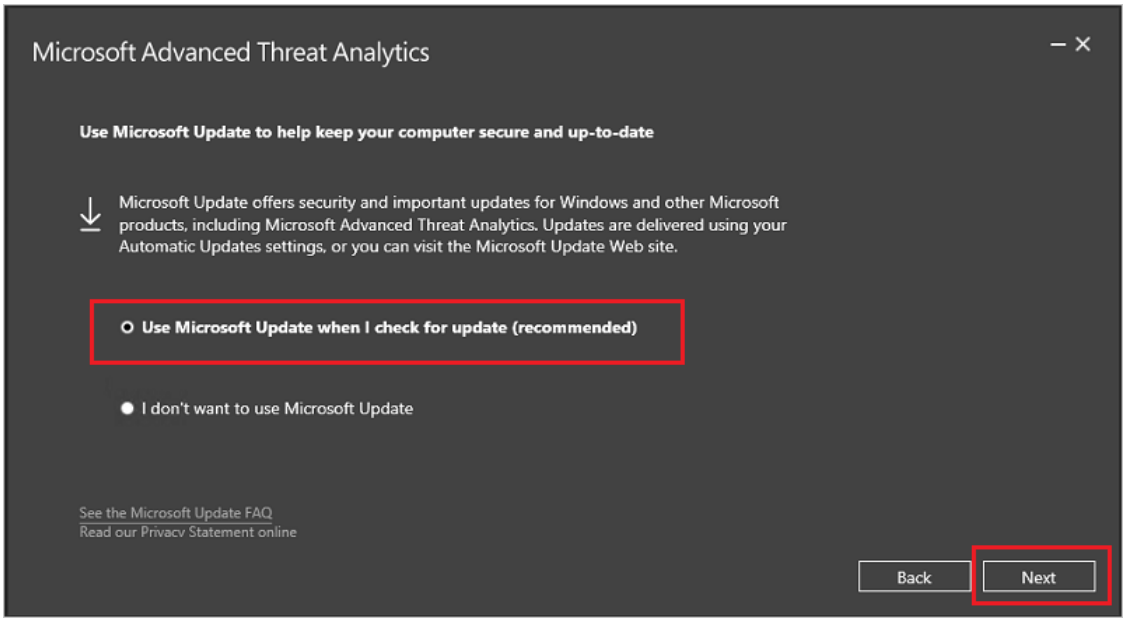
   a. ATA 1.6 requires .Net Framework 4.6.1 to be installed. If not already installed, ATA installation installs .Net Framework 4.6.1 as part of the installation.

   > **NOTE**
   >
   > The installation of .Net Framework 4.6.1 may require restarting the server. ATA installation will proceed only after the server was restarted.

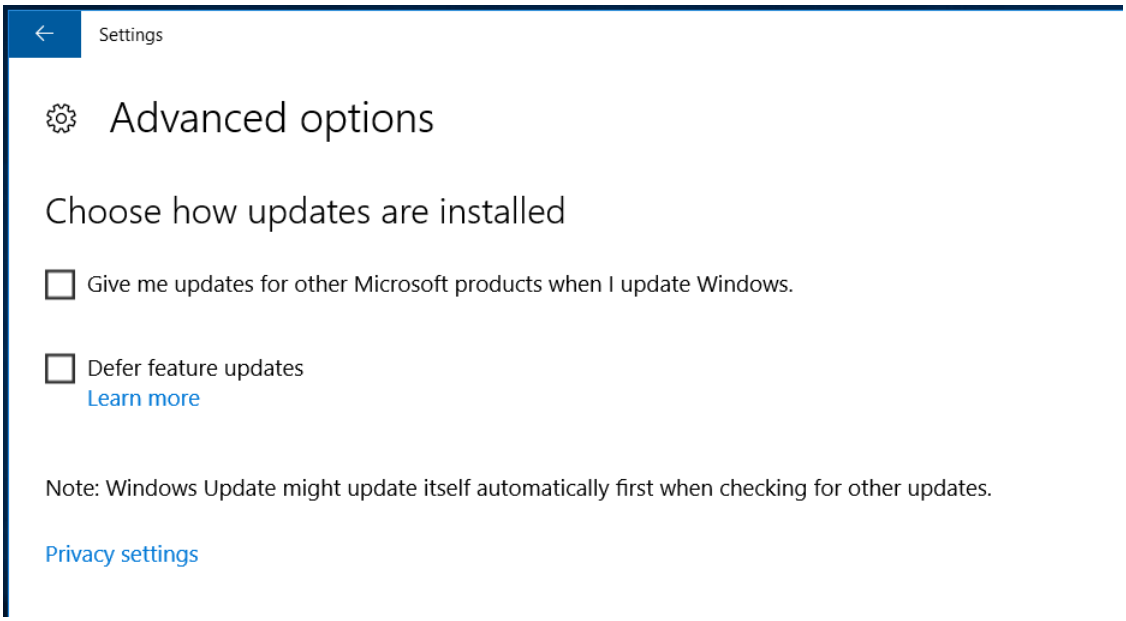
   b. On the **Welcome** page, select your language and click **Next**.

   c. Read the End-User License Agreement and if you accept the terms, click **Next**.

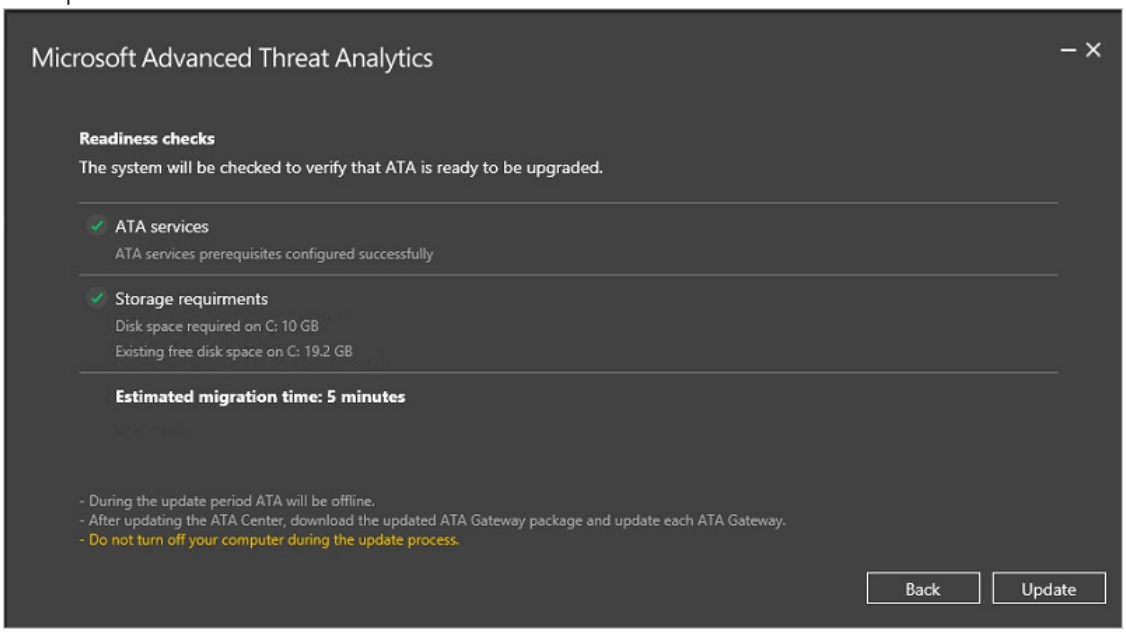
   d. It is now possible to use Microsoft Update for ATA to remain up-to-date. In the Microsoft Update page, select **Use Microsoft Update when I check for updates (recommended)**.



   This adjusts the Windows settings to enable updates for other Microsoft products (including ATA), as seen here.

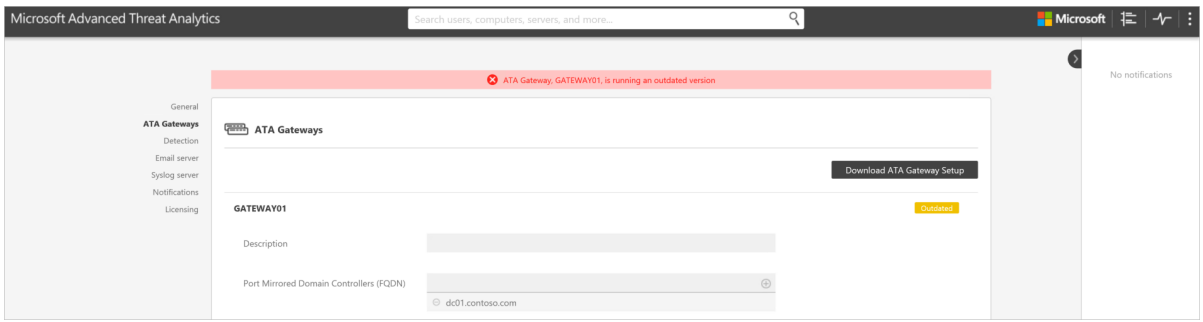


e. Before installation begins, ATA performs a readiness check. Review the results of the check to make sure the prerequisites are configured successfully and that you have at least the minimum amount of disk space.



f. Click **Update**. After you click Update, ATA is offline until the update procedure is complete.

3. After updating the ATA Center, the ATA Gateways will report that they are now outdated.



IMPORTANT

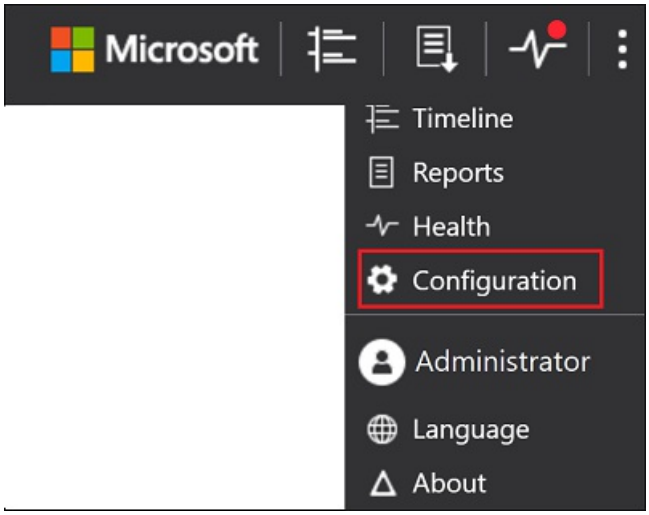
Update all the ATA Gateways to make sure ATA functions properly.

Step 2. Download the ATA Gateway setup package

After configuring the domain connectivity settings, you can download the ATA Gateway setup package.

To download the ATA Gateway package:

1. Delete any previous versions of the ATA Gateway package you previously downloaded.
2. On the ATA Gateway machine, open a browser and enter the IP address you configured in the ATA Center for the ATA Console. When the ATA Console opens, click on the settings icon and select **Configuration**.



3. In the **ATA Gateways** tab, click **Download ATA Gateway Setup**.
4. Save the package locally.

The zip file includes the following files:

- ATA Gateway installer
- Configuration setting file with the required information to connect to the ATA Center

Step 3: Update the ATA Gateways

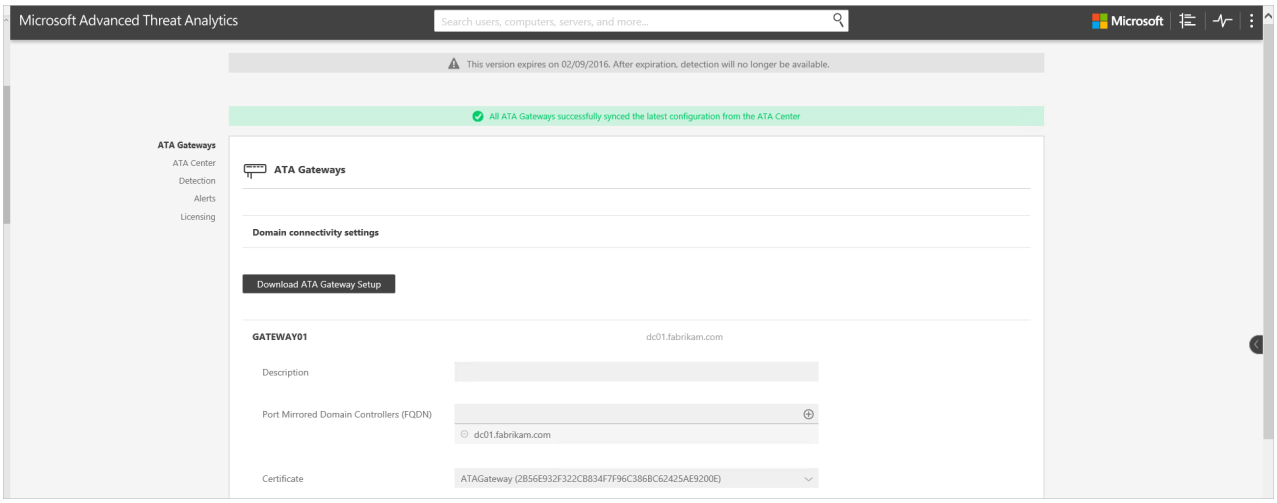
1. On each ATA Gateway, extract the files from the ATA Gateway package and run the file **Microsoft ATA Gateway Setup.exe**.

   > **NOTE**
   > You can also use this ATA Gateway package to install new ATA Gateways.

2. Your previous settings are preserved, but it may take a few minutes for the service to restart.
3. Repeat this step for all other ATA Gateways deployed.

> **NOTE**
> After successfully updating an ATA Gateway, the outdated notification for the specific ATA Gateway will be resolved.

You know that all the ATA Gateways have been successfully updated when all the ATA Gateways report that they are successfully synced and the message that an updated ATA Gateway package is available is no longer displayed.



See Also

- Check out the ATA forum!

What's new in ATA version 1.5

7/20/2020 • 2 minutes to read • Edit Online

These release notes provide information about known issues in this version of Advanced Threat Analytics.

What's new in the ATA 1.5 update?

The update to ATA 1.5 provides improvements in the following areas:

- Faster detection times
- Enhanced automatic detection algorithm for NAT (network address translation) devices
- Enhanced name resolution process for non-domain joined devices
- Support for data migration during product updates
- Better UI responsiveness for suspicious activities with thousands of entities involved
- Improved auto-resolution of health alerts
- Additional performance counters for enhanced monitoring and troubleshooting

Known issues

The following known issues exist in this version.

New ATA Gateway installation fails

After updating your ATA deployment to ATA version 1.5, you get the following error when installing a new ATA Gateway: Microsoft Advanced Threat Analytics Gateway is not installed

Workaround: Send an email to ataeval@microsoft.com to request workaround steps.

Deployment

The folder specified for the "Database data path" and "Database journal path" has to be empty (no files or subfolders). If it is not empty, the deployment does not progress.

Installation from Zip file

When installing the ATA Gateway, make sure to extract the files from the zip file to a local directory and install it from there. Do not install the ATA Gateway directly from within the zip file or the installation fails.

Configuration

After the configuration for an ATA Gateway is set, when the ATA Gateway starts for the first time, the "Not Synced" label is displayed until the service is fully started which may take up to 10 minutes the first time the service starts.

Network Capture Software

On the ATA Gateway, the only supported network capture software you can install is Microsoft Network Monitor 3.4. Do not install Microsoft Message Analyzer or any other network capturing software. Installing other software will cause the ATA Gateway to stop functioning properly.

KB on virtualization host

Do not install KB 3047154 on a virtualization host. This may cause port mirroring to stop working properly.

See Also

Update ATA to version 1.5 - migration guide

Update ATA to version 1.6 - migration guide

Check out the ATA forum!

ATA update to 1.5 migration guide

7/20/2020 • 3 minutes to read • Edit Online

The update to ATA 1.5 provides improvements in the following areas:

- Faster detection times
- Enhanced automatic detection algorithm for NAT (network address translation) devices
- Enhanced name resolution process for non-domain joined devices
- Support for data migration during product updates
- Better UI responsiveness for suspicious activities with thousands of entities involved
- Improved auto-resolution of health alerts
- Additional performance counters for enhanced monitoring and troubleshooting

Updating ATA to version 1.5

> **NOTE**
> If ATA is not installed in your environment, download the full version of ATA, which includes version 1.5 and follow the standard installation procedure described in Install ATA.

If you already have ATA version 1.4 deployed, this procedure walks you through the steps necessary to update your installation.

Follow these steps to update to ATA version 1.5:

1. Download ATA v1.5 from VLSC or MSDN.

   > **NOTE**
   > You can also use the updated full version of ATA to perform the update to version 1.5.

2. Update the ATA Center
3. Download the updated ATA Gateway package
4. Update the ATA Gateways

   > **IMPORTANT**
   > Update all the ATA Gateways to make sure ATA functions properly.

Step 1: Update the ATA Center

1. Back up your database: (optional)

   - If the ATA Center is running as a virtual machine and you want to take a checkpoint, shut down the virtual machine first.

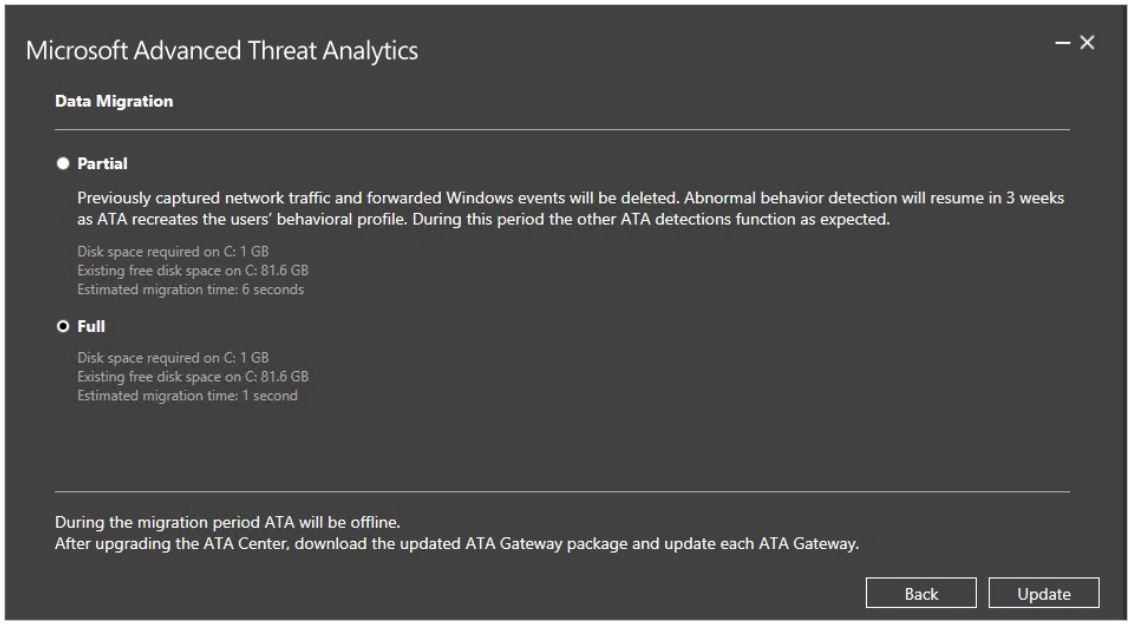
- If the ATA Center is running on a physical server, follow the recommended procedure to back up MongoDB.

2. Run the update file, Microsoft ATA Center Update.exe, and follow the instructions on the screen to install the update.

   a. In the **Welcome** page, select your language and click **Next**.

   b. Read the End-User License Agreement and if you accept the terms, click the checkbox, and click **Next**.

   c. Select whether you want to run the full (default) or partial migration.

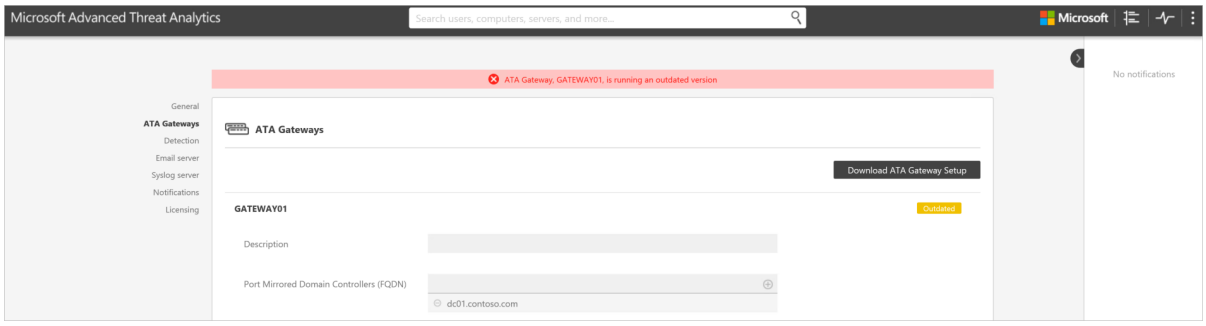


   - If you select **Partial** migration, any network traffic collected and forwarded Windows events analyzed by ATA are deleted and user behavioral profiles have to be relearned; this takes a minimum of three weeks. If you are running low on disk space, then it is helpful to run a **Partial** migration.

   - If you run a **Full** migration, you need additional disk space, as calculated for you on the upgrade page, and the migration may take longer, depending on the network traffic. The full migration retains all previously collected data and user behavioral profiles are maintained, meaning that it will not take additional time for ATA to learn behavior profiles and anomalous behavior can be detected immediately after update.

3. Click **Update**. Once you click Update, ATA is offline until the update procedure is complete.

4. After updating the ATA Center, the ATA Gateways will report that they are now outdated.



IMPORTANT

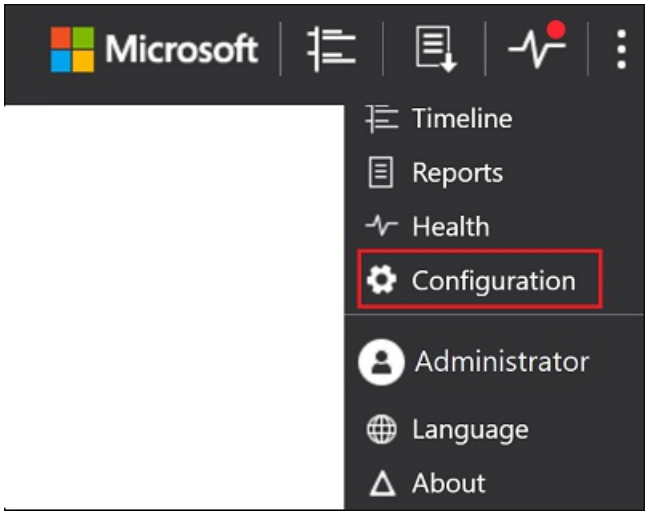
- Update all the ATA Gateways to make sure ATA functions properly.

Step 2. Download the ATA Gateway setup package

After configuring the domain connectivity settings, you can download the ATA Gateway setup package.

To download the ATA Gateway package:

1. Delete any previous versions of the ATA Gateway package you previously downloaded.
2. On the ATA Gateway machine, open a browser and enter the IP address you configured in the ATA Center for the ATA Console. When the ATA Console opens, click on the settings icon and select **Configuration**.



3. In the **ATA Gateways** tab, click **Download ATA Gateway Setup**.
4. Save the package locally.

The zip file includes the following files:

- ATA Gateway installer
- Configuration setting file with the required information to connect to the ATA Center

Step 3: Update the ATA Gateways

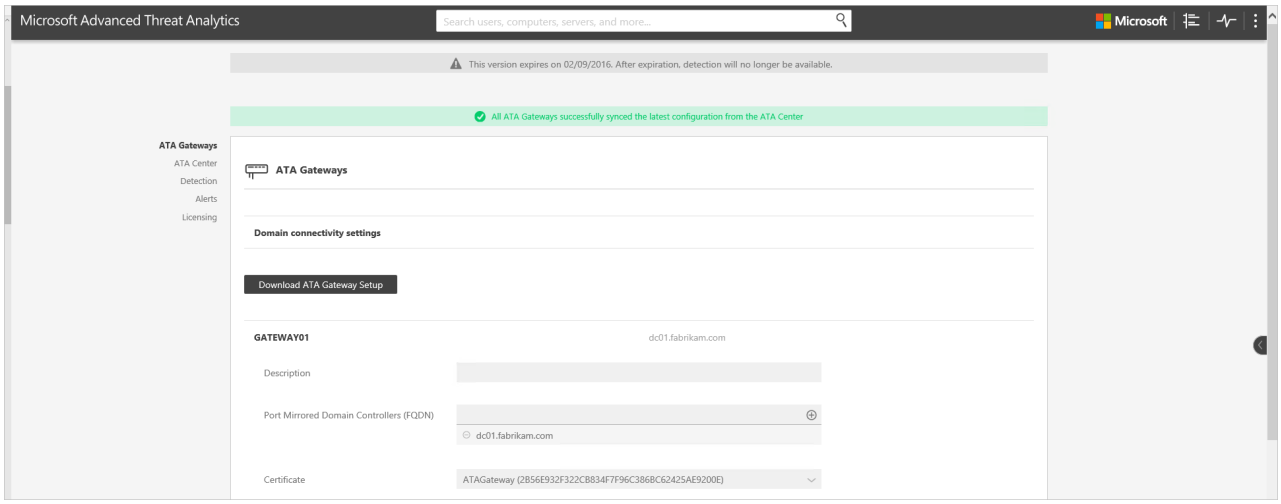
1. On each ATA Gateway, extract the files from the ATA Gateway package and run the file Microsoft ATA Gateway Setup.

   > **NOTE**
   > You can also use this ATA Gateway package to install new ATA Gateways.

2. Your previous settings are preserved, but it may take a few minutes until for the service to restart.
3. Repeat this step for all other ATA Gateways deployed.

> **NOTE**
> After successfully updating an ATA Gateway, the outdated notification for the specific ATA Gateway will go away.

You will know that all the ATA Gateways have been successfully updated when all the ATA Gateways report that they are successfully synced and the message that an updated ATA Gateway package is available is no longer displayed.



See Also

- Check out the ATA forum!

What's new in ATA version 1.4

7/20/2020 • 3 minutes to read • Edit Online

These release notes provide information about known issues in version 1.4 of Advanced Threat Analytics.

What's new in this version?

- Support for Windows Event Forwarding (WEF) to send events directly from the domain controllers to the ATA gateway.
- Pass-The-Hash detection enhancements on corporate resources by combining DPI (Deep Packet Inspection) and Windows event logs.
- Enhancements for the support of non-domain joined devices and non-Windows devices for detection and visibility.
- Performance improvements to support more traffic per ATA Gateway.
- Performance improvements to support more ATA Gateways per ATA Center.
- A new automatic name resolution process was added which matches computer names and IP addresses – this unique capability saves precious time in the investigation process and provide strong evidence for security analysts
- Improved ability to collect input from users to automatically fine-tune the detection process.
- Automatic detection for NAT devices.
- Automatic failover when domain controllers are not reachable.
- System health monitoring and notifications now provide the overall health state of the deployment as well as specific issues related to configuration and connectivity.
- Visibility into sites and locations where entities operate.
- Multi-domain support.
- Support for Single Label Domains (SLD).
- Support for modifying the IP address and certificate of the ATA Gateways and ATA Center.
- Telemetry to help improve customer experience.

Known issues

The following known issues exist in this version.

Network Capture Software

On the ATA Gateway, the only supported network capture software you can install is Microsoft Network Monitor 3.4. Do not install Microsoft Message Analyzer or any other network capturing software. Installing other software causes the ATA Gateway to stop functioning properly.

Installation from Zip file

When installing the ATA Gateway, make sure to extract the files from the zip file to a local directory and install it from there. Do not install the ATA Gateway directly from within the zip file or the installation fails.

Uninstalling previous versions of ATA

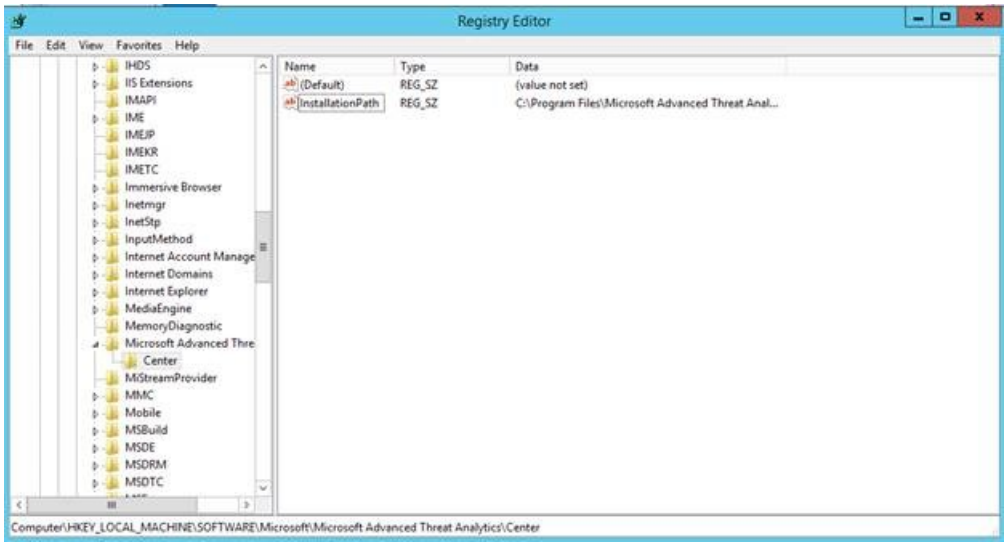
If you installed a previous version of ATA, Public Preview or Private Preview versions, you must uninstall the ATA Center and ATA Gateways before installing this release of ATA.

You must also delete the Database files and log files. The databases from previous versions of ATA are not compatible with the GA version of ATA.

If the ATA installation opens instead of the uninstallation when you attempt to uninstall the ATA Center or ATA Gateway, you need to add the following registry key and then uninstall ATA again.

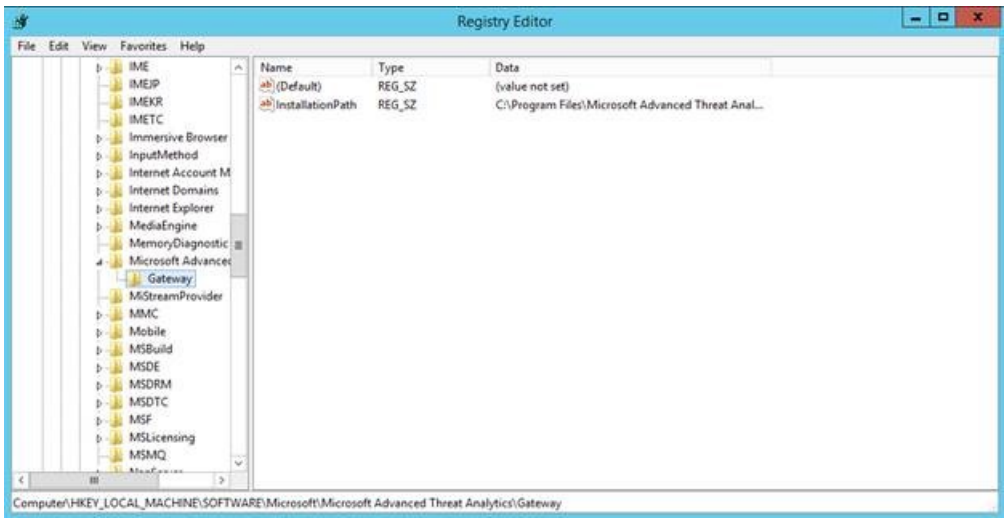
ATA Center

- HKLM\SOFTWARE\Microsoft\Microsoft Advanced Threat Analytics\Center
- Add a new String value named `InstallationPath` with a value of `C:\Program Files\Microsoft Advanced Threat Analytics\Center`. This is the default installation folder. If you changed the installation folder, enter the path where ATA is installed.



ATA Gateway

- HKLM\SOFTWARE\Microsoft\Microsoft Advanced Threat Analytics\Gateway
- Add a new String value named `InstallationPath` with a value of `C:\Program Files\Microsoft Advanced Threat Analytics\Gateway`. This is the default installation folder. If you changed the installation folder, enter the path where ATA is installed.



After uninstalling, delete the installation folder on both the ATA Center and the ATA Gateway. If you installed the Database in a separate folder, delete the Database folder on the ATA Center.

Health alert - disconnected ATA Gateway

If you have more than one ATA Gateway and have Disconnected ATA Gateway alerts, automatic resolve works on only one of them, leaving the rest in an Open status. Manually confirm that the ATA Gateway is up and the service is running and manually resolve the alert.

KB on virtualization host

Do not install KB 3047154 on a virtualization host. This may cause port mirroring to stop working properly.

See Also

Update ATA to version 1.6 - migration guide

Check out the ATA forum!

ATA frequently asked questions

7/20/2020 • 7 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

This article provides a list of frequently asked questions about ATA and provides insight and answers.

Where can I get a license for Advanced Threat Analytics (ATA)?

If you have an active Enterprise Agreement, you can download the software from the Microsoft Volume Licensing Center (VLSC).

If you acquired a license for Enterprise Mobility + Security (EMS) directly via the Microsoft 365 portal or through the Cloud Solution Partner (CSP) licensing model and you do not have access to ATA through the Microsoft Volume Licensing Center (VLSC), contact Microsoft Customer Support to obtain the process to activate Advanced Threat Analytics (ATA).

What should I do if the ATA Gateway won't start?

Look at the most recent error in the current error log (Where ATA is installed under the "Logs" folder).

How can I test ATA?

You can simulate suspicious activities which is an end to end test by doing one of the following:

1. DNS reconnaissance by using Nslookup.exe
2. Remote execution by using psexec.exe

This needs to run remotely against the domain controller being monitored and not from the ATA Gateway.

Which ATA build corresponds to each version?

For version upgrade information, see ATA upgrade path.

What version should I use to upgrade my current ATA deployment to the latest version?

For the ATA version upgrade matrix, see ATA upgrade path.

How does the ATA Center update its latest signatures?

The ATA detection mechanism is enhanced when a new version is installed on the ATA Center. You can upgrade the Center either by using Microsoft Update (MU) or by manually downloading the new version from Download Center or Volume License Site.

How do I verify Windows Event Forwarding?

You can place the the following code into a file and then execute it from a command prompt in the directory: **\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin** as follows:

mongo.exe ATA filename

```
db.getCollectionNames().forEach(function(collection) {
if (collection.substring(0,10)=="NtlmEvent_") {
        if (db[collection].count() > 0) {
                          print ("Found "+db[collection].count()+" NTLM events")
                        }
        }
});
```

Does ATA work with encrypted traffic?

ATA relies on analyzing multiple network protocols, as well as events collected from the SIEM or via Windows Event Forwarding. Detections based on network protocols with encrypted traffic (for example, LDAPS and IPSEC) will not be analyzed.

Does ATA work with Kerberos Armoring?

Enabling Kerberos Armoring, also known as Flexible Authentication Secure Tunneling (FAST), is supported by ATA, with the exception of over-pass the hash detection which will not work.

How many ATA Gateways do I need?

The number of ATA Gateways depend on your network layout, volume of packets and volume of events captured by ATA. To determine the exact number, see ATA Lightweight Gateway Sizing.

How much storage do I need for ATA?

For every one full day with an average of 1000 packets/sec you need 0.3 GB of storage.

For more information about ATA Center sizing see, ATA Capacity Planning.

Why are certain accounts considered sensitive?

This happens when an account is a member of certain groups which we designate as sensitive (for example: "Domain Admins").

To understand why an account is sensitive you can review its group membership to understand which sensitive groups it belongs to (the group that it belongs to can also be sensitive due to another group, so the same process should be performed until you locate the highest level sensitive group).

In addition, you can manually tag a user, group or computer as sensitive. For more information, see Tag sensitive accounts.

How do I monitor a virtual domain controller using ATA?

Most virtual domain controllers can be covered by the ATA Lightweight Gateway, to determine whether the ATA Lightweight Gateway is appropriate for your environment, see ATA Capacity Planning.

If a virtual domain controller can't be covered by the ATA Lightweight Gateway, you can have either a virtual or physical ATA Gateway as described in Configure port mirroring.
The easiest way is to have a virtual ATA Gateway on every host where a virtual domain controller exists.
If your virtual domain controllers move between hosts, you need to perform one of the following steps:

- When the virtual domain controller moves to another host, preconfigure the ATA Gateway in that host to receive the traffic from the recently moved virtual domain controller.
- Make sure that you affiliate the virtual ATA Gateway with the virtual domain controller so that if it is moved, the

ATA Gateway moves with it.

- There are some virtual switches that can send traffic between hosts.

How do I back up ATA?

Refer to ATA disaster recovery

What can ATA detect?

ATA detects known malicious attacks and techniques, security issues, and risks. For the full list of ATA detections, see What detections does ATA perform?.

What kind of storage do I need for ATA?

We recommend fast storage (7200-RPM disks are not recommended) with low latency disk access (less than 10 ms). The RAID configuration should support heavy write loads (RAID-5/6 and their derivatives are not recommended).

How many NICs does the ATA Gateway require?

The ATA Gateway needs a minimum of two network adapters:
1. A NIC to connect to the internal network and the ATA Center
2. A NIC that is used to capture the domain controller network traffic via port mirroring.
* This does not apply to the ATA Lightweight Gateway, which natively uses all of the network adapters that the domain controller uses.

What kind of integration does ATA have with SIEMs?

ATA has a bi-directional integration with SIEMs as follows:

1. ATA can be configured to send a Syslog alert, to any SIEM server using the CEF format, when a suspicious activity is detected.
2. ATA can be configured to receive Syslog messages for Windows events from these SIEMs.

Can ATA monitor domain controllers virtualized on your IaaS solution?

Yes, you can use the ATA Lightweight Gateway to monitor domain controllers that are in any IaaS solution.

Is this an on-premises or in-cloud offering?

Microsoft Advanced Threat Analytics is an on-premises product.

Is this going to be a part of Azure Active Directory or on-premises Active Directory?

This solution is currently a standalone offering—it is not a part of Azure Active Directory or on-premises Active Directory.

Do you have to write your own rules and create a threshold/baseline?

With Microsoft Advanced Threat Analytics, there is no need to create rules, thresholds, or baselines and then fine-tune. ATA analyzes the behaviors among users, devices, and resources—as well as their relationship to one another—and can detect suspicious activity and known attacks fast. Three weeks after deployment, ATA starts to detect behavioral suspicious activities. On the other hand, ATA will start detecting known malicious attacks and security

issues immediately after deployment.

If you are already breached, can Microsoft Advanced Threat Analytics identify abnormal behavior?

Yes, even when ATA is installed after you have been breached, ATA can still detect suspicious activities of the hacker. ATA is not only looking at the user's behavior but also against the other users in the organization security map. During the initial analysis time, if the attacker's behavior is abnormal, then it is identified as an "outlier" and ATA keeps reporting on the abnormal behavior. Additionally ATA can detect the suspicious activity if the hacker attempts to steal another users credentials, such as Pass-the-Ticket, or attempts to perform a remote execution on one of the domain controllers.

Does this only leverage traffic from Active Directory?

In addition to analyzing Active Directory traffic using deep packet inspection technology, ATA can also collect relevant events from your Security Information and Event Management (SIEM) and create entity profiles based on information from Active Directory Domain Services. ATA can also collect events from the event logs if the organization configures Windows Event Log forwarding.

What is port mirroring?

Also known as SPAN (Switched Port Analyzer), port mirroring is a method of monitoring network traffic. With port mirroring enabled, the switch sends a copy of all network packets seen on one port (or an entire VLAN) to another port, where the packet can be analyzed.

Does ATA monitor only domain-joined devices?

No. ATA monitors all devices in the network performing authentication and authorization requests against Active Directory, including non-Windows and mobile devices.

Does ATA monitor computer accounts as well as user accounts?

Yes. Since computer accounts (as well as any other entities) can be used to perform malicious activities, ATA monitors all computer accounts behavior and all other entities in the environment.

Can ATA support multi-domain and multi-forest?

Microsoft Advanced Threat Analytics supports multi-domain environments within the same forest boundary. Multiple forests require an ATA deployment for each forest.

Can you see the overall health of the deployment?

Yes, you can view the overall health of the deployment as well as specific issues related to configuration, connectivity etc., and you are alerted as they occur.

See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

ATA data security and privacy

7/20/2020 • 3 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

> **NOTE**
> This article provides steps for how to delete personal data from the device or service and can be used to support your obligations under the GDPR. If you're looking for general info about GDPR, see the GDPR section of the Service Trust portal.

Searching for and identifying personal data

All data in ATA that relates to entities is derived from Active Directory (AD) and replicated to ATA from there. When searching for personal data, the first place you should consider searching is AD.

From the ATA Center, use the search bar to view the identifiable personal data that is stored in the database. Users can search for a specific user or device. Clicking on the entity will open the user or device profile page. The profile provides you with the comprehensive details about the entity, it's history, and related network activity derived from AD.

Updating personal data

Personal data about users and entities in ATA is derived from the user's object in your organization's AD. Because of this, any changes made to the user profile in AD are reflected in ATA.

Deleting personal data

Although data in ATA is replicated and always updated from AD, when an entity is deleted in AD, the entity's data in ATA is maintained for purposes of security investigation.

To permanently delete user-related data from the ATA database, follow this procedure:

1. Download the MongoDB script (gdpr.js).
2. Copy the script into the ATA folder (located at `"C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB` and run the following command from the ATA Center machine:

Use the ATA GDPR database script to delete entities and delete entity activity data, as described in the following sections.

Delete entities

This action permanently deletes an entity from the ATA database. To run this command, provide the command name `deleteAccount`, and the `SamName`, `UpnName` or `GUID` of the computer or username you wish to delete. For example:

```
"C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\mongo.exe" ATA --eval "var
params='deleteAccount,admin1@contoso.com';" GDPR.js
```

Running this completely removes the entity with the UPN admin1@contoso.com from the database along with all the activities and security alerts associated with the entity.

Delete entity activity data

This action permanently deletes an entity's activities data from the ATA database. All entities will are unchanged but the activities and security alerts related to them for the specified timeframe are deleted.

To run this command, provide the command name `deleteOldData`, and the number of days of data you want to keep in the database.

For example:

```
"C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\mongo.exe" ATA --eval "var
params='deleteOldData,30';" GDPR.js
```

This script removes all data for all entity activities and security alerts from the database that are older than 30 days. You will retain only the last 30 days of data.

Exporting personal data

Because the data related to entities in ATA is derived from AD, only a subset of that data is stored in the ATA database. For this reason, you should export entity-related data from AD.

ATA enables you to export to Excel all security-related information, which might include personal data.

Opt-out of system-generated logs

ATA collects anonymized system-generated logs about each deployment and transmits this data over HTTPS to Microsoft servers. This data is used by Microsoft to help improve future versions of ATA.

For more information, see Manage system-generated logs.

To disable data collection:

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**.

Additional resources

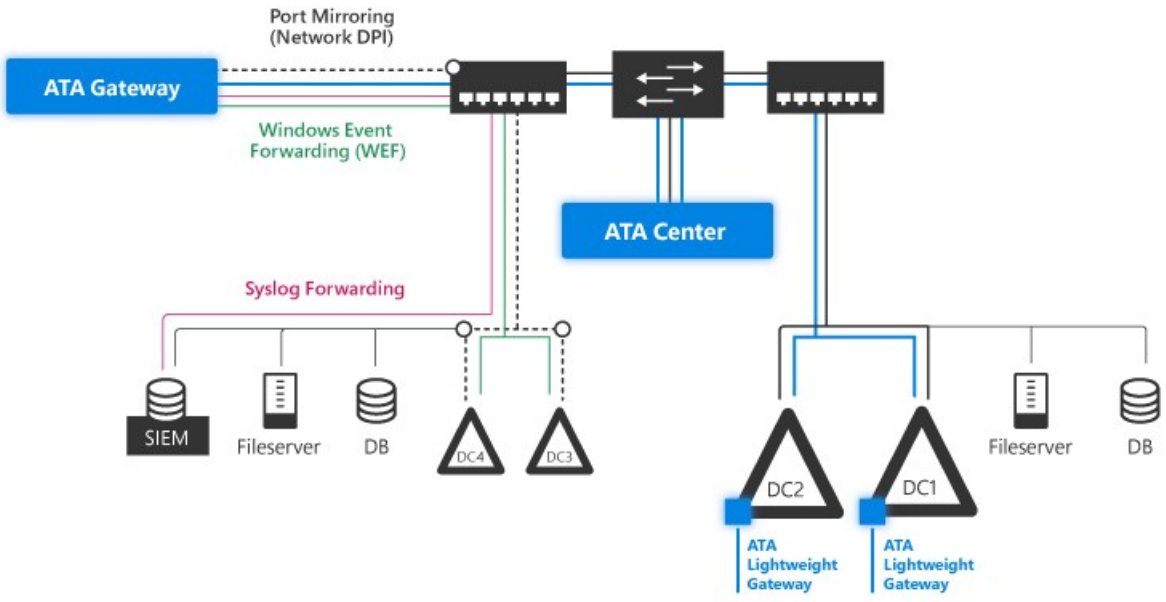
- For information about ATA trust and compliance, see the Service Trust portal and the Microsoft 365 Enterprise GDPR Compliance site.

ATA Architecture

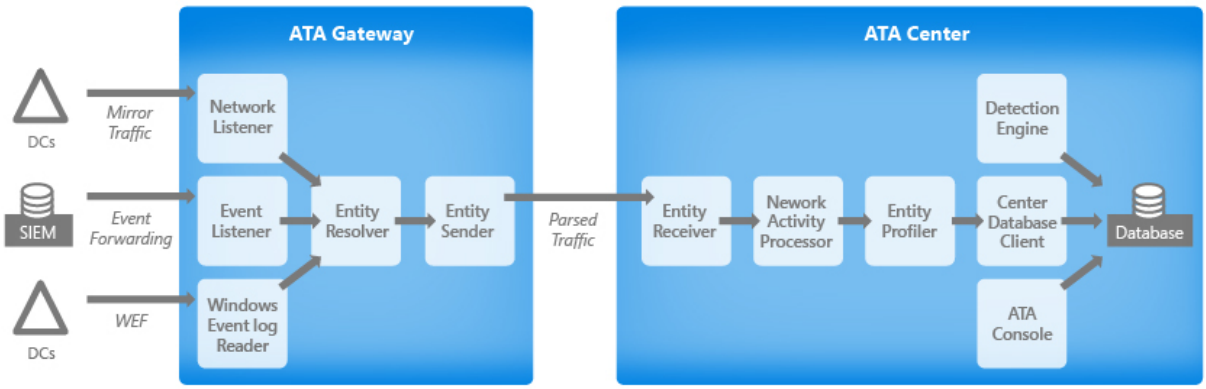
7/20/2020 • 9 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

The Advanced Threat Analytics architecture is detailed in this diagram:



ATA monitors your domain controller network traffic by utilizing port mirroring to an ATA Gateway using physical or virtual switches. If you deploy the ATA Lightweight Gateway directly on your domain controllers, it removes the requirement for port mirroring. In addition, ATA can leverage Windows events (forwarded directly from your domain controllers or from a SIEM server) and analyze the data for attacks and threats. This section describes the flow of network and event capturing and drills down to describe the functionality of the main components of ATA: the ATA Gateway, ATA Lightweight Gateway (which has the same core functionality as the ATA Gateway), and the ATA Center.



ATA Components

ATA consists of the following components:

- **ATA Center**
  The ATA Center receives data from any ATA Gateways and/or ATA Lightweight Gateways you deploy.
- **ATA Gateway**
  The ATA Gateway is installed on a dedicated server that monitors the traffic from your domain controllers using either port mirroring or a network TAP.
- **ATA Lightweight Gateway**
  The ATA Lightweight Gateway is installed directly on your domain controllers and monitors their traffic directly, without the need for a dedicated server or configuration of port mirroring. It is an alternative to the ATA Gateway.

An ATA deployment can consist of a single ATA Center connected to all ATA Gateways, all ATA Lightweight Gateways, or a combination of ATA Gateways and ATA Lightweight Gateways.

Deployment options

You can deploy ATA using the following combination of gateways:

- **Using only ATA Gateways**
  Your ATA deployment can contain only ATA Gateways, without any ATA Lightweight Gateways: All the domain controllers must be configured to enable port mirroring to an ATA Gateway or network TAPs must be in place.
- **Using only ATA Lightweight Gateways**
  Your ATA deployment can contain only ATA Lightweight Gateways: The ATA Lightweight Gateways are deployed on each domain controller and no additional servers or port mirroring configuration is necessary.
- **Using both ATA Gateways and ATA Lightweight Gateways**
  Your ATA deployment includes both ATA Gateways and ATA Lightweight Gateways. The ATA Lightweight Gateways are installed on some of your domain controllers (for example, all domain controllers in your branch sites). At the same time, other domain controllers are monitored by ATA Gateways (for example, the larger domain controllers in your main data centers).

In all these scenarios, all the gateways send their data to the ATA Center.

ATA Center

The **ATA Center** performs the following functions:

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

The ATA Center receives parsed traffic from the ATA Gateway and ATA Lightweight Gateway. It then performs profiling, runs deterministic detection, and runs machine learning and behavioral algorithms to learn about your network, enable detection of anomalies and warn you of suspicious activities.

Entity Receiver	Receives batches of entities from all ATA Gateways and ATA Lightweight Gateways.
Network Activity Processor	Processes all the network activities within each batch received. For example, matching between the various Kerberos steps performed from potentially different computers
Entity Profiler	Profiles all the Unique Entities according to the traffic and events. For example, ATA updates the list of logged-on computers for each user profile.
Center Database	Manages the writing process of the Network Activities and events into the database.
Database	ATA utilizes MongoDB for purposes of storing all the data in the system: - Network activities - Event activities - Unique entities - Suspicious activities - ATA configuration
Detectors	The Detectors use machine learning algorithms and deterministic rules to find suspicious activities and abnormal user behavior in your network.
ATA Console	The ATA Console is for configuring ATA and monitoring suspicious activities detected by ATA on your network. The ATA Console is not dependent on the ATA Center service and runs even when the service is stopped, as long as it can communicate with the database.

Consider the following criteria when deciding how many ATA Centers to deploy on your network:

- One ATA Center can monitor a single Active Directory forest. If you have more than one Active Directory forest, you need a minimum of one ATA Center per Active Directory forest.
- In large Active Directory deployments, a single ATA Center might not be able to handle all the traffic of all your domain controllers. In this case, multiple ATA Centers are required. The number of ATA Centers should be dictated by ATA capacity planning.

ATA Gateway and ATA Lightweight Gateway

Gateway core functionality

The **ATA Gateway** and **ATA Lightweight Gateway** both have the same core functionality:

- Capture and inspect domain controller network traffic. This is port mirrored traffic for ATA Gateways and local traffic of the domain controller in ATA Lightweight Gateways.
- Receive Windows events from SIEM or Syslog servers, or from domain controllers using Windows Event Forwarding
- Retrieve data about users and computers from the Active Directory domain
- Perform resolution of network entities (users, groups, and computers)

- Transfer relevant data to the ATA Center
- Monitor multiple domain controllers from a single ATA Gateway, or monitor a single domain controller for an ATA Lightweight Gateway.

The ATA Gateway receives network traffic and Windows Events from your network and processes it in the following main components:

Network Listener	The Network Listener captures network traffic and parsing the traffic. This is a CPU-heavy task, so it is especially important to check ATA Prerequisites when planning your ATA Gateway or ATA Lightweight Gateway.
Event Listener	The Event Listener captures and parsing Windows Events forwarded from a SIEM server on your network.
Windows Event Log Reader	The Windows Event Log Reader reads and parsing Windows Events forwarded to the ATA Gateway's Windows Event Log from the domain controllers.
Network Activity Translator	Translates parsed traffic into a logical representation of the traffic used by ATA (NetworkActivity).
Entity Resolver	The Entity Resolver takes the parsed data (network traffic and events) and resolves it data with Active Directory to find account and identity information. It is then matched with the IP addresses found in the parsed data. The Entity Resolver inspects the packet headers efficiently, to enable parsing of authentication packets for machine names, properties, and identities. The Entity Resolver combines the parsed authentication packets with the data in the actual packet.
Entity Sender	The Entity Sender sends the parsed and matched data to the ATA Center.

ATA Lightweight Gateway features

The following features work differently depending on whether you are running an ATA Gateway or an ATA Lightweight Gateway.

- The ATA Lightweight Gateway can read events locally, without the need to configure event forwarding.
- **Domain synchronizer candidate**
  The domain synchronizer gateway is responsible for synchronizing all entities from a specific Active Directory domain proactively (similar to the mechanism used by the domain controllers themselves for replication). One gateway is chosen randomly, from the list of candidates, to serve as the domain synchronizer.

  If the synchronizer is offline for more than 30 minutes, another candidate is chosen instead. If there is no domain synchronizer candidate available for a specific domain, ATA proactively synchronizes entities and their changes, however ATA will reactively retrieve new entities as they are detected in the monitored traffic.
  When no domain synchronizer is available, searching for an entity without traffic related to it displays no results.

By default, all ATA Gateways are domain synchronizer candidates.

Because all ATA Lightweight Gateways are more likely to be deployed in branch sites and on small domain controllers, they are not synchronizer candidates by default.

In an environment with only Lightweight Gateways, it is recommended to assign two of the gateways as synchronizer candidates, where one Lightweight Gateway is the default synchronizer candidate and one is the the backup in case the default is offline for more than 30 minutes.

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

  No matter what happens on the domain controller, this process always frees up resources to make sure the domain controller's core functionality is not affected.

  If this causes the ATA Lightweight Gateway to run out of resources, only partial traffic is monitored and the health alert "Dropped port mirrored network traffic" appears in the Health page.

The following table provides an example of a domain controller with enough compute resource available to allow for a larger quota then is currently needed, so that all traffic is monitored:

Active Directory (Lsass.exe)	ATA Lightweight Gateway (Microsoft.Tri.Gateway .exe)	Miscellaneous (other processes)	ATA Lightweight Gateway Quota	Gateway dropping
30%	20%	10%	45%	No

If Active Directory needs more compute, the quota needed by the ATA Lightweight Gateway is reduced. In the following example, The ATA Lightweight Gateway needs more than the allocated quota and drops some of the traffic (monitoring only partial traffic):

Active Directory (Lsass.exe)	ATA Lightweight Gateway (Microsoft.Tri.Gateway .exe)	Miscellaneous (other processes)	ATA Lightweight Gateway Quota	Is gateway dropping
60%	15%	10%	15%	Yes

Your network components

In order to work with ATA, make sure to check that the following components are set up.

Port mirroring

If you are using ATA Gateways, you have to set up port mirroring for the domain controllers that are monitored and set the ATA Gateway as the destination using the physical or virtual switches. Another option is to use network TAPs. ATA works if some but not all of your domain controllers are monitored, but detections are less effective.

While port mirroring mirrors all the domain controller network traffic to the ATA Gateway, only a small percentage of that traffic is then sent, compressed, to the ATA Center for analysis.

Your domain controllers and the ATA Gateways can be physical or virtual, see Configure port mirroring for more information.

Events

To enhance ATA detection of Pass-the-Hash, Brute Force, Modification to sensitive groups and Honey Tokens, ATA needs the following Windows events: 4776, 4732, 4733, 4728, 4729, 4756, 4757. These can either be read automatically by the ATA Lightweight Gateway or in case the ATA Lightweight Gateway is not deployed, it can be forwarded to the ATA Gateway in one of two ways, by configuring the ATA Gateway to listen for SIEM events or by Configuring Windows Event Forwarding.

- Configuring the ATA Gateway to listen for SIEM events
  Configure your SIEM to forward specific Windows events to ATA. ATA supports a number of SIEM vendors. For more information, see Configure event collection.

- Configuring Windows Event Forwarding
  Another way ATA can get your events is by configuring your domain controllers to forward Windows events 4776, 4732, 4733, 4728, 4729, 4756 and 4757 to your ATA Gateway. This is especially useful if you don't have a SIEM or if your SIEM is not currently supported by ATA. To complete your configuration of Windows Event Forwarding in ATA, see Configuring Windows event forwarding. This only applies to physical ATA Gateways - not to the ATA Lightweight Gateway.

Related Videos

- Choosing the right ATA Gateway type

See Also

- ATA prerequisites
- ATA sizing tool
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

ATA capacity planning

7/20/2020 • 6 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

This article helps you determine how many ATA servers are needed to monitor your network. It helps you estimate how many ATA Gateways and/or ATA Lightweight Gateways you need and the server capacity for your ATA Center and ATA Gateways.

> **NOTE**
> The ATA Center can be deployed on any IaaS vendor as long as the performance requirements described in this article are met.

Using the sizing tool

The recommended and simplest way to determine capacity for your ATA deployment is to use the ATA Sizing Tool. Run the ATA Sizing Tool and from the Excel file results, use the following fields to determine the ATA capacity you need:

- ATA Center CPU and Memory: Match the **Busy Packets/sec** field in the ATA Center table results file to the **PACKETS PER SECOND** field in the ATA Center table.
- ATA Center Storage: Match the **Avg Packets/sec** field in the ATA Center table results file to the **PACKETS PER SECOND** field in the ATA Center table.
- ATA Gateway: Match the **Busy Packets/sec** field in the ATA Gateway table in the results file to the **PACKETS PER SECOND** field in the ATA Gateway table or the ATA Lightweight Gateway table, depending on the gateway type you choose.

Number of DCs	4				
Number of Samples	69				
Overall Start Time UTC	2016-07-21 10:41:54				
Overall End Time UTC	2016-07-21 10:43:09				
Display DC Times as UTC/Local	Universal Time (UTC)				
Center	**Max Packets/sec**	**Avg Packets/sec**	**Busy Packets/sec**	**Busy Packets/sec Start UTC**	**Busy Packets/sec End UTC**
Grand Total	1,616	1,184	1,184	10:41:55	10:43:08
DC	**Max Packets/sec**	**Avg Packets/sec**	**Busy Packets/sec**	**Busy Packets/sec Start Time**	**Busy Packets/sec End Time**
DC1	644	457	457	10:41:54	10:43:08
DC3	334	234	234	10:41:54	10:43:08
DC4	408	249	249	10:41:54	10:43:08
DC2	405	244	244	10:41:54	10:43:08
Total	**1,792**	**1,184**	**1,184**		

> **NOTE**
> Because different environments vary and have multiple special and unexpected network traffic characteristics, after you initially deploy ATA and run the sizing tool, you may need to adjust and fine tune your deployment for capacity.

If for some reason you cannot use the ATA Sizing Tool, manually gather the packet/sec counter information from all your Domain Controllers for 24 hours with a low collection interval (approximately 5 seconds). Then, for each Domain Controller, calculate the daily average and the busiest period (15 minutes) average. The following sections provide instructions about how to collect the packets/sec counter from one Domain

Controller.

> **NOTE**
> Because different environments vary and have multiple special and unexpected network traffic characteristics, after you initially deploy ATA and run the sizing tool, you may need to adjust and fine tune your deployment for capacity.

ATA Center Sizing

The ATA Center requires a recommended minimum of 30 days of data for user behavioral analytics.

PACKETS PER SECOND FROM ALL DCS	CPU (CORES*)	MEMORY (GB)	DATABASE STORAGE PER DAY (GB)	DATABASE STORAGE PER MONTH (GB)	IOPS**
1,000	2	32	0.3	9	30 (100)
40,000	4	48	12	360	500 (750)
200,000	8	64	60	1,800	1,000 (1,500)
400,000	12	96	120	3,600	2,000 (2,500)
750,000	24	112	225	6,750	2,500 (3,000)
1,000,000	40	128	300	9,000	4,000 (5,000)

*This includes physical cores, not hyper-threaded cores.

**Average numbers (Peak numbers)

> **NOTE**
> - The ATA Center can handle an aggregated maximum of 1M packets per second from all monitored domain controllers. In some environments, the same ATA Center can handle overall traffic that is higher than 1M and some environments may exceed ATA capacity. Contact us at azureatpfeedback@microsoft.com for assistance in planning and estimating large environments.

- If your free space reaches a minimum of either 20% or 200 GB, the oldest collection of data is deleted. If it is not possible to successfully reduce the data collection to this level, an alert will be logged. ATA will continue functioning until the threshold of 5% or 50 GB free is reached. At this point, ATA will stop populating the database and an additional alert will be issued.
- It's possible to deploy the ATA Center on any IaaS vendor as long as the performance requirements that are described in this article are met.
- The storage latency for read and write activities should be below 10 ms.
- The ratio between read and write activities is approximately 1:3 below 100,000 packets-per-second and 1:6 above 100,000 packets-per-second.
- When running the Center as a virtual machine (VM) the Center requires all memory be allocated to the VM, all the time. For more information on running ATA Center as a virtual machine, see ATA Center requirements
- For optimal performance, set the **Power Option** of the ATA Center to **High Performance**.
- When working on a physical server, the ATA database needs you to **disable** Non-uniform memory access (NUMA) in the BIOS. Your system may refer to NUMA as Node Interleaving, in which case you have to **enable** Node Interleaving to disable NUMA. For more information, see your BIOS

> documentation. This is not relevant when the ATA Center is running on a virtual server.

Choosing the right gateway type for your deployment

In an ATA deployment any combination of the ATA Gateway types is supported:

- Only ATA Gateways
- Only ATA Lightweight Gateways
- A combination of both

When deciding the Gateway deployment type, consider the following benefits:

GATEWAY TYPE	BENEFITS	COST	DEPLOYMENT TOPOLOGY	DOMAIN CONTROLLER USE
ATA Gateway	The Out of band deployment makes it harder for attackers to discover ATA is present	Higher	Installed alongside the domain controller (out of band)	Supports up to 50,000 packets per second
ATA Lightweight Gateway	Doesn't require a dedicated server and port-mirroring configuration	Lower	Installed on the domain controller	Supports up to 10,000 packets per second

The following are examples of scenarios in which domain controllers should be covered by the ATA Lightweight Gateway:

- Branch sites
- Virtual domain controllers deployed in the cloud (IaaS)

The following are examples of scenarios in which domain controllers should be covered by the ATA Gateway:

- Headquarter data centers (having domain controllers with more than 10,000 packets per seconds)

ATA Lightweight Gateway Sizing

An ATA Lightweight Gateway can support the monitoring of one domain controller based on the amount of network traffic the domain controller generates.

PACKETS PER SECOND*	CPU (CORES**)	MEMORY (GB)***
1,000	2	6
5,000	6	16
10,000	10	24

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

**Total number of non-hyper threaded cores that this domain controller has installed.
While hyper threading is acceptable for the ATA Lightweight Gateway, when planning for capacity, you should count actual cores and not hyper threaded cores.

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

NOTE

- If the domain controller does not have the resources required by the ATA Lightweight Gateway, domain controller performance is not effected, but the ATA Lightweight Gateway might not operate as expected.
- When running the Gateway as a virtual machine (VM) the Gateway requires all memory be allocated to the VM, all the time. For more information on running ATA Gateway as a virtual machine, see Dynamic memory requirements)
- For optimal performance, set the **Power Option** of the ATA Lightweight Gateway to **High Performance**.
- A minimum of 5 GB of space is required and 10 GB is recommended, including space needed for the ATA binaries, ATA logs, and performance logs.

ATA Gateway Sizing

Consider the following issues when deciding how many ATA Gateways to deploy.

- **Active Directory forests and domains**
  ATA can monitor traffic from multiple domains from a single Active Directory forest. Monitoring multiple Active Directory forests requires separate ATA deployments. Do not configure a single ATA deployment to monitor network traffic of domain controllers from different forests.
- **Port Mirroring**
  Port mirroring considerations might require you to deploy multiple ATA Gateways per data Gateway or branch site.
- **Capacity**
  An ATA Gateway can support monitoring multiple domain controllers, depending on the amount of network traffic of the domain controllers being monitored.

PACKETS PER SECOND*	CPU (CORES**)	MEMORY (GB)
1,000	1	6
5,000	2	10
10,000	3	12
20,000	6	24
50,000	16	48

*Total average number of packets-per-second from all domain controllers being monitored by the specific ATA Gateway during their busiest hour of the day.

*The total amount of domain controller port-mirrored traffic cannot exceed the capacity of the capture NIC on the ATA Gateway.

**Hyper-threading must be disabled.

NOTE

- When running the Gateway as a virtual machine (VM) the Gateway requires all memory be allocated to the VM, all the time. For more information on running ATA Gateway as a virtual machine, see Dynamic memory requirements
- For optimal performance, set the **Power Option** of the ATA Gateway to **High Performance**.
- A minimum of 5 GB of space is required and 10 GB is recommended, including space needed for the ATA binaries, ATA logs, and performance logs.

Related Videos

- Choosing the right ATA Gateway type

See Also

- ATA sizing tool
- ATA prerequisites
- ATA architecture
- Check out the ATA forum!

ATA prerequisites

7/20/2020 • 13 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

This article describes the requirements for a successful ATA deployment in your environment.

> **NOTE**
> For information on how to plan resources and capacity, see ATA capacity planning.

ATA is composed of the ATA Center, the ATA Gateway and/or the ATA Lightweight Gateway. For more information about the ATA components, see ATA architecture.

The ATA System works on active directory forest boundary and supports Forest Functional Level (FFL) of Windows 2003 and above.

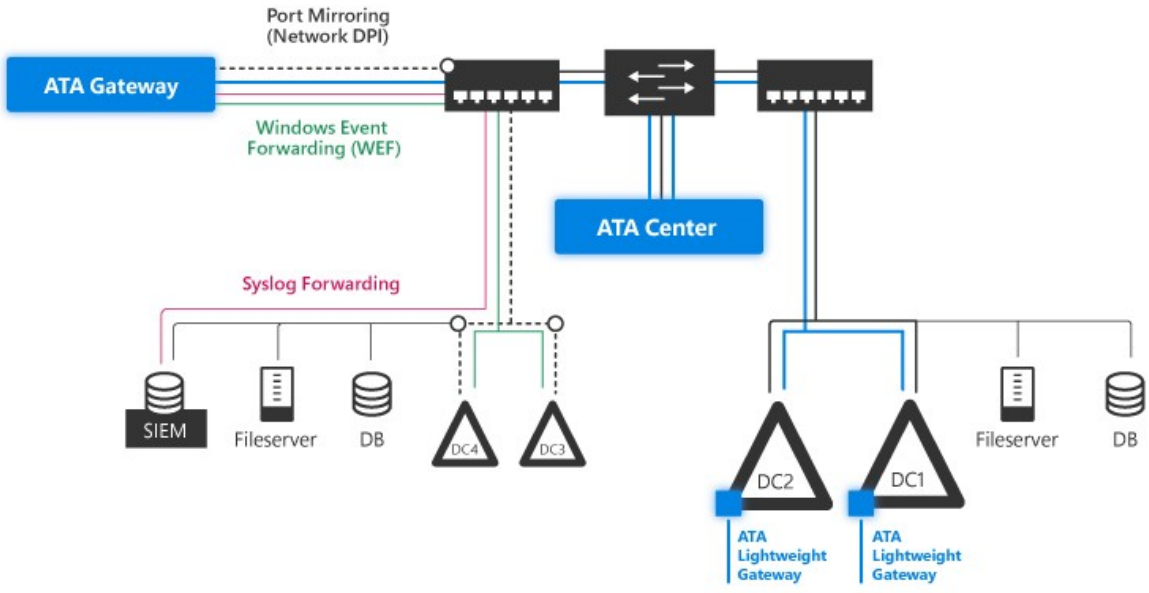
Before you start: This section lists information you should gather and accounts and network entities you should have, before starting ATA installation.

ATA Center: This section lists ATA Center hardware, software requirements as well as settings you need to configure on your ATA Center server.

ATA Gateway: This section lists ATA Gateway hardware, software requirements as well as settings you need to configure on your ATA Gateway servers.

ATA Lightweight Gateway: This section lists ATA Lightweight Gateway hardware, and software requirements.

ATA Console: This section lists browser requirements for running the ATA Console.



Before you start

This section lists information you should gather as well as accounts and network entities you should have before starting ATA installation.

- User account and password with read access to all objects in the monitored domains.

  > **NOTE**
  > If you have set custom ACLs on various Organizational Units (OU) in your domain, make sure that the selected user has read permissions to those OUs.

- Do not install Microsoft Message Analyzer on an ATA Gateway or Lightweight Gateway. The Message Analyzer driver conflicts with the ATA Gateway and Lightweight Gateway drivers. If you run Wireshark on ATA Gateway, you will need to restart the Microsoft Advanced Threat Analytics Gateway Service after you have stopped the Wireshark capture. If not, the Gateway stops capturing traffic. Running Wireshark on an ATA Lightweight Gateway does not interfere with the ATA Lightweight Gateway.

- Recommended: User should have read-only permissions on the Deleted Objects container. This allows ATA to detect bulk deletion of objects in the domain. For information about configuring read-only permissions on the Deleted Objects container, see the **Changing permissions on a deleted object container** section in the View or Set Permissions on a Directory Object article.

- Optional: A user account of a user with no network activities. This account is configurable as an ATA Honeytoken user. To configure an account as a Honeytoken user, only the username is required. For Honeytoken configuration information, see Configure IP address exclusions and Honeytoken user.

- Optional: In addition to collecting and analyzing network traffic to and from the domain controllers, ATA can use Windows events 4776, 4732, 4733, 4728, 4729, 4756 and 4757 to further enhance ATA Pass-the-Hash, Brute Force, Modification to sensitive groups and Honey Tokens detections. These events can be received from your SIEM or by setting Windows Event Forwarding from your domain controller. Events collected provide ATA with additional information that is not available via the domain controller network traffic.

ATA Center requirements

This section lists the requirements for the ATA Center.

General

The ATA Center supports installation on a server running Windows Server 2012 R2 Windows Server 2016 and Windows Server 2019.

> **NOTE**
> The ATA Center does not support Windows Server core.

The ATA Center can be installed on a server that is a member of a domain or workgroup.

Before installing ATA Center running Windows 2012 R2, confirm that the following update has been installed: KB2919355.

You can check by running the following Windows PowerShell cmdlet: `[Get-HotFix -Id kb2919355]`.

Installation of the ATA Center as a virtual machine is supported.

Server specifications

When working on a physical server, the ATA database necessitates that you **disable** Non-uniform memory access (NUMA) in the BIOS. Your system may refer to NUMA as Node Interleaving, in which case you have to **enable** Node Interleaving in order to disable NUMA. For more information, see your BIOS documentation.

For optimal performance, set the **Power Option** of the ATA Center to **High Performance**.
The number of domain controllers you are monitoring and the load on each of the domain controllers dictates the server specifications needed. For more information, see ATA capacity planning.

For Windows Operating systems 2008R2 and 2012, Gateway is not supported in a Multi Processor Group mode. For more information about multi-processor group mode, see troubleshooting.

Time synchronization

The ATA Center server, the ATA Gateway servers, and the domain controllers must have time synchronized to within five minutes of each other.

Network adapters

You should have the following set:

- At least one network adapter (if using physical server in VLAN environment, it is recommended to use two network adapters)
- An IP address for communication between the ATA Center and the ATA Gateway that is encrypted using SSL on port 443. (The ATA service binds to all IP addresses that the ATA Center has on port 443.)

Ports

The following table lists the minimum ports that have to be opened for the ATA Center to work properly.

PROTOCOL	TRANSPORT	PORT	TO/FROM	DIRECTION
SSL (ATA Communications)	TCP	443	ATA Gateway	Inbound
HTTP (optional)	TCP	80	Company Network	Inbound
HTTPS	TCP	443	Company Network and ATA Gateway	Inbound
SMTP (optional)	TCP	25	SMTP Server	Outbound
SMTPS (optional)	TCP	465	SMTP Server	Outbound
Syslog (optional)	TCP/UPS/TLS (configurable)	514 (default)	Syslog server	Outbound
LDAP	TCP and UDP	389	Domain controllers	Outbound
LDAPS (optional)	TCP	636	Domain controllers	Outbound
DNS	TCP and UDP	53	DNS servers	Outbound
Kerberos (optional if domain joined)	TCP and UDP	88	Domain controllers	Outbound
Windows Time (optional if domain joined)	UDP	123	Domain controllers	Outbound

> **NOTE**
> LDAP is required to test the credentials to be used between the ATA Gateways and the domain controllers. The test is performed from the ATA Center to a domain controller to test the validity of these credentials, after which the ATA Gateway uses LDAP as part of its normal resolution process.

Certificates

To install and deploy ATA more quickly, you can install self-signed certificates during installation. If you have chosen to use self-signed certificates, after the initial deployment it is recommended to replace self-signed certificates with certificates from an internal Certification Authority to be used by the ATA Center.

Make sure the ATA Center and ATA Gateways have access to your CRL distribution point. If they don't have Internet access, follow the procedure to manually import a CRL, taking care to install all the CRL distribution points for the whole chain.

The certificate must have:

- A private key
- A provider type of either Cryptographic Service Provider (CSP) or Key Storage Provider (KSP)
- A public key length of 2048 bits
- A value set for KeyEncipherment and ServerAuthentication usage flags
- KeySpec (KeyNumber) value of "KeyExchange" (AT_KEYEXCHANGE). The value "Signature" (AT_SIGNATURE) is *not* supported.
- All Gateway machines must be able to fully validate and trust the selected Center certificate.

For example, you can use the standard **Web server** or **Computer** templates.

> **WARNING**
> The process of renewing an existing certificate is not supported. The only way to renew a certificate is by creating a new certificate and configuring ATA to use the new certificate.

> **NOTE**
> - If you are going to access the ATA Console from other computers, ensure that those computers trust the certificate being used by ATA Center otherwise you get a warning page that there is a problem with the website's security certificate before getting to the log in page.
> - Starting with ATA version 1.8 the ATA Gateways and Lightweight Gateways are managing their own certificates and need no administrator interaction to manage them.

ATA Gateway requirements

This section lists the requirements for the ATA Gateway.

General

The ATA Gateway supports installation on a server running Windows Server 2012 R2 or Windows Server 2016 and Windows Server 2019 (including server core). The ATA Gateway can be installed on a server that is a member of a domain or workgroup. The ATA Gateway can be used to monitor Domain Controllers with Domain Functional Level of Windows 2003 and above.

Before installing ATA Gateway running Windows 2012 R2, confirm that the following update has been installed: KB2919355.

You can check by running the following Windows PowerShell cmdlet: `[Get-HotFix -Id kb2919355]`.

For information on using virtual machines with the ATA Gateway, see Configure port mirroring.

> **NOTE**
> A minimum of 5 GB of space is required and 10 GB is recommended. This includes space needed for the ATA binaries, ATA logs, and performance logs.

Server specifications

For optimal performance, set the **Power Option** of the ATA Gateway to **High Performance**.
An ATA Gateway can support monitoring multiple domain controllers, depending on the amount of network traffic to and from the domain controllers.

To learn more about dynamic memory or any other virtual machine memory management feature, see Dynamic memory.

For more information about the ATA Gateway hardware requirements, see ATA capacity planning.

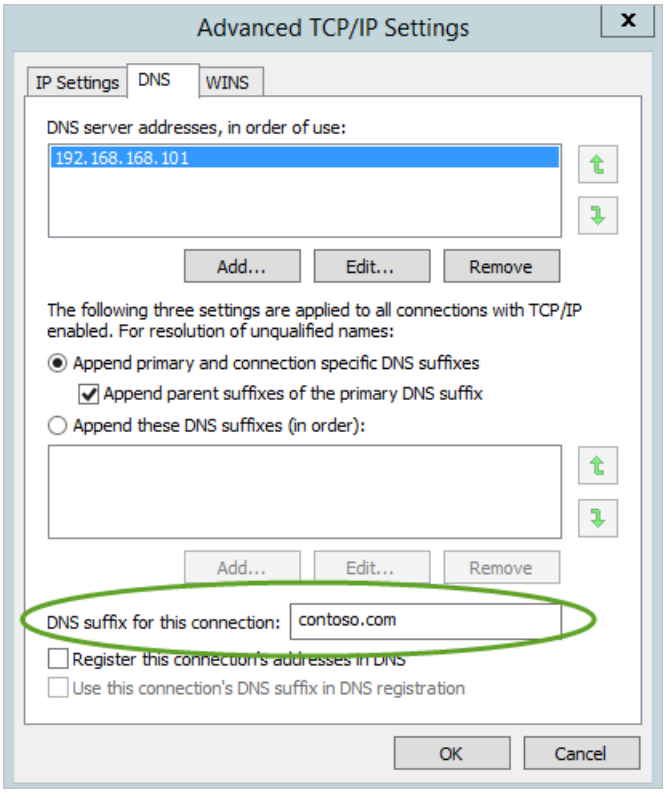
Time synchronization

The ATA Center server, the ATA Gateway servers, and the domain controllers must have time synchronized to within five minutes of each other.

Network adapters

The ATA Gateway requires at least one Management adapter and at least one Capture adapter:

- **Management adapter** - used for communications on your corporate network. This adapter should be configured with the following settings:
  - Static IP address including default gateway
  - Preferred and alternate DNS servers
  - The **DNS suffix for this connection** should be the DNS name of the domain for each domain being monitored.



> **NOTE**
> If the ATA Gateway is a member of the domain, this may be configured automatically.

- **Capture adapter** - used to capture traffic to and from the domain controllers.

> **IMPORTANT**
> - Configure port mirroring for the capture adapter as the destination of the domain controller network traffic. For more information, see Configure port mirroring. Typically, you need to work with the networking or virtualization team to configure port mirroring.
> - Configure a static non-routable IP address for your environment with no default gateway and no DNS server addresses. For example, 1.1.1.1/32. This ensures that the capture network adapter can capture the maximum amount of traffic and that the management network adapter is used to send and receive the required network traffic.

Ports

The following table lists the minimum ports that the ATA Gateway requires configured on the management adapter:

PROTOCOL	TRANSPORT	PORT	TO/FROM	DIRECTION
LDAP	TCP and UDP	389	Domain controllers	Outbound
Secure LDAP (LDAPS)	TCP	636	Domain controllers	Outbound
LDAP to Global Catalog	TCP	3268	Domain controllers	Outbound
LDAPS to Global Catalog	TCP	3269	Domain controllers	Outbound
Kerberos	TCP and UDP	88	Domain controllers	Outbound
Netlogon (SMB, CIFS, SAM-R)	TCP and UDP	445	All devices on network	Outbound
Windows Time	UDP	123	Domain controllers	Outbound
DNS	TCP and UDP	53	DNS Servers	Outbound
NTLM over RPC	TCP	135	All devices on the network	Both
NetBIOS	UDP	137	All devices on the network	Both
SSL	TCP	443	ATA Center	Outbound
Syslog (optional)	UDP	514	SIEM Server	Inbound

NOTE

As part of the resolution process done by the ATA Gateway, the following ports need to be open inbound on devices on the network from the ATA Gateways.

- NTLM over RPC (TCP Port 135)
- NetBIOS (UDP port 137)
- Using the Directory service user account, the ATA Gateway queries endpoints in your organization for local admins using SAM-R (network logon) in order to build the lateral movement path graph. For more information, see Configure SAM-R required permissions.
- The following ports need to be open inbound on devices on the network from the ATA Gateway:
- NTLM over RPC (TCP Port 135) for resolution purposes
- NetBIOS (UDP port 137) for resolution purposes

ATA Lightweight Gateway requirements

This section lists the requirements for the ATA Lightweight Gateway.

General

The ATA Lightweight Gateway supports installation on a domain controller running Windows Server 2008 R2 SP1 (not including Server Core), Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 and Windows Server 2019 (including Core but not Nano).

The domain controller can be a read-only domain controller (RODC).

Before installing ATA Lightweight Gateway on a domain controller running Windows Server 2012 R2, confirm that the following update has been installed: KB2919355.

You can check by running the following Windows PowerShell cmdlet: `[Get-HotFix -Id kb2919355]`

If the installation is for Windows server 2012 R2 Server Core, the following update should also be installed: KB3000850.

You can check by running the following Windows PowerShell cmdlet: `[Get-HotFix -Id kb3000850]`

During installation, the .Net Framework 4.6.1 is installed and might cause a reboot of the domain controller.

NOTE

A minimum of 5 GB of space is required and 10 GB is recommended. This includes space needed for the ATA binaries, ATA logs, and performance logs.

Server specifications

The ATA Lightweight Gateway requires a minimum of 2 cores and 6 GB of RAM installed on the domain controller. For optimal performance, set the **Power Option** of the ATA Lightweight Gateway to **High Performance**. The ATA Lightweight Gateway can be deployed on domain controllers of various loads and sizes, depending on the amount of network traffic to and from the domain controllers and the amount of resources installed on that domain controller.

To learn more about dynamic memory or any other virtual machine memory management feature, see Dynamic memory.

For more information about the ATA Lightweight Gateway hardware requirements, see ATA capacity planning.

Time synchronization

The ATA Center server, the ATA Lightweight Gateway servers, and the domain controllers must have time

synchronized to within five minutes of each other.

Network adapters

The ATA Lightweight Gateway monitors the local traffic on all of the domain controller's network adapters.

After deployment, you can use the ATA Console if you ever want to modify which network adapters are monitored.

> **NOTE**
> The Lightweight Gateway is not supported on domain controllers running Windows 2008 R2 with Broadcom Network Adapter Teaming enabled.

Ports

The following table lists the minimum ports that the ATA Lightweight Gateway requires:

PROTOCOL	TRANSPORT	PORT	TO/FROM	DIRECTION
DNS	TCP and UDP	53	DNS Servers	Outbound
NTLM over RPC	TCP	135	All devices on the network	Both
NetBIOS	UDP	137	All devices on the network	Both
SSL	TCP	443	ATA Center	Outbound
Syslog (optional)	UDP	514	SIEM Server	Inbound
Netlogon (SMB, CIFS, SAM-R)	TCP and UDP	445	All devices on network	Outbound

> **NOTE**
> As part of the resolution process performed by the ATA Lightweight Gateway, the following ports need to be open inbound on devices on the network from the ATA Lightweight Gateways.
>
> - NTLM over RPC
> - NetBIOS
> - Using the Directory service user account, the ATA Lightweight Gateway queries endpoints in your organization for local admins using SAM-R (network logon) in order to build the lateral movement path graph. For more information, see Configure SAM-R required permissions.
> - The following ports need to be open inbound on devices on the network from the ATA Gateway:
> - NTLM over RPC (TCP Port 135) for resolution purposes
> - NetBIOS (UDP port 137) for resolution purposes

Dynamic memory

> **NOTE**
> When running ATA services as a virtual machine (VM) the service requires all memory be allocated to the VM, all the time.

VM RUNNING ON	DESCRIPTION
Hyper-V	Ensure that **Enable Dynamic Memory** is not enabled for the VM.
VMWare	Ensure that the amount of memory configured and the reserved memory are the same, or select the following option in the VM setting – **Reserve all guest memory (All locked)**.
Other virtualization host	Refer to the vendor supplied documentation on how to ensure that memory is fully allocated to the VM at all times.

If you run the ATA Center as a virtual machine, shut down the server before creating a new checkpoint to avoid potential database corruption.

ATA Console

Access to the ATA Console is via a browser, supporting the browsers and settings:

- Internet Explorer version 10 and above
- Microsoft Edge
- Google Chrome 40 and above
- Minimum screen width resolution of 1700 pixels

Related Videos

- Choosing the right ATA Gateway type

See Also

- ATA sizing tool
- ATA architecture
- Install ATA
- Check out the ATA forum!

Recommended upgrade path for ATA

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

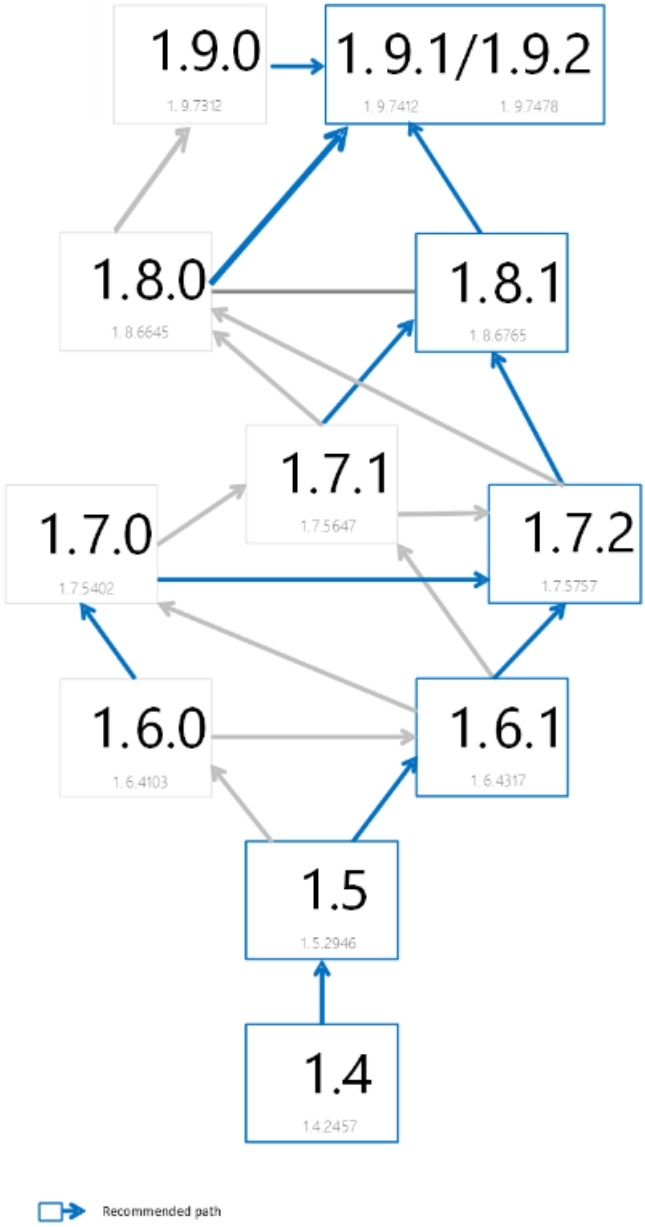
This article provides information about available Advanced Threat Analytics versions and how to upgrade ATA depending on which version you have running.

ATA versions

VERSION	BUILD #
1.6	1.6.4103
1.6 Update 1	1.6.4317
1.7	1.7.5402
1.7 Update 1	1.7.5647
1.7 Update 2	1.7.5757
1.8	1.8.6645
1.8 Update 1	1.8.6765
1.9	1.9.7312
1.9 Update 1	1.9.7412
1.9 Update 2	1.9.7478

Upgrade paths

Refer to the upgrade path diagram to determine the correct upgrade path for your current installation.



See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

Install ATA - Step 1

7/20/2020 • 4 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

This installation procedure provides instructions for performing a fresh installation of ATA 1.9. For information on updating an existing ATA deployment from an earlier version, see the ATA migration guide for version 1.9.

IMPORTANT

If using Windows 2012 R2, you can install KB2934520 on the ATA Center server and on the ATA Gateway servers before beginning installation, otherwise the ATA installation installs this update and requires a restart in the middle of the ATA installation.

Step 1. Download and Install the ATA Center

After you have verified that the server meets the requirements, you can proceed with the installation of the ATA Center.

NOTE

If you acquired a license for Enterprise Mobility + Security (EMS) directly via the Microsoft 365 portal or through the Cloud Solution Partner (CSP) licensing model and you do not have access to ATA through the Microsoft Volume Licensing Center (VLSC), contact Microsoft Customer Support to obtain the process to activate Advanced Threat Analytics (ATA).

Perform the following steps on the ATA Center server.

1. Download ATA from the Microsoft Volume Licensing Service Center or from the TechNet Evaluation Center or from MSDN.
2. Log in to the computer on to which you are installing the ATA Center as a user who is a member of the local administrators group.
3. Run **Microsoft ATA Center Setup.EXE** and follow the setup wizard.

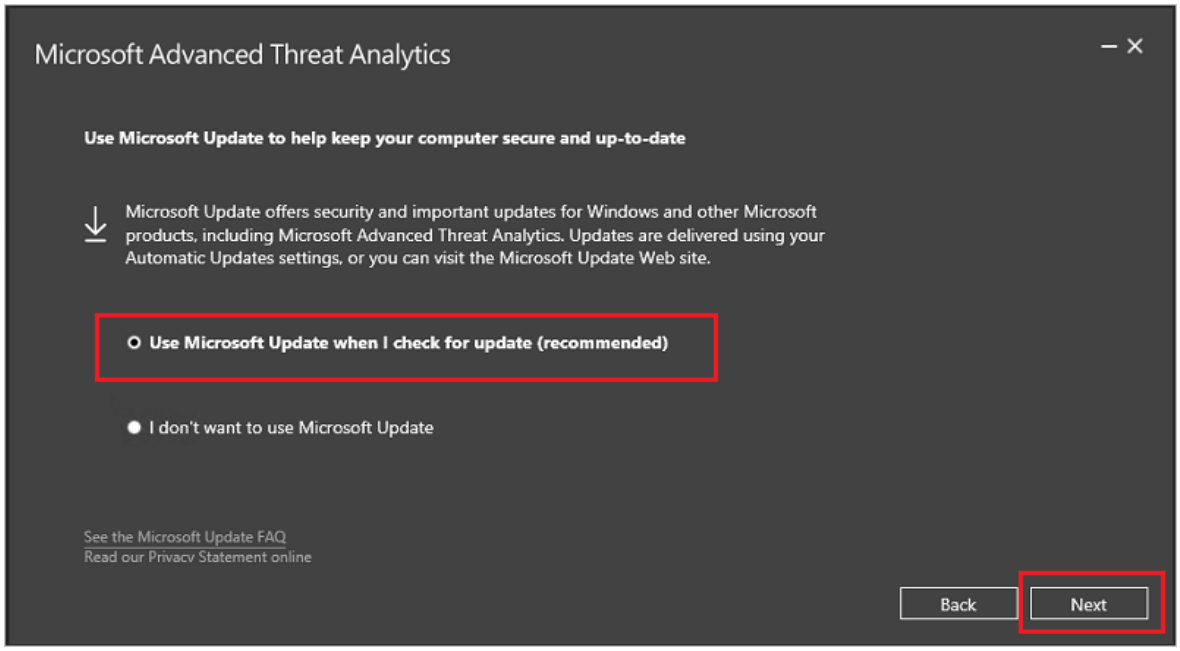
   NOTE

   Make sure to run the installation file from a local drive and not from a mounted ISO file to avoid issues in case a reboot is required as part of the installation.

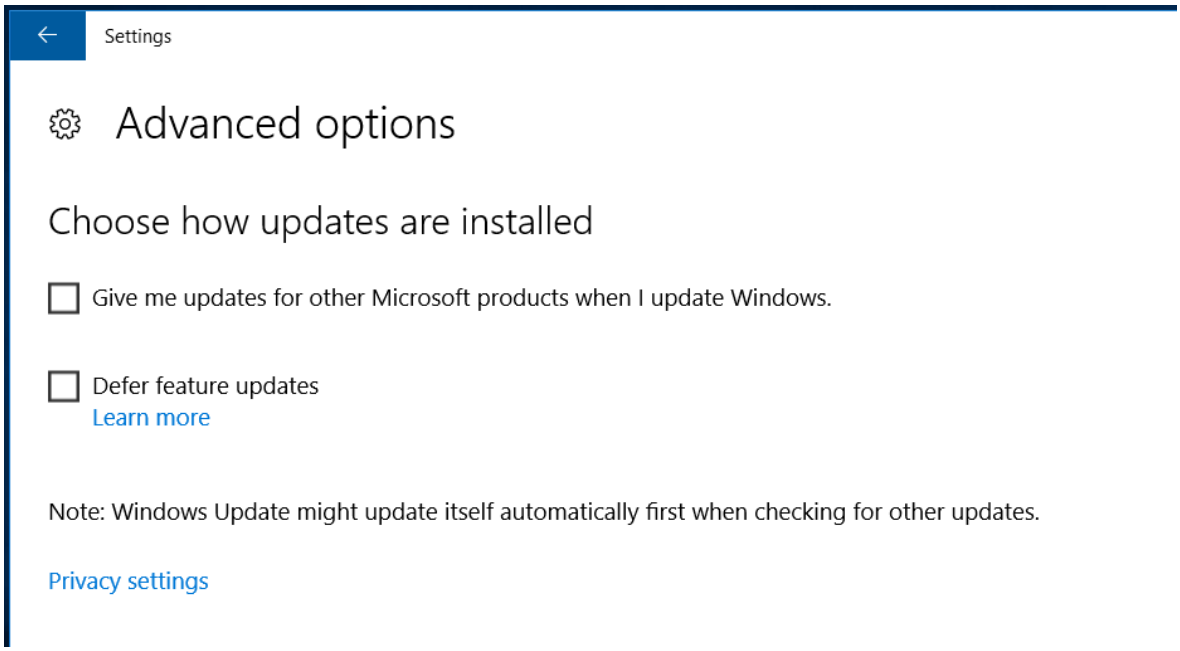
4. If Microsoft .NET Framework is not installed, you are prompted to install it when you start installation. You may be prompted to reboot after .NET Framework installation.
5. On the **Welcome** page, select the language to be used for the ATA installation screens and click **Next**.
6. Read the Microsoft Software License Terms, after accepting the terms, click the acceptance check box, then

click **Next**.

7. We recommend setting ATA to update automatically. If Windows isn't set to update automatically on your computer, you'll see the **Use Microsoft Update to help keep your computer secure and up to date** screen.



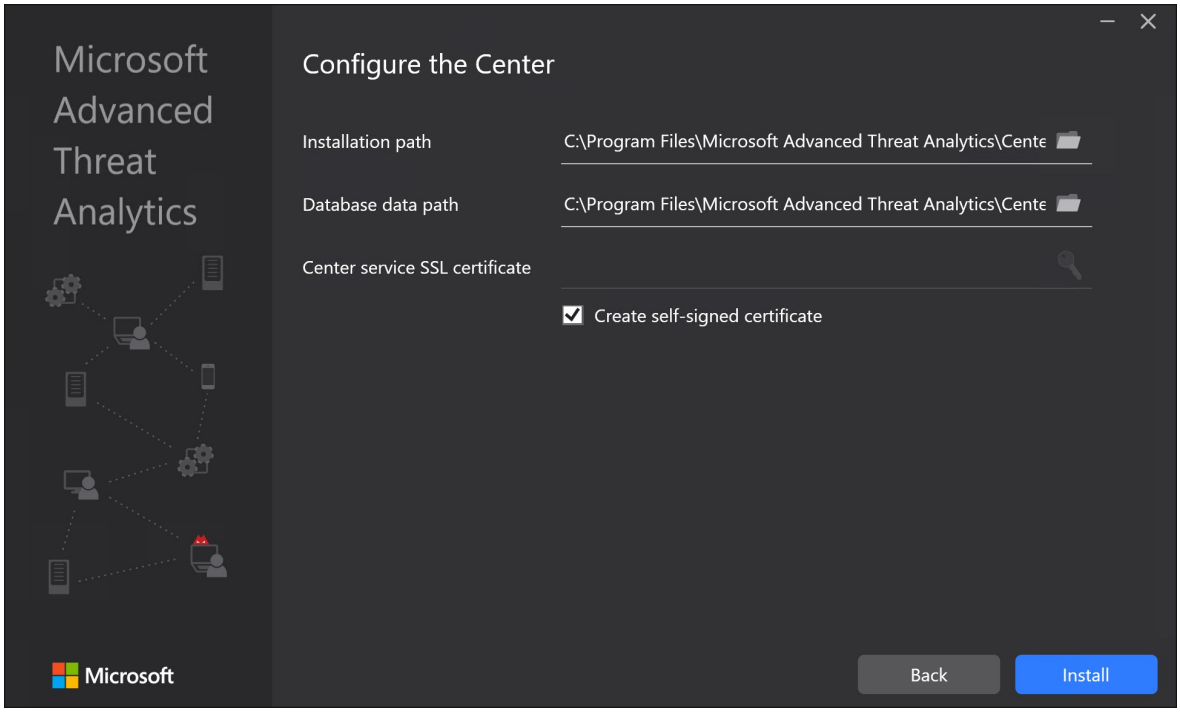
8. Select **Use Microsoft Update when I check for updates (recommended)**. This adjusts the Windows settings to enable updates for other Microsoft products (including ATA).



9. On the **Configure the Center** page, enter the following information based on your environment:

FIELD	DESCRIPTION	COMMENTS
Installation Path	This is the location where the ATA Center is installed. By default this is %programfiles%\Microsoft Advanced Threat Analytics\Center	Leave the default value

FIELD	DESCRIPTION	COMMENTS
Database Data Path	This is the location where the MongoDB database files are located. By default this is %programfiles%\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\data	Change the location to a place where you have room to grow based on your sizing. **Note:** • In production environments, you should use a drive that has enough space based on capacity planning. • For large deployments the database should be on a separate physical disk. See ATA capacity planning for sizing information.
Center Service SSL Certificate	This is the certificate that is used by the ATA Console and ATA Center service.	Click the key icon to select an installed certificate or use the checkbox to create a self-signed certificate.



> **NOTE**
> Make sure to pay attention to health alerts regarding the Center Service SSL Certificate status and expiration warnings. If the certificate expires, you'll need to completely re-deploy ATA.

10. Click **Install** to install the ATA Center and its components.
    The following components are installed and configured during the installation of ATA Center:
    - ATA Center service
    - MongoDB
    - Custom Performance Monitor data collection set
    - Self-signed certificates (if selected during the installation)
11. When the installation is complete, click **Launch** to open the ATA Console and complete setup from the

Configuration page. The **General** settings page will open automatically to continue the configuration and the deployment of the ATA Gateways. Because you are logging into the site using an IP address, you receive a warning related to the certificate, this is normal and you should click **Continue to this website**.

Validate installation

1. Check if the service **Microsoft Advanced Threat Analytics Center**, is running.
2. On the desktop, click the **Microsoft Advanced Threat Analytics** shortcut to connect to the ATA Console. Log in with the user credentials you used to install the ATA Center.

Set anti-virus exclusions

After installing the ATA Center, exclude the MongoDB database directory from being continuously scanned by your anti-virus application. The default location in the database is: **C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\data**.

Make sure to also exclude the following folders and processes from AV scanning:

Folders
C:\Program Files\Microsoft Advanced Threat Analytics\Center\ParentKerberosAsBloomFilters
C:\Program Files\Microsoft Advanced Threat Analytics\Center\ParentKerberosTgsBloomFilters
C:\Program Files\Microsoft Advanced Threat Analytics\Center\Backup
C:\Program Files\Microsoft Advanced Threat Analytics\Center\Logs

Processes
mongod.exe
Microsoft.Tri.Center.exe

If you installed ATA in different directory, make sure to change the folder paths according to your installation.

« PRE-INSTALL | STEP 2 »

Related Videos

- Choosing the right ATA Gateway type
- ATA Deployment Overview

See Also

- ATA POC deployment guide
- ATA sizing tool
- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

Install ATA - Step 2

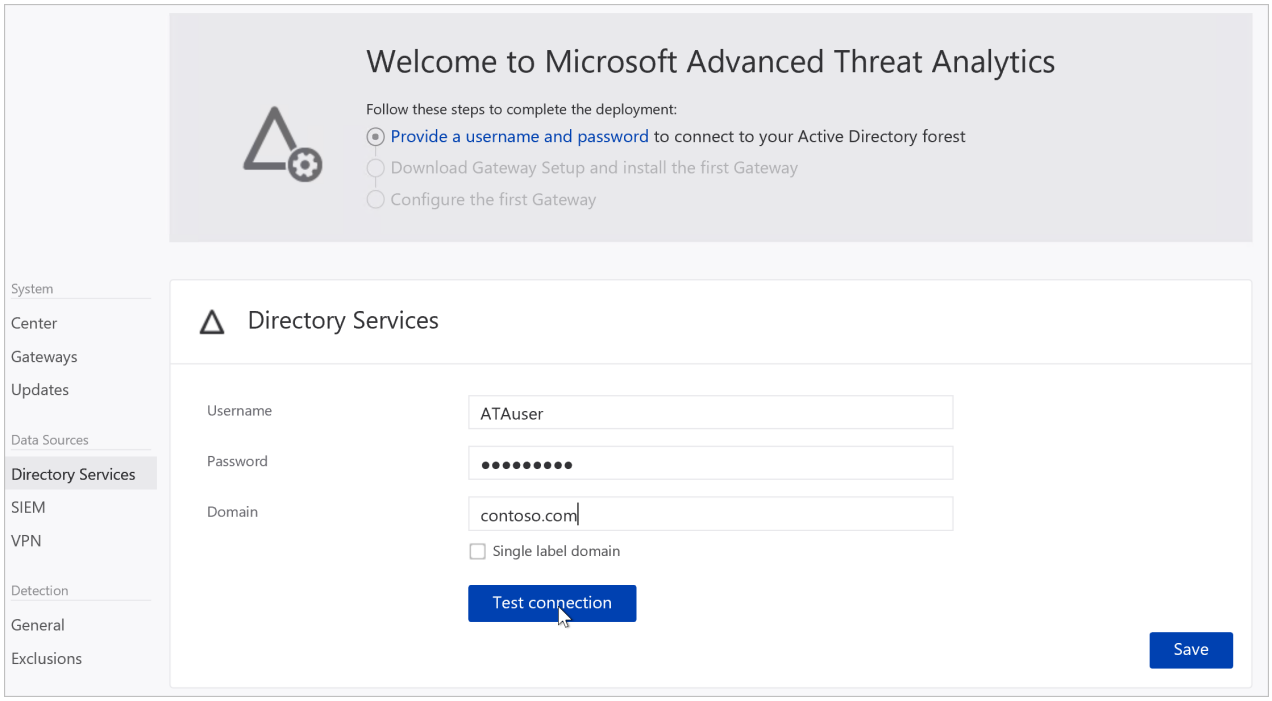
7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

« STEP 1 STEP 3 »

Step 2. Provide a Username and Password to connect to your Active Directory Forest

The first time you open the ATA Console, the following screen appears:

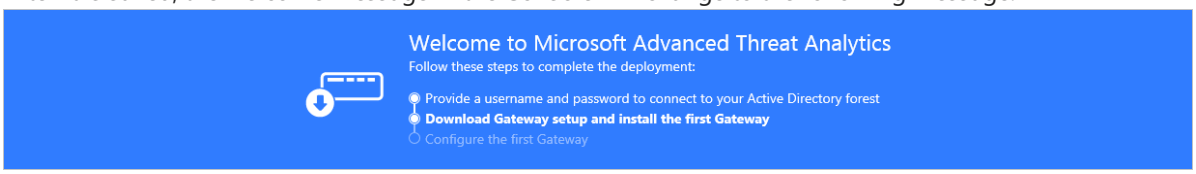


1. Enter the following information and click **Save**:

FIELD	COMMENTS
Username (required)	Enter the read-only user name, for example: **ATAuser**. **Note:** Do **not** use the UPN format for your username.
Password (required)	Enter the password for the read-only user, for example: **Pencil1**.
Domain (required)	Enter the domain for the read-only user, for example, **contoso.com**. **Note:** It is important that you enter the complete FQDN of the domain where the user is located. For example, if the user's account is in domain corp.contoso.com, you need to enter `corp.contoso.com` not contoso.com

2. You can click **Test connection** to test connectivity to the domain and check that the credentials supplied provide access. This works if the ATA Center has connectivity to the domain.

   After it is saved, the welcome message in the Console will change to the following message:



3. In the Console, click **Download Gateway setup and install the first Gateway** to continue.

« STEP 1 STEP 3 »

See Also

Related Videos

- ATA Deployment Overview
- Choosing the right ATA Gateway type

See Also

- ATA POC deployment guide
- ATA sizing tool
- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

Install ATA - Step 3

7/20/2020 • 2 minutes to read • Edit Online

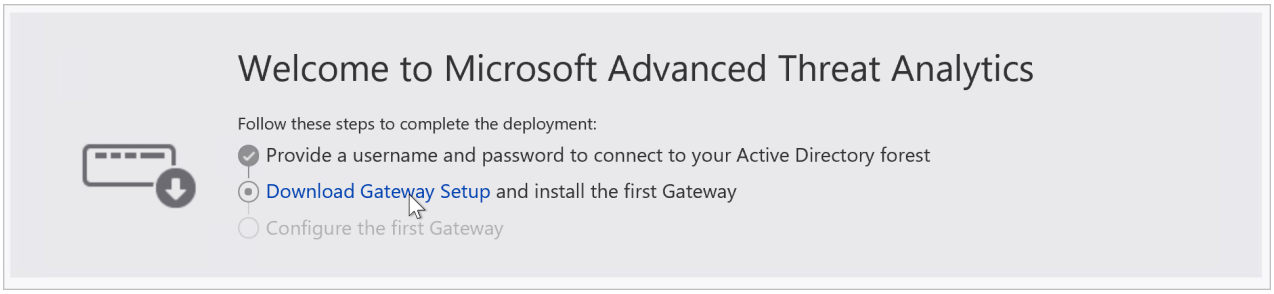
Applies to: Advanced Threat Analytics version 1.9

« STEP 2 STEP 4 »

Step 3. Download the ATA Gateway setup package

After configuring the domain connectivity settings, you can download the ATA Gateway setup package. The ATA Gateway can be installed on a dedicated server or on a domain controller. If you install it on a domain controller, it is installed as an ATA Lightweight Gateway. For more information on the ATA Lightweight Gateway, see ATA Architecture.

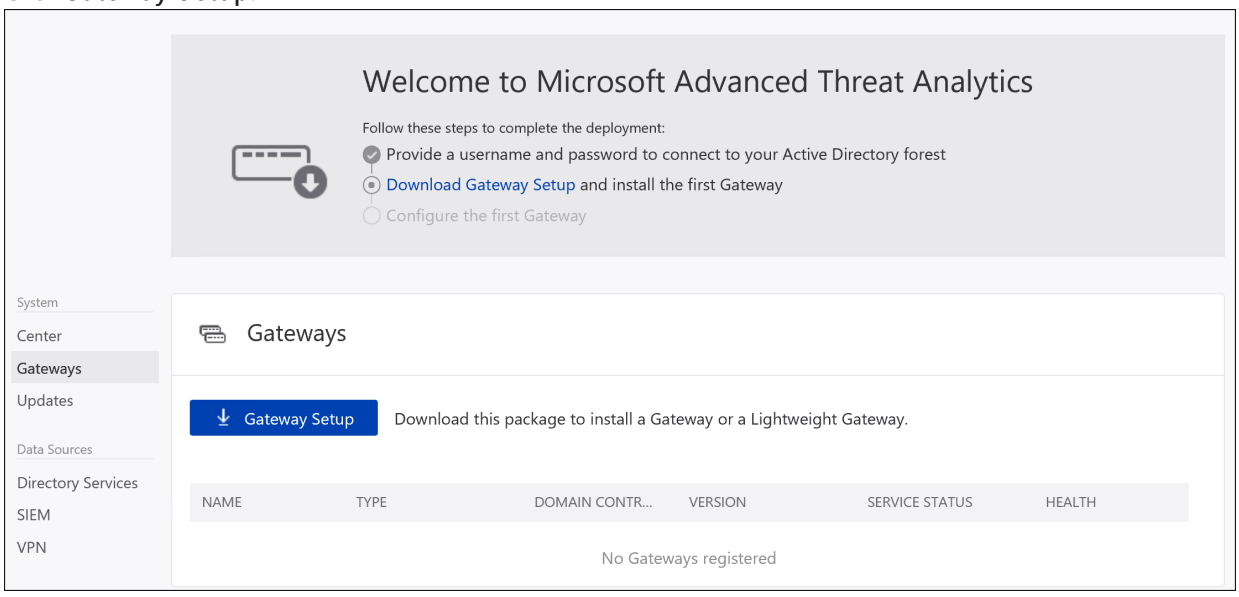
Click **Download Gateway Setup** in the list of steps at the top of the page to go to the **Gateways** page.



NOTE

To reach the Gateway configuration screen later, click the **settings icon** (upper right corner) and select **Configuration**, then, under **System**, click **Gateways**.

1. Click **Gateway Setup**.



2. Save the package locally.

3. Copy the package to the dedicated server or domain controller onto which you are installing the ATA Gateway. Alternatively, you can open the ATA Console from the dedicated server or domain controller and skip this step.

The zip file includes the following files:

- ATA Gateway installer
- Configuration setting file with the required information to connect to the ATA Center

« STEP 2 STEP 4 »

Related Videos

- ATA Deployment Overview
- Choosing the right ATA Gateway type

See Also

- ATA POC deployment guide
- ATA sizing tool
- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

Install ATA - Step 4

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

« STEP 3 STEP 5 »

Step 4. Install the ATA Gateway

Before installing the ATA Gateway on a dedicated server, validate that port mirroring is properly configured and that the ATA Gateway can see traffic to and from the domain controllers. For more information, see Validate port mirroring.

IMPORTANT

Make sure that KB2919355 has been installed. Run the following PowerShell cmdlet to check if the hotfix is installed:

```
Get-HotFix -Id kb2919355
```

Perform the following steps on the ATA Gateway server.

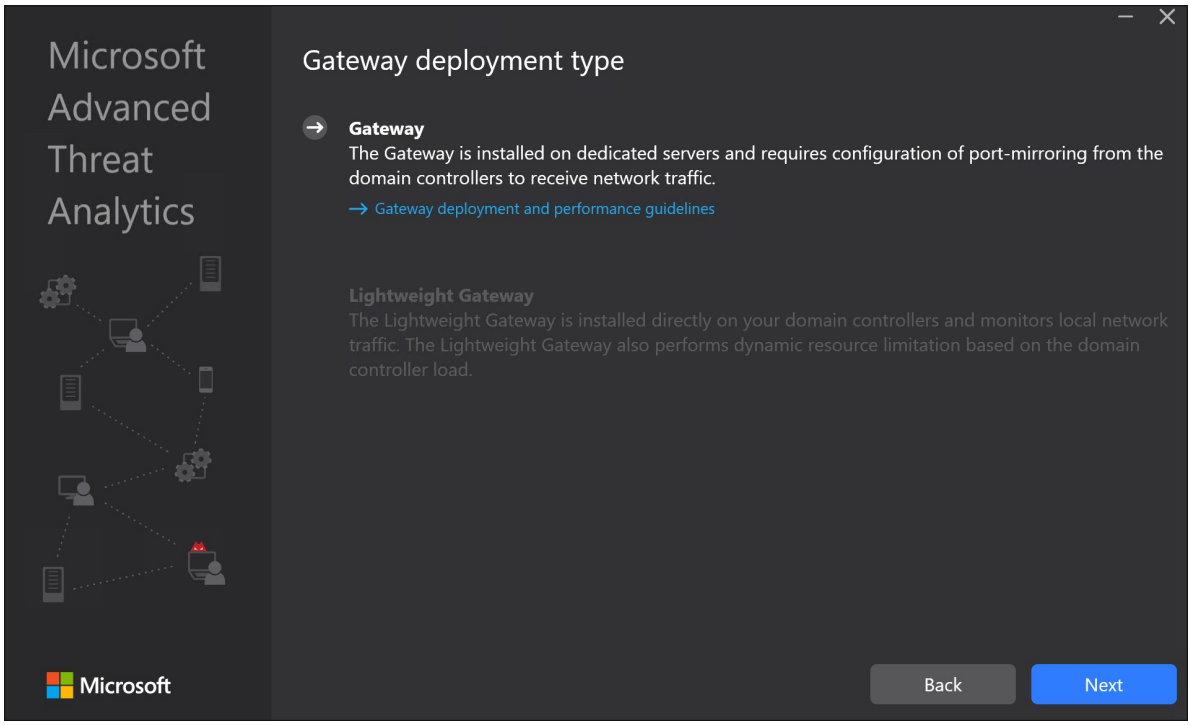
1. Extract the files from the zip file.

   NOTE

   Installing directly from the zip file fails.

2. Run **Microsoft ATA Gateway Setup.exe** and follow the setup wizard.
3. On the **Welcome** page, select your language and click **Next**.
4. The installation wizard automatically checks if the server is a domain controller or a dedicated server. If it is a domain controller, the ATA Lightweight Gateway is installed, if it is a dedicated server, the ATA Gateway is installed.

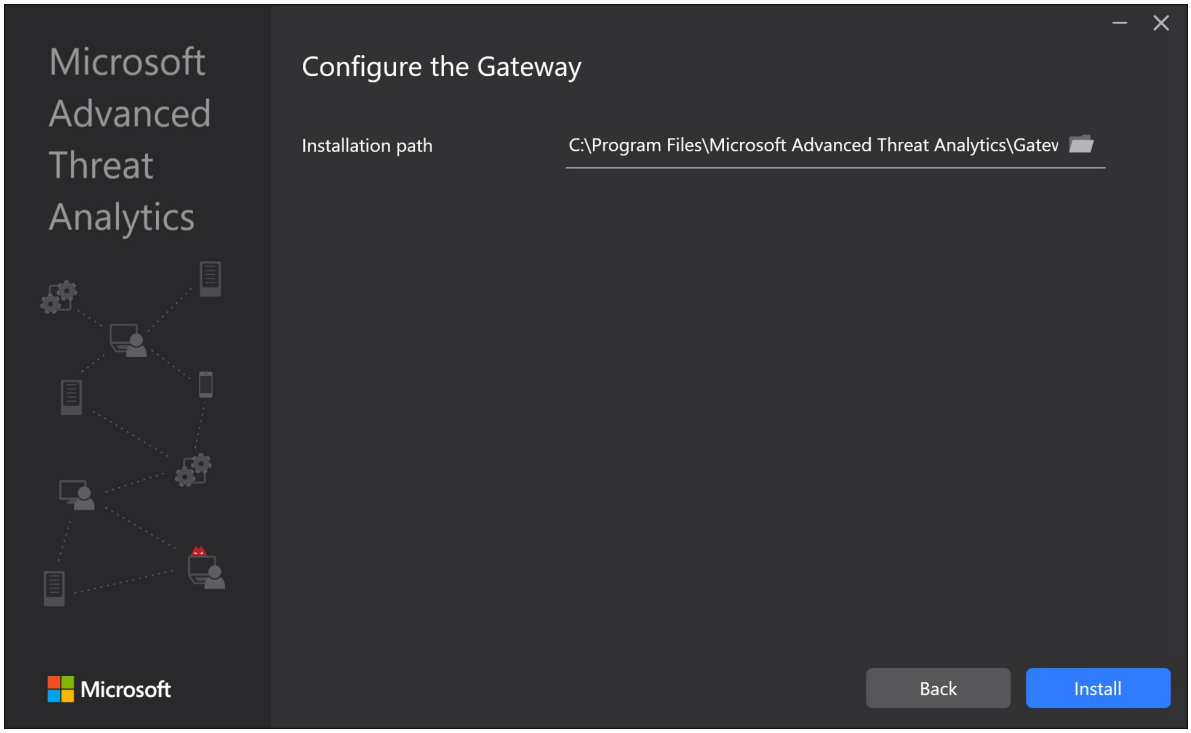
   For example, for an ATA Gateway, the following screen is displayed to let you know that an ATA Gateway will be installed on your dedicated server:



Click **Next**.

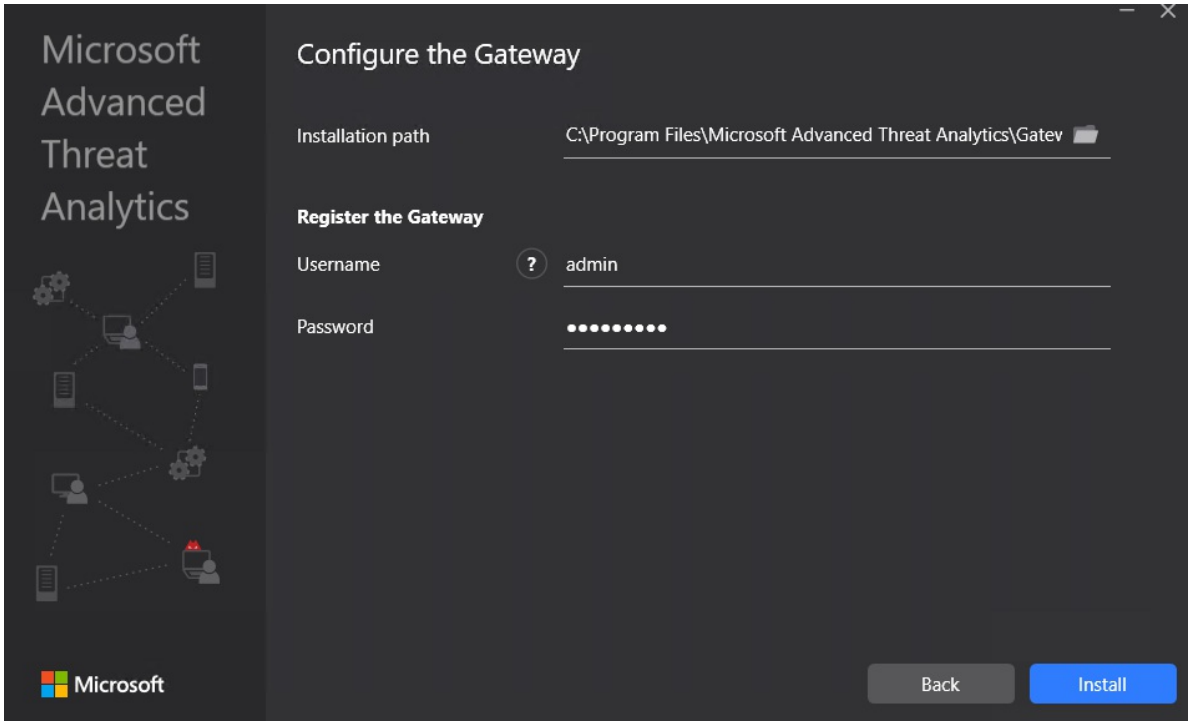
> **NOTE**
>
> If the domain controller or dedicated server does not meet the minimum hardware requirements for the installation, you receive a warning. This does not prevent you from clicking **Next** and proceeding with installation. This might be the right option for installation of ATA in a small lab test environment in which you don't need as much room for data storage. For production environments, it is highly recommended to work with ATA's capacity planning guide to make sure your domain controllers or dedicated servers meet the necessary requirements.

5. Under **Configure the Gateway**, enter the following information based on your environment:



NOTE

When you deploy the ATA Gateway, you do not have to provide credentials. If the ATA Gateway installation fails to retrieve your credentials using single sign-on (for example, this may happen if the ATA Center is not in the domain, if the ATA Gateway isn't in the domain, you do not have ATA admin credentials), you are prompted to provide credentials, as in the following screen:



- Installation Path: This is the location where the ATA Gateway is installed. By default this is %programfiles%\Microsoft Advanced Threat Analytics\Gateway. Leave the default value.

6. Click **Install**. The following components are installed and configured during the installation of the ATA Gateway:

   - KB 3047154 (for Windows Server 2012 R2 only)

     IMPORTANT

     - Do not install KB 3047154 on a virtualization host (the host that is running the virtualization, it is fine to run it on a virtual machine). This may cause port mirroring to stop working properly.
     - Do not install Message Analyzer, Wireshark, or other network capture software on the ATA Gateway. If you need to capture network traffic, install and use Microsoft Network Monitor 3.4.

   - ATA Gateway service
   - Microsoft Visual C++ 2013 Redistributable
   - Custom Performance Monitor data collection set

7. After the installation completes, for the ATA Gateway, click **Launch** to open your browser and log in to the ATA Console, for the ATA Lightweight Gateway, click **Finish**.

« STEP 3 STEP 5 »

Related Videos

- ATA Deployment Overview
- Choosing the right ATA Gateway type

See Also

- ATA POC deployment guide
- ATA sizing tool
- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

Install ATA - Step 5

7/20/2020 • 3 minutes to read • Edit Online

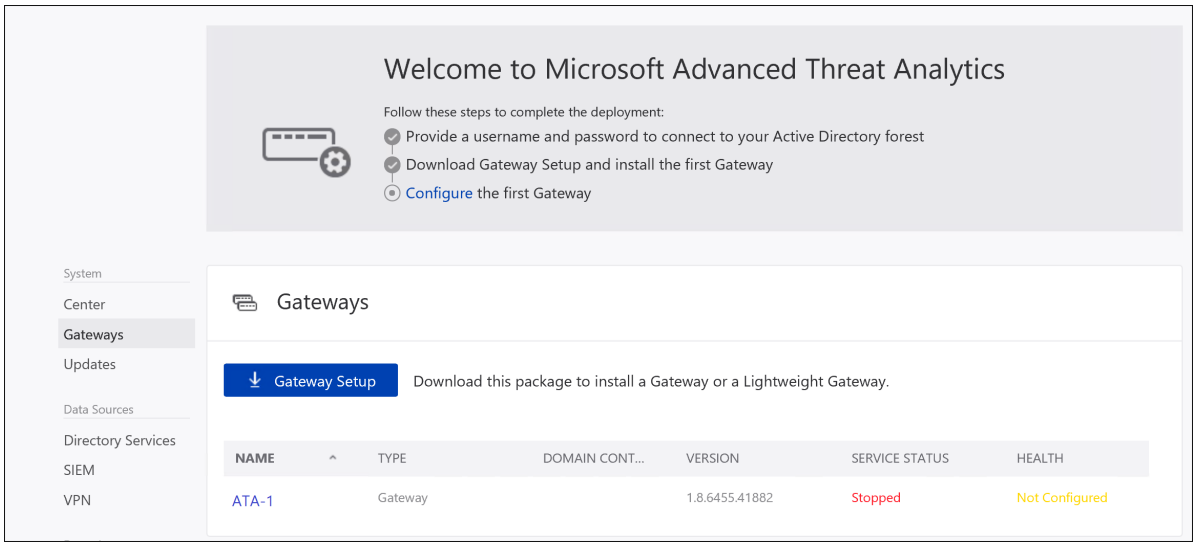
Applies to: Advanced Threat Analytics version 1.9

« STEP 4 STEP 6 »

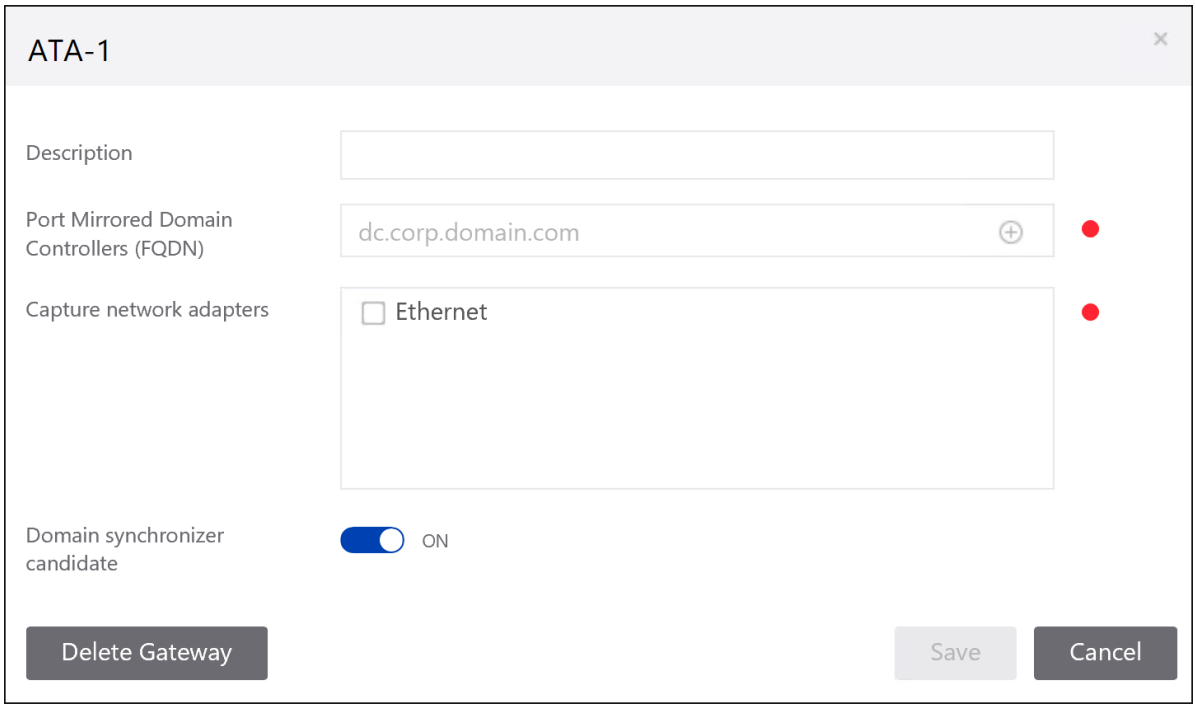
Step 5. Configure the ATA Gateway settings

After the ATA Gateway was installed, perform the following steps to configure the settings for the ATA Gateway.

1. In the ATA Console, go to **Configuration** and, under **System**, select **Gateways**.



2. Click on the Gateway you want to configure and enter the following information:



- **Description**: Enter a description for the ATA Gateway (optional).
- **Port Mirrored Domain Controllers (FQDN)** (required for the ATA Gateway, this cannot be changed for the ATA Lightweight Gateway): Enter the complete FQDN of your domain controller and click the plus sign to add it to the list. For example, **dc01.contoso.com**

The following information applies to the servers you enter in the **Domain Controllers** list:

- All domain controllers whose traffic is being monitored via port mirroring by the ATA Gateway must be listed in the **Domain Controllers** list. If a domain controller is not listed in the **Domain Controllers** list, detection of suspicious activities might not function as expected.
- At least one domain controller in the list should be a global catalog. This enables ATA to resolve computer and user objects in other domains in the forest.
- **Capture Network adapters** (required):
- For an ATA Gateway on a dedicated server, select the network adapters that are configured as the destination mirror port. These receive the mirrored domain controller traffic.
- For an ATA Lightweight Gateway, this should be all the network adapters that are used for communication with other computers in your organization.
- **Domain synchronizer candidate**: Any ATA Gateway set to be a domain synchronizer candidate can be responsible for synchronization between ATA and your Active Directory domain. Depending on the size of the domain, the initial synchronization might take some time and is resource-intensive. By default, only ATA Gateways are set as Domain synchronizer candidates. It is recommended that you disable any remote site ATA Gateways from being Domain synchronizer candidates. If your domain controller is read-only, do not set it as a Domain synchronizer candidate. For more information, see ATA architecture.

> **NOTE**
> It will take a few minutes for the ATA Gateway service to start the first time after installation because it builds the cache of the network capture parsers. The configuration changes are applied to the ATA Gateway on the next scheduled sync between the ATA Gateway and the ATA Center.

3. Optionally, you can set the Syslog listener and Windows Event Forwarding Collection.

4. Enable **Update ATA Gateway automatically** so that in upcoming version releases when you update the ATA Center, this ATA Gateway is automatically updated.

5. Click **Save**.

Validate installations

To validate that the ATA Gateway has been successfully deployed, check the following steps:

1. Check that the service named **Microsoft Advanced Threat Analytics Gateway** is running. After you save the ATA Gateway settings, it might take a few minutes for the service to start.

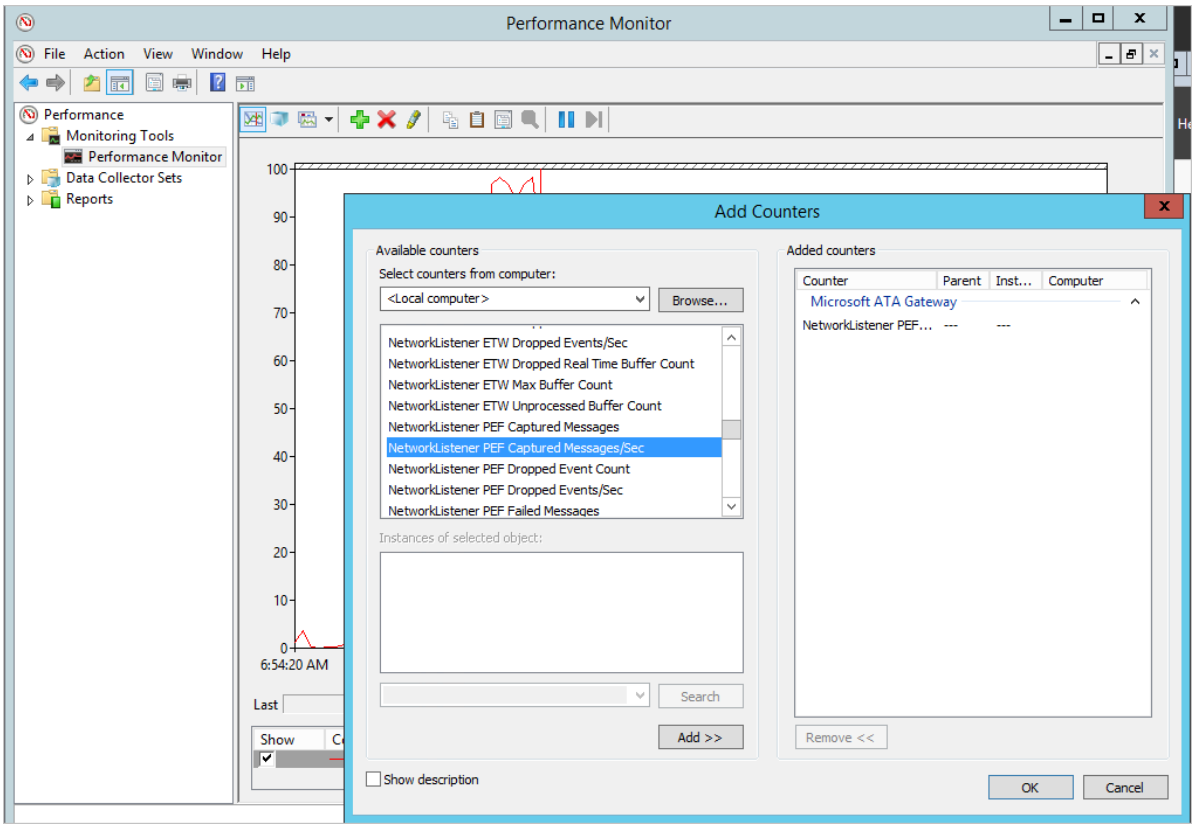
2. If the service does not start, review the "Microsoft.Tri.Gateway-Errors.log" file located in the following default folder, "%programfiles%\Microsoft Advanced Threat Analytics\Gateway\Logs" and Check ATA Troubleshooting for help.

3. If this is the first ATA Gateway installed, after a few minutes, log into the ATA Console and open the notification pane by swiping the right side of the screen open. You should see a list of **Entities Recently Learned** in the notification bar on the right side of the console.

4. On the desktop, click the **Microsoft Advanced Threat Analytics** shortcut to connect to the ATA Console. Log in with the same user credentials that you used to install the ATA Center.

5. In the console, search for something in the search bar, such as a user or a group on your domain.

6. Open Performance Monitor. In the Performance tree, click on **Performance Monitor** and then click the plus icon to **Add a Counter**. Expand **Microsoft ATA Gateway** and scroll down to **Network Listener PEF Captured Messages/Sec** and add it. Then, make sure you see activity on the graph.



Set anti-virus exclusions

After installing the ATA Gateway, exclude the ATA directory from being continuously scanned by your anti-virus application. The default location in the database is: **C:\Program Files\Microsoft Advanced Threat Analytics**.

Make sure to also exclude the following processes from AV scanning:

Processes
Microsoft.Tri.Gateway.exe
Microsoft.Tri.Gateway.Updater.exe

If you installed ATA in different directory, make sure to change the folder paths according to your installation.

« STEP 4 STEP 6 »

Related Videos

- ATA Deployment Overview
- Choosing the right ATA Gateway type

See Also

- ATA POC deployment guide
- ATA sizing tool
- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

Install ATA - Step 6

7/20/2020 • 5 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

« STEP 5 STEP 7 »

Step 6. Configure event collection

Configure Event Collection

To enhance detection capabilities, ATA needs the following Windows events: 4776, 4732, 4733, 4728, 4729, 4756, 4757, and 7045. These Windows events are either read automatically by the ATA Lightweight Gateway or in case the ATA Lightweight Gateway is not deployed, they can be forwarded to the ATA Gateway in one of two ways, either by configuring the ATA Gateway to listen for SIEM events or by Configuring Windows Event Forwarding.

> **NOTE**
> For ATA versions 1.8 and higher, Windows event collection configuration is no longer necessary for ATA Lightweight Gateways. The ATA Lightweight Gateway now read events locally, without the need to configure event forwarding.

In addition to collecting and analyzing network traffic to and from the domain controllers, ATA can use Windows events to further enhance detections. It uses event 4776 for NTLM, which enhances various detections and events 4732, 4733, 4728, 4729, 4756, and 4757 for enhancing detection of sensitive group modifications. This can be received from your SIEM or by setting Windows Event Forwarding from your domain controller. Events collected provide ATA with additional information that is not available via the domain controller network traffic.

SIEM/Syslog

For ATA to be able to consume data from a Syslog server, you need to perform the following steps:

- Configure your ATA Gateway servers to listen to and accept events forwarded from the SIEM/Syslog server.

> **NOTE**
> ATA only listens on IPv4 and not IPv6.
>
> - Configure your SIEM/Syslog server to forward specific events to the ATA Gateway.

> **IMPORTANT**
> - Do not forward all the Syslog data to the ATA Gateway.
> - ATA supports UDP traffic from the SIEM/Syslog server.

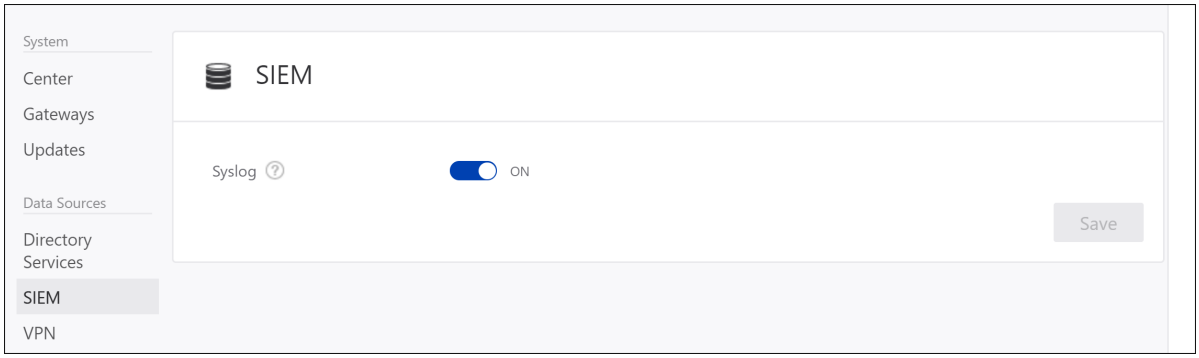
Refer to your SIEM/Syslog server's product documentation for information on how to configure forwarding of specific events to another server.

NOTE

If you do not use a SIEM/Syslog server, you can configure your Windows domain controllers to forward Windows Event ID 4776 to be collected and analyzed by ATA. Windows Event ID 4776 provides data regarding NTLM authentications.

Configuring the ATA Gateway to listen for SIEM events

1. In ATA Configuration, under **Data sources** click **SIEM** and turn on **Syslog** and click **Save**.



2. Configure your SIEM or Syslog server to forward Windows Event ID 4776 to the IP address of one of the ATA Gateways. For additional information on configuring your SIEM, see your SIEM online help or technical support options for specific formatting requirements for each SIEM server.

ATA supports SIEM events in the following formats:

RSA Security Analytics

<Syslog Header>RsaSA\n2015-May-19 09:07:09\n4776\nMicrosoft-Windows-Security-Auditing\nSecurity\XXXXX.subDomain.domain.org.il\nYYYYY$\nMMMMM \n0x0

- Syslog header is optional.
- "\n" character separator is required between all fields.
- The fields, in order, are:
    1. RsaSA constant (must appear).
    2. The timestamp of the actual event (make sure it's not the timestamp of the arrival to the EM or when it's sent to ATA). Preferably in milliseconds accuracy, this is important.
    3. The Windows event ID
    4. The Windows event provider name
    5. The Windows event log name
    6. The name of the computer receiving the event (the DC in this case)
    7. The name of the user authenticating
    8. The name of the source host name
    9. The result code of the NTLM
- The order is important and nothing else should be included in the message.

MicroFocus ArcSight

CEF:0|Microsoft|Microsoft Windows||Microsoft-Windows-Security-Auditing:4776|The domain controller attempted to validate the credentials for an account.|Low| externalId=4776 cat=Security rt=1426218619000 shost=KKKKKK dhost=YYYYYY.subDomain.domain.com duser=XXXXXX cs2=Security cs3=Microsoft-Windows-Security-Auditing cs4=0x0 cs3Label=EventSource cs4Label=Reason or Error Code

- Must comply with the protocol definition.
- No syslog header.

- The header part (the part that's separated by a pipe) must exist (as stated in the protocol).
- The following keys in the *Extension* part must be present in the event:
  - externalId = the Windows event ID
  - rt = the timestamp of the actual event (make sure it's not the timestamp of the arrival to the SIEM or when it's sent to ATA). Preferably in milliseconds accuracy, this is important.
  - cat = the Windows event log name
  - shost = the source host name
  - dhost = the computer receiving the event (the DC in this case)
  - duser = the user authenticating
- The order is not important for the *Extension* part
- There must be a custom key and keyLable for these two fields:
  - "EventSource"
  - "Reason or Error Code" = The result code of the NTLM

Splunk

<Syslog Header>\r\nEventCode=4776\r\nLogfile=Security\r\nSourceName=Microsoft-Windows-Security-Auditing\r\nTimeGenerated=20150310132717.784882-000\r\ComputerName=YYYYY\r\nMessage=

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Logon Account: Administrator

Source Workstation: SIEM

Error Code: 0x0

- Syslog header is optional.
- There's a "\r\n" character separator between all required fields.
- The fields are in key=value format.
- The following keys must exist and have a value:
  - EventCode = the Windows event ID
  - Logfile = the Windows event log name
  - SourceName = The Windows event provider name
  - TimeGenerated = the timestamp of the actual event (make sure it's not the timestamp of the arrival to the SIEM or when it's sent to ATA). The format should match yyyyMMddHHmmss.FFFFFF, preferably in milliseconds accuracy, this is important.
  - ComputerName = the source host name
  - Message = the original event text from the Windows event
- The Message Key and value MUST be last.
- The order is not important for the key=value pairs.

QRadar

QRadar enables event collection via an agent. If the data is gathered using an agent, the time format is gathered without millisecond data. Because ATA necessitates millisecond data, it is necessary to set QRadar to use agentless Windows event collection. For more information, see http://www-01.ibm.com/support/docview.wss?uid=swg21700170.

```
<13>Feb 11 00:00:00 %IPADDRESS% AgentDevice=WindowsLog AgentLogFile=Security Source=Microsoft-Windows-
Security-Auditing Computer=%FQDN% User= Domain= EventID=4776 EventIDCode=4776 EventType=8 EventCategory=14336
RecordNumber=1961417 TimeGenerated=1456144380009 TimeWritten=1456144380009 Message=The computer attempted to
validate the credentials for an account. Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon
Account: Administrator Source Workstation: HOSTNAME Error Code: 0x0
```

The fields needed are:

- The agent type for the collection
- The Windows event log provider name
- The Windows event log source
- The DC fully qualified domain name
- The Windows event ID

TimeGenerated is the timestamp of the actual event (make sure it's not the timestamp of the arrival to the SIEM or when it's sent to ATA). The format should match yyyyMMddHHmmss.FFFFFF, preferably in milliseconds accuracy, this is important.

Message is the original event text from the Windows event

Make sure to have \t between the key=value pairs.

> **NOTE**
> Using WinCollect for Windows event collection is not supported.

« STEP 5 STEP 7 »

Related Videos

- ATA Deployment Overview
- Choosing the right ATA Gateway type

See Also

- ATA POC deployment guide
- ATA sizing tool
- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

Install ATA - Step 7

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

« STEP 5 STEP 8 »

Step 7. Integrate VPN

Microsoft Advanced Threat Analytics (ATA) version 1.8 and higher can collect accounting information from VPN solutions. When configured, the user's profile page includes information from the VPN connections, such as the IP addresses and locations where connections originated. This complements the investigation process by providing additional information on user activity. The call to resolve an external IP address to a location is anonymous. No personal identifier is sent in this call.

ATA integrates with your VPN solution by listening to RADIUS accounting events forwarded to the ATA Gateways. This mechanism is based on standard RADIUS Accounting (RFC 2866), and the following VPN vendors are supported:

- Microsoft
- F5
- Cisco ASA

> **IMPORTANT**
> As of September 2019, the Advanced Threat Analytics VPN geo-location service responsible for detecting VPN locations now exclusively supports TLS 1.2. Make sure your ATA Center is configured to support TLS 1.2, as versions 1.1 and 1.0 are no longer be supported.

Prerequisites

To enable VPN integration, make sure you set the following parameters:

- Open port UDP 1813 on your ATA Gateways and ATA Lightweight Gateways.
- The ATA Center must be able to access *ti.ata.azure.com* using HTTPS (port 443) so that it can query the location of incoming IP addresses.

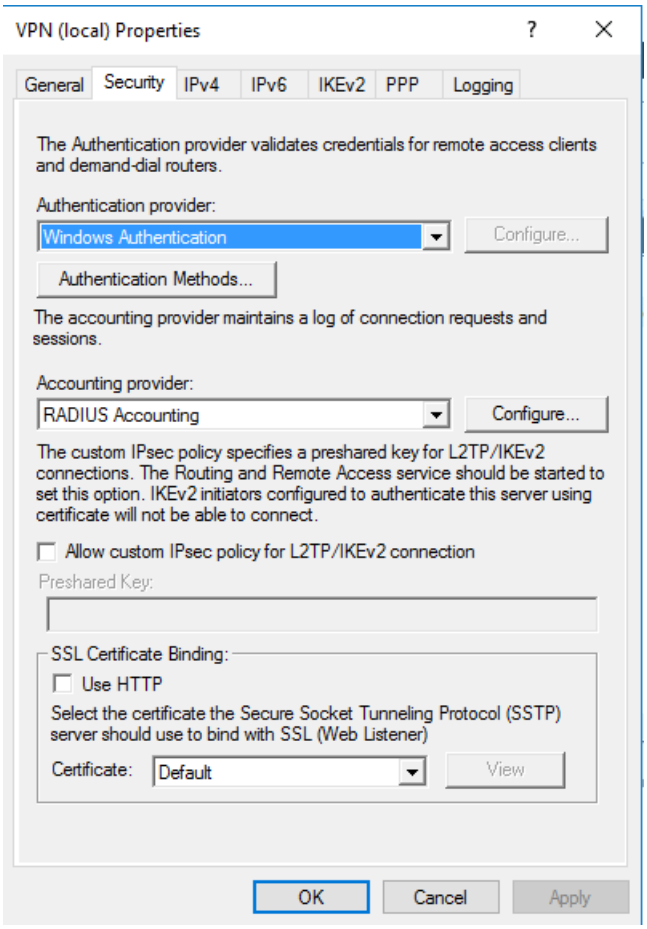
The example below uses Microsoft Routing and Remote Access Server (RRAS) to describe the VPN configuration process.

If you're using a third party VPN solution, consult their documentation for instructions on how to enable RADIUS Accounting.

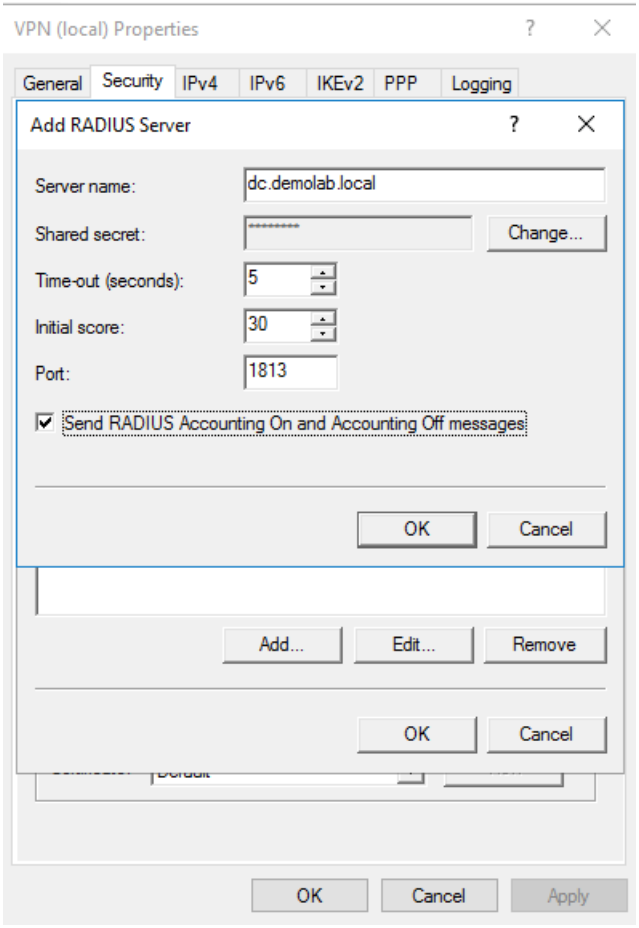
Configure RADIUS Accounting on the VPN system

Perform the following steps on your RRAS server.

1. Open the Routing and Remote Access console.
2. Right-click the server name and click **Properties**.
3. In the **Security** tab, under **Accounting provider**, select **RADIUS Accounting** and click **Configure**.



4. In the **Add RADIUS Server** window, type the **Server name** of the closest ATA Gateway or ATA Lightweight Gateway. Under **Port**, make sure the default of 1813 is configured. Click **Change** and type a new shared secret string of alphanumeric characters that you can remember. You need to fill it out later in your ATA Configuration. Check the **Send RADIUS Account On and Accounting Off messages** box and then click **OK** on all open dialog boxes.

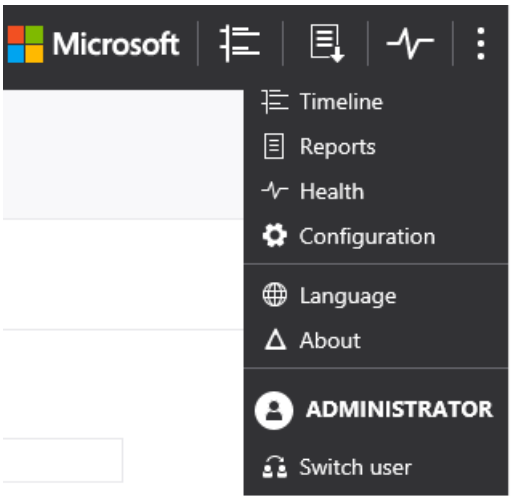


Configure VPN in ATA

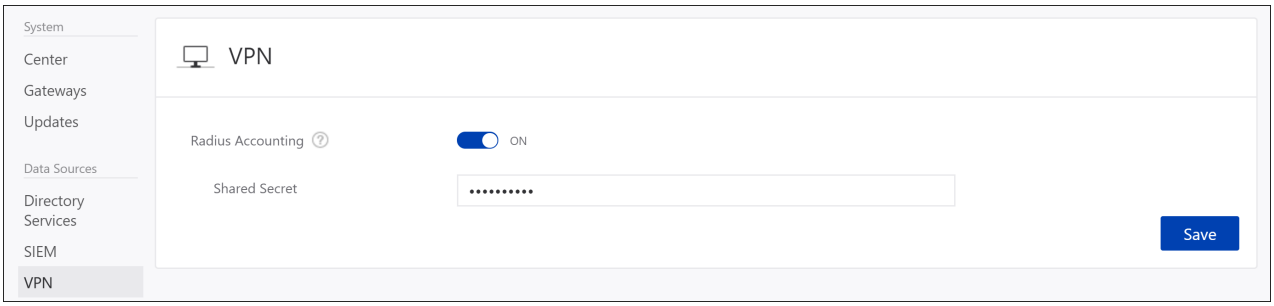
ATA collects VPN data and identifies when and where credentials are being used via VPN and integrates that data into your investigation. This provides additional information to help you investigate alerts reported by ATA.

To configure VPN data in ATA:

1. In the ATA console, open the ATA Configuration page and go to **VPN**.

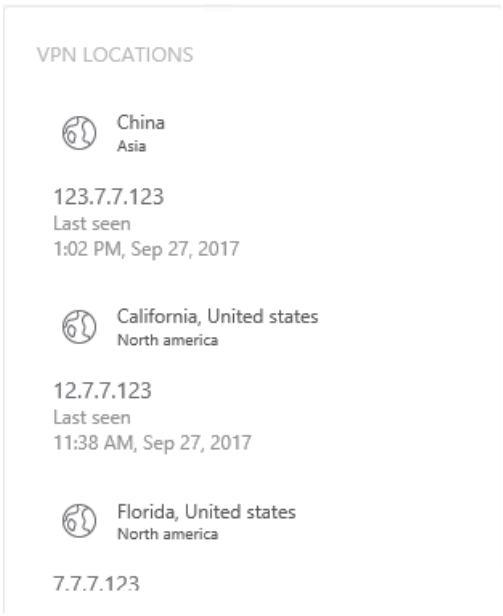


2. Turn on **Radius Accounting**, and type the **Shared Secret** you configured previously on your RRAS VPN Server. Then click **Save**.



After this is enabled, all ATA Gateways and Lightweight Gateways listen on port 1813 for RADIUS accounting events.

Your setup is complete, and you can now see VPN activity in the users' profile page:



After the ATA Gateway receives the VPN events and sends them to the ATA Center for processing, the ATA Center needs access to *ti.ata.azure.com* using HTTPS (port 443) to be able to resolve the external IP addresses in the VPN events to their geographic location.

« STEP 6 STEP 8 »

Related Videos

- ATA Deployment Overview
- Choosing the right ATA Gateway type

See Also

- ATA POC deployment guide
- ATA sizing tool
- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

Install ATA - Step 8

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

« STEP 7 STEP 9 »

Step 8. Configure IP address exclusions and Honeytoken user

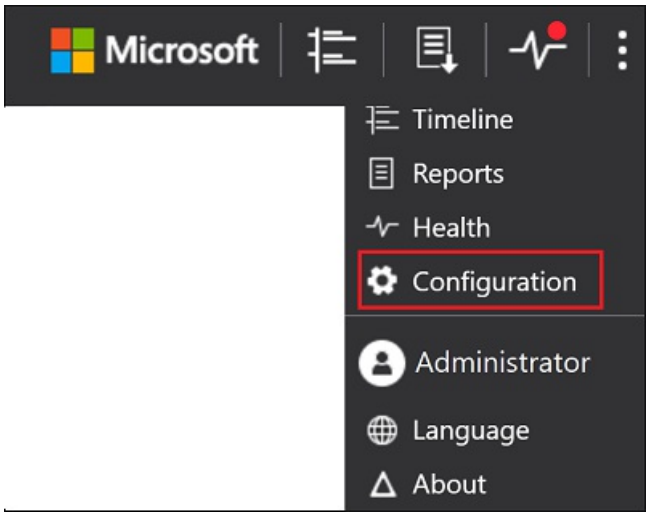
ATA enables the exclusion of specific IP addresses or users from a number of detections.

For example, a **DNS Reconnaissance exclusion** could be a security scanner that uses DNS as a scanning mechanism. The exclusion helps ATA ignore such scanners. An example of a *Pass-the-Ticket* exclusion is a NAT device.

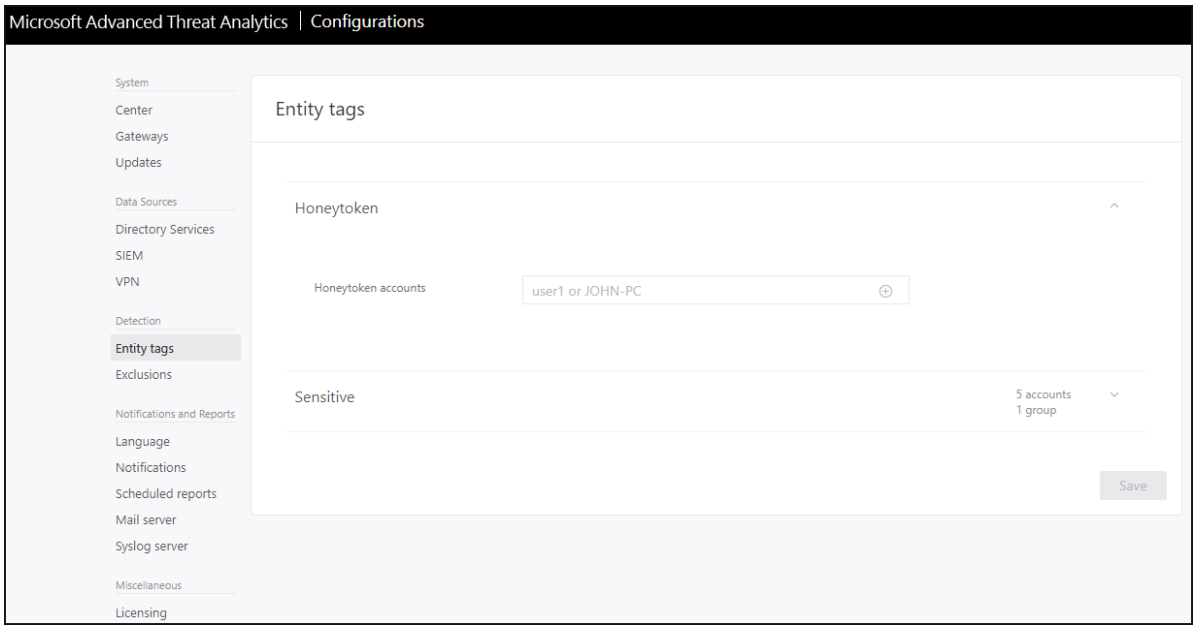
ATA also enables the configuration of a Honeytoken user, which is used as a trap for malicious actors - any authentication associated with this (normally dormant) account triggers an alert.

To configure this, follow these steps:

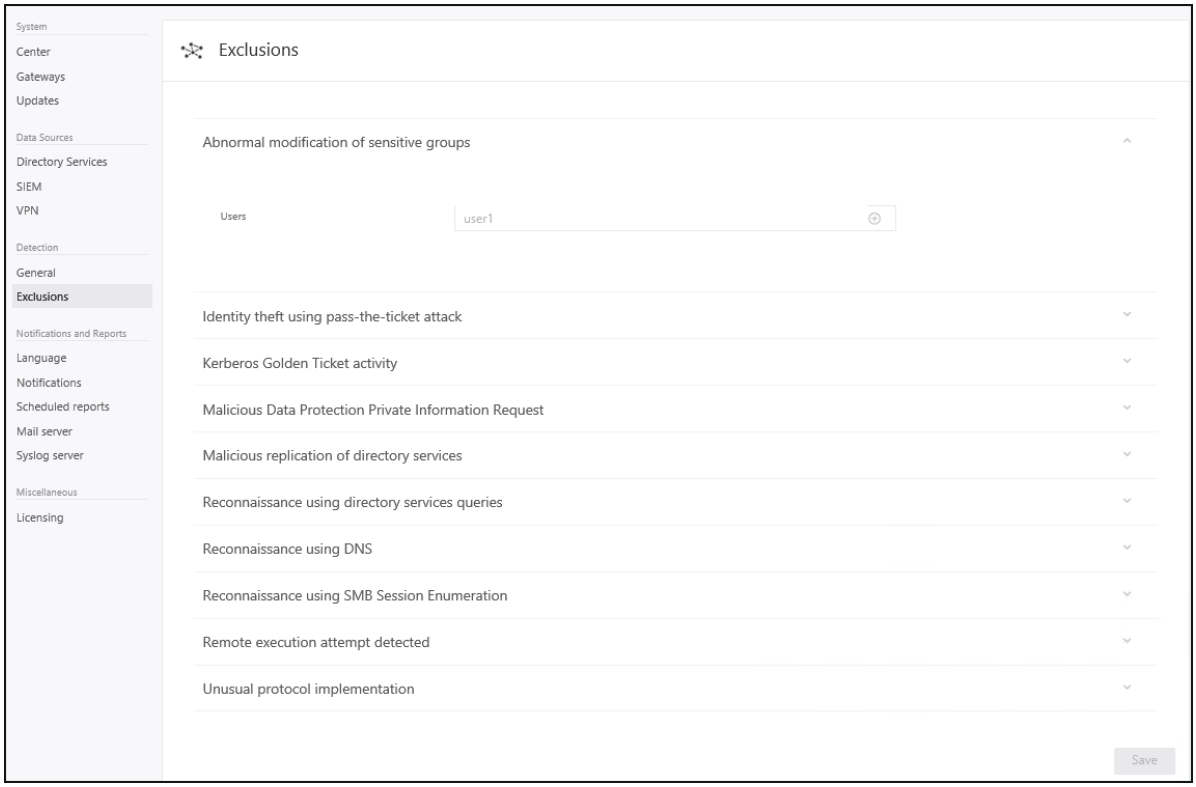
1. From the ATA Console, click on the settings icon and select **Configuration**.



2. Under **Detection**, click **Entity tags**.
3. Under **Honeytoken accounts** enter the Honeytoken account name. The Honeytoken accounts field is searchable and automatically displays entities in your network.



4. Click **Exclusions**. For each type of threat, enter a user account or IP address to be excluded from the detection of these threats and click the *plus* sign. The **Add entity** (user or computer) field is searchable and will autofill with entities in your network. For more information, see Excluding entities from detections



5. Click **Save**.

Congratulations, you have successfully deployed Microsoft Advanced Threat Analytics!

Check the attack time line to view detected suspicious activities and search for users or computers and view their profiles.

ATA starts scanning for suspicious activities immediately. Some activities, such as some of the suspicious behavior activities, is not available until ATA has had time to build behavioral profiles (minimum of three weeks).

To check that ATA is up and running and catching breaches in your network, you can check out the ATA attack simulation playbook.

« STEP 7

STEP 9 »

Related Videos

- ATA Deployment Overview
- Choosing the right ATA Gateway type

See Also

- ATA POC deployment guide
- ATA sizing tool
- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

Install ATA - Step 9

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

« STEP 8

NOTE

Before enforcing any new policy, always make sure that your environment remains secure, without impacting application compatibility by first enabling and verifying your proposed changes in audit mode.

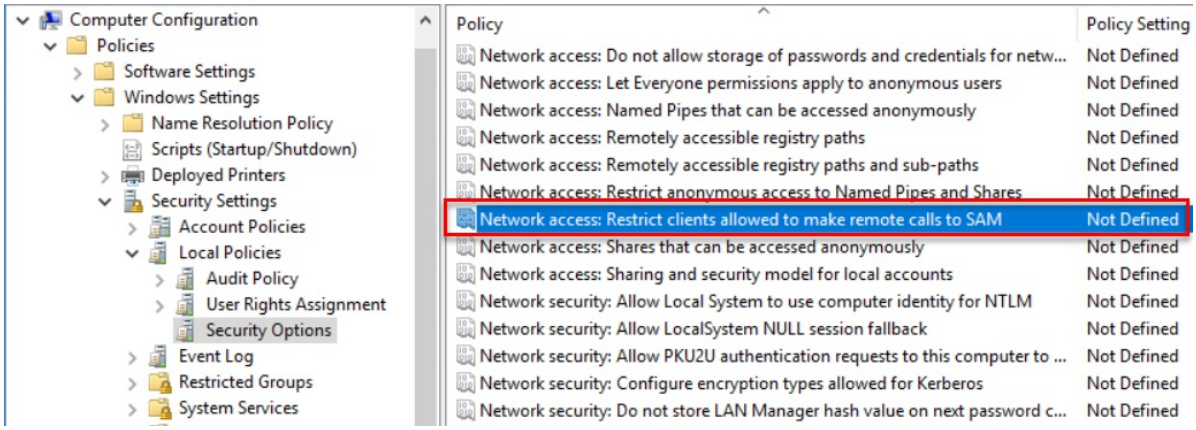
Step 9. Configure SAM-R required permissions

The lateral movement path detection relies on queries that identify local admins on specific machines. These queries are performed using the SAM-R protocol, via the ATA Service account created in Step 2. Connect to AD.

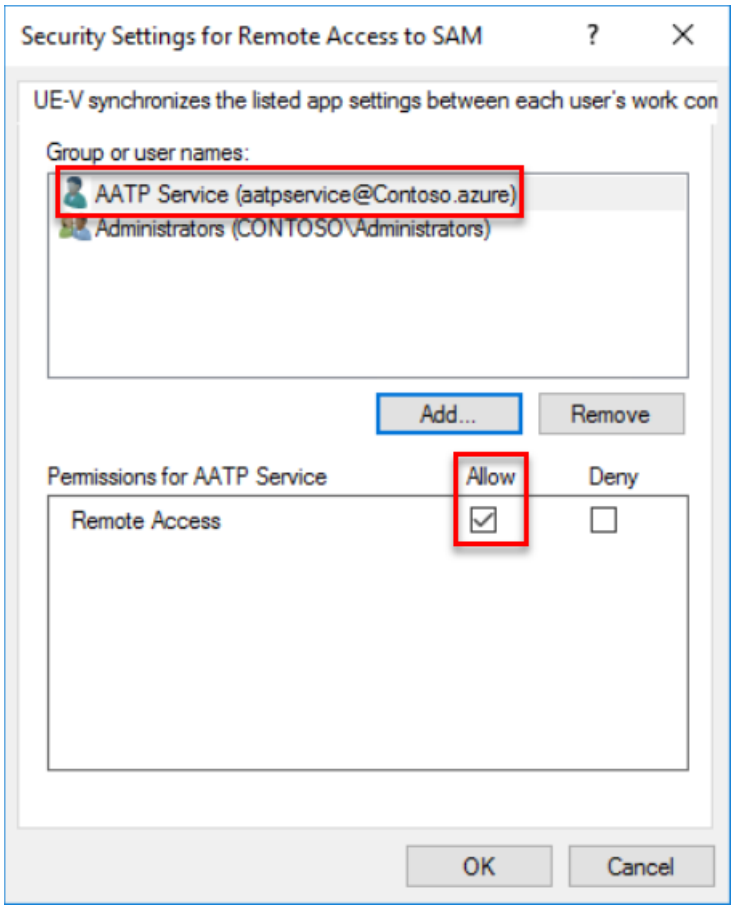
To ensure that Windows clients and servers allow the ATA service account to perform this SAM-R operation, a modification to your **Group policy** must be made that adds the ATA service account in addition to the configured accounts listed in the **Network access** policy. This group policy should be applied for every device in your organization.

1. Locate the policy:

   - Policy Name: Network access - Restrict clients allowed to make remote calls to SAM
   - Location: Computer configuration, Windows settings, Security settings, Local policies, Security options



2. Add the ATA service to the list of approved accounts able to perform this action on your modern Windows systems.



3. The **ATA Service** (the ATA service created during installation) now has the proper privileges to perform SAM-R in the environment.

For more information on SAM-R and Group Policy, see Network access: Restrict clients allowed to make remote calls to SAM.

« STEP 8

See Also

- ATA POC deployment guide
- ATA sizing tool
- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

ATA silent installation

7/20/2020 • 5 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

This article provides instructions for silently installing ATA.

Prerequisites

ATA version 1.9 requires the installation of Microsoft .NET Framework 4.6.1.

When you install or update ATA, .Net Framework 4.6.1 is automatically installed as part of the deployment of Microsoft ATA.

> **NOTE**
> The installation of .Net framework 4.6.1 may require rebooting the server. When installing ATA Gateway on Domain Controllers, consider scheduling a maintenance window for these Domain Controllers. When using ATA silent installation method, the installer is configured to automatically restart the server at the end of the installation (if necessary). Because of a Windows Installer bug, the norestart flag cannot be reliably used to make sure the server does not restart, so make sure to only run silent installation during a maintenance window.

To track the progress of the deployment, monitor ATA installer logs, which are located in **%AppData%\Local\Temp**.

Install the ATA Center

Use the following command to install the ATA Center:

Syntax:

```
"Microsoft ATA Center Setup.exe" [/quiet] [/Help] [--LicenseAccepted] [NetFrameworkCommandLineArguments="/q"]
[InstallationPath="<InstallPath>"] [DatabaseDataPath= "<DBPath>"] [CertificateThumbprint="<CertThumbprint>"]
```

Installation options:

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
Quiet	/quiet	Yes	Runs the installer displaying no UI and no prompts.
Help	/help	No	Provides help and quick reference. Displays the correct use of the setup command including a list of all options and behaviors.

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
NetFrameworkCommandLineArguments="/q"	NetFrameworkCommandLineArguments="/q"	Yes	Specifies the parameters for the .Net Framework installation. Must be set to enforce the silent installation of .Net Framework.
LicenseAccepted	--LicenseAccepted	Yes	Indicates that the license was read and approved. Must be set on silent installation.

Installation parameters:

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
InstallationPath	InstallationPath=""	No	Sets the path for the installation of ATA binaries. Default path: C:\Program Files\Microsoft Advanced Threat Analytics\Center
DatabaseDataPath	DatabaseDataPath= ""	No	Sets the path for the ATA Database data folder. Default path: C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\data
CenterCertificateThumbprint	CenterCertificateThumbprint=""	No	Sets the certificate thumbprint for the ATA Center. This Certificate is used to secure communication for ATA Gateway to the ATA Center and to validate the identity of the ATA Console website. If not set, the installation generates a self-signed certificate.

Example:

To install the ATA Center with default installation paths and user-defined certificate thumbprint:

```
"Microsoft ATA Center Setup.exe" /quiet --LicenseAccepted NetFrameworkCommandLineArguments ="/q"
CenterCertificateThumbprint= "1E2079739F624148ABDF502BF9C799FCB8C7212F"
```

Update the ATA Center

Use the following command to update the ATA Center:

Syntax:

```
"Microsoft ATA Center Setup.exe" [/quiet] [/Help] [NetFrameworkCommandLineArguments="/q"]
```

Installation options:

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
Quiet	/quiet	Yes	Runs the installer displaying no UI and no prompts.
Help	/help	No	Provides help and quick reference. Displays the correct use of the setup command including a list of all options and behaviors.
NetFrameworkCommandLineArguments="/q"	NetFrameworkCommandLineArguments="/q"	Yes	Specifies the parameters for the .Net Framework installation. Must be set to enforce the silent installation of .Net Framework.

When updating ATA, the installer automatically detects that ATA is already installed on the server, and no update installation option is required.

Examples:

To update the ATA Center silently. In large environments, the ATA Center update can take a while to complete. Monitor ATA logs to track the progress of the update.

```
"Microsoft ATA Center Setup.exe" /quiet NetFrameworkCommandLineArguments="/q"
```

Uninstall the ATA Center silently

Use the following command to perform a silent uninstall of the ATA Center:

Syntax:

```
"Microsoft ATA Center Setup.exe" [/quiet] [/Uninstall] [/Help] [--DeleteExistingDatabaseData]
```

Installation options:

NAME	SYNTAX	MANDATORY FOR SILENT UNINSTALLATION?	DESCRIPTION
Quiet	/quiet	Yes	Runs the uninstaller displaying no UI and no prompts.
Uninstall	/uninstall	Yes	Runs the silent uninstallation of the ATA Center from the server.

NAME	SYNTAX	MANDATORY FOR SILENT UNINSTALLATION?	DESCRIPTION
Help	/help	No	Provides help and quick reference. Displays the correct use of the setup command including a list of all options and behaviors.

Installation parameters:

NAME	SYNTAX	MANDATORY FOR SILENT UNINSTALLATION?	DESCRIPTION
DeleteExistingDatabaseData	DeleteExistingDatabaseData	No	Deletes all the files in the existing database.

Examples:

To silently uninstall the ATA Center from the server, removing all existing database data:

```
"Microsoft ATA Center Setup.exe" /quiet /uninstall --DeleteExistingDatabaseData
```

ATA Gateway silent installation

> **NOTE**
> When silently deploying the ATA Lightweight Gateway via System Center Configuration Manager or other software deployment system, it is recommended to create two deployment packages:
> - Net Framework 4.6.1 including rebooting the domain controller
> - ATA Gateway.
> Make the ATA Gateway package dependent on the deployment of the .Net Framework package deployment.
> Get the .Net Framework 4.6.1 offline deployment package.

Use the following command to silently install the ATA Gateway:

Syntax:

```
"Microsoft ATA Gateway Setup.exe" [/quiet] [/Help] [NetFrameworkCommandLineArguments="/q"]
[ConsoleAccountName="<AccountName>"] [ConsoleAccountPassword="<AccountPassword>"]
```

> **NOTE**
> If you are working on a domain joined computer and have logged in using your ATA admin username and password, it is unnecessary to provide your credentials here.

Installation options:

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
Quiet	/quiet	Yes	Runs the installer displaying no UI and no prompts.

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
Help	/help	No	Provides help and quick reference. Displays the correct use of the setup command including a list of all options and behaviors.
NetFrameworkCommandLineArguments="/q"	NetFrameworkCommandLineArguments="/q"	Yes	Specifies the parameters for the .Net Framework installation. Must be set to enforce the silent installation of .Net Framework.

Installation parameters:

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
InstallationPath	InstallationPath=""	No	Sets the path for the installation of ATA binaries. Default path: C:\Program Files\Microsoft Advanced Threat Analytics\Center
ConsoleAccountName	ConsoleAccountName=""	Yes	Sets the name of the user account (user@domain.com) that is used to register the ATA Gateway with the ATA Center.
ConsoleAccountPassword	ConsoleAccountPassword=""	Yes	Sets the password for the user account (user@domain.com) that is used to register the ATA Gateway with the ATA Center.

Examples:

To silently install the ATA Gateway, log into the domain joined computer with your ATA admin credentials so that you do not need to specify credentials as part of the installation. Otherwise, register it with the ATA Center using the specified credentials:

```
"Microsoft ATA Gateway Setup.exe" /quiet NetFrameworkCommandLineArguments="/q"
ConsoleAccountName="user@contoso.com" ConsoleAccountPassword="userpwd"
```

Update the ATA Gateway

Use the following command to silently update the ATA Gateway:

Syntax:

```
"Microsoft ATA Gateway Setup.exe" [/quiet] [/Help] [NetFrameworkCommandLineArguments="/q"]
```

Installation options:

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
Quiet	/quiet	Yes	Runs the installer displaying no UI and no prompts.
Help	/help	No	Provides help and quick reference. Displays the correct use of the setup command including a list of all options and behaviors.
NetFrameworkCommandLineArguments="/q"	NetFrameworkCommandLineArguments="/q"	Yes	Specifies the parameters for the .Net Framework installation. Must be set to enforce the silent installation of .Net Framework.

Examples:

To update the ATA Gateway silently:

```
"Microsoft ATA Gateway Setup.exe" /quiet NetFrameworkCommandLineArguments="/q"
```

Uninstall the ATA Gateway silently

Use the following command to perform a silent uninstall of the ATA Gateway:

Syntax:

```
"Microsoft ATA Gateway Setup.exe" [/quiet] [/Uninstall] [/Help]
```

Installation options:

NAME	SYNTAX	MANDATORY FOR SILENT UNINSTALLATION?	DESCRIPTION
Quiet	/quiet	Yes	Runs the uninstaller displaying no UI and no prompts.
Uninstall	/uninstall	Yes	Runs the silent uninstallation of the ATA Gateway from the server.
Help	/help	No	Provides help and quick reference. Displays the correct use of the setup command including a list of all options and behaviors.

Examples:

To silently uninstall the ATA Gateway from the server:

```
"Microsoft ATA Gateway Setup.exe" /quiet /uninstall
```

See Also

- Check out the ATA forum!
- Configure event collection
- ATA prerequisites

Configure Port Mirroring

7/20/2020 • 3 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

> **NOTE**
> This article is relevant only if you deploy ATA Gateways instead of ATA Lightweight Gateways. To determine if you need to use ATA Gateways, see Choosing the right gateways for your deployment.

The main data source used by ATA is deep packet inspection of the network traffic to and from your domain controllers. For ATA to see the network traffic, you must either configure port mirroring, or use a Network TAP.

For port mirroring, configure **port mirroring** for each domain controller to be monitored, as the **source** of the network traffic. Typically, you need to work with the networking or virtualization team to configure port mirroring. For more information, see your vendor's documentation.

Your domain controllers and ATA Gateways can be either physical or virtual. The following are common methods for port mirroring and some considerations. For more information, see your switch or virtualization server product documentation. Your switch manufacturer might use different terminology.

Switched Port Analyzer (SPAN) – Copies network traffic from one or more switch ports to another switch port on the same switch. Both the ATA Gateway and domain controllers must be connected to the same physical switch.

Remote Switch Port Analyzer (RSPAN) – Allows you to monitor network traffic from source ports distributed over multiple physical switches. RSPAN copies the source traffic into a special RSPAN configured VLAN. This VLAN needs to be trunked to the other switches involved. RSPAN works at Layer 2.

Encapsulated Remote Switch Port Analyzer (ERSPAN) – Is a Cisco proprietary technology working at Layer 3. ERSPAN allows you to monitor traffic across switches without the need for VLAN trunks. ERSPAN uses generic routing encapsulation (GRE) to copy monitored network traffic. ATA currently cannot directly receive ERSPAN traffic. For ATA to work with ERSPAN traffic, a switch or router that can decapsulate the traffic needs to be configured as the destination of ERSPAN where the traffic is decapsulated. Then configure the switch or router to forward the decapsulated traffic to the ATA Gateway using either SPAN or RSPAN.

> **NOTE**
> If the domain controller being port mirrored is connected over a WAN link, make sure the WAN link can handle the additional load of the ERSPAN traffic. ATA only supports traffic monitoring when the traffic reaches the NIC and the domain controller in the same manner. ATA does not support traffic monitoring when the traffic is broken out to different ports.

Supported port mirroring options

ATA GATEWAY	DOMAIN CONTROLLER	CONSIDERATIONS
Virtual	Virtual on same host	The virtual switch needs to support port mirroring. Moving one of the virtual machines to another host by itself may break the port mirroring.

ATA GATEWAY	DOMAIN CONTROLLER	CONSIDERATIONS
Virtual	Virtual on different hosts	Make sure your virtual switch supports this scenario.
Virtual	Physical	Requires a dedicated network adapter otherwise ATA sees all of the traffic coming in and out of the host, even the traffic it sends to the ATA Center.
Physical	Virtual	Make sure your virtual switch supports this scenario - and port mirroring configuration on your physical switches based on the scenario: If the virtual host is on the same physical switch, you need to configure a switch level span. If the virtual host is on a different switch, you need to configure RSPAN or ERSPAN*.
Physical	Physical on the same switch	Physical switch must support SPAN/Port Mirroring.
Physical	Physical on a different switch	Requires physical switches to support RSPAN or ERSPAN*.

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

> **NOTE**
> Make sure that domain controllers and the ATA Gateways to which they connect have time synchronized to within five minutes of each other.

If you are working with virtualization clusters:

- For each domain controller running on the virtualization cluster in a virtual machine with the ATA Gateway, configure affinity between the domain controller and the ATA Gateway. This way when the domain controller moves to another host in the cluster the ATA Gateway follows it. This works well when there are a few domain controllers.

> **NOTE**
> If your environment supports Virtual to Virtual on different hosts (RSPAN) you do not need to worry about affinity.

- To make sure the ATA Gateways are properly sized to handle monitoring all of the DCs by themselves, try this option: Install a virtual machine on each virtualization host and install an ATA Gateway on each host. Configure each ATA Gateway to monitor all of the domain controllers that run on the cluster. This way, any host the domain controllers run on is monitored.

After configuring port mirroring, validate that port mirroring is working before installing the ATA Gateway.

See Also

- Validate port mirroring
- Check out the ATA forum!

Validate Port Mirroring

7/20/2020 • 4 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

> **NOTE**
> This article is relevant only if you deploy ATA Gateways instead of ATA Lightweight Gateways. To determine if you need to use ATA Gateways, see Choosing the right gateways for your deployment.

The following steps walk you through the process for validating that port mirroring is properly configured. For ATA to work properly, the ATA Gateway must be able to see the traffic to and from the domain controller. The main data source used by ATA is deep packet inspection of the network traffic to and from your domain controllers. For ATA to see the network traffic, port mirroring needs to be configured. Port mirroring copies the traffic from one port (the source port) to another port (the destination port).

Validate port mirroring using a Windows PowerShell script

1. Save the text of this script into a file called *ATAdiag.ps1*.
2. Run this script on the ATA Gateway that you want to validate. The script generates ICMP traffic from the ATA Gateway to the domain controller and looks for that traffic on the Capture NIC on the domain controller. If the ATA Gateway sees ICMP traffic with a destination IP address the same as the DC IP addressed you entered in the ATA Console, it deems port mirroring configured.

Sample for how to run the script:

```
# ATAdiag.ps1 -CaptureIP n.n.n.n -DCIP n.n.n.n -TestCount n

param([parameter(Mandatory=$true)][string]$CaptureIP, [parameter(Mandatory=$true)][string]$DCIP,
[int]$PingCount = 10)

# Set variables

    $ErrorActionPreference = "stop"
$starttime = get-date
$byteIn = new-object byte[] 4
$byteOut = new-object byte[] 4
$byteData = new-object byte[] 4096  # size of data

$byteIn[0] = 1  # for promiscuous mode
$byteIn[1-3] = 0
$byteOut[0-3] = 0



# Convert network data to host format
    function NetworkToHostUInt16 ($value)
 {
 [Array]::Reverse($value)
 [BitConverter]::ToUInt16($value,0)
 }

function NetworkToHostUInt32 ($value)
 {
 [Array]::Reverse($value)
 [BitConverter]::ToUInt32($value,0)
```

```
 }

function ByteToString ($value)
 {
 $AsciiEncoding = new-object system.text.asciiencoding
 $AsciiEncoding.GetString($value)
     }

Write-Host "Testing Port Mirroring..." -ForegroundColor Yellow
Write-Host ""
Write-Host "Here is a summary of the connection we will test." -ForegroundColor Yellow

# Initialize a first ping connection
Test-Connection -Count 1 -ComputerName $DCIP -ea SilentlyContinue
Write-Host ""

Write-Host "Press any key to continue..." -ForegroundColor Red
[void][System.Console]::ReadKey($true)
Write-Host ""
Write-Host "Sending ICMP and Capturing data..." -ForegroundColor Yellow

# Open a socket

$socket = new-object system.net.sockets.socket([Net.Sockets.AddressFamily]::InterNetwork,
[Net.Sockets.SocketType]::Raw,[Net.Sockets.ProtocolType]::IP)

# Include the IP header
$socket.setsocketoption("IP","HeaderIncluded",$true)

$socket.ReceiveBufferSize = 10000

$ipendpoint = new-object system.net.ipendpoint([net.ipaddress]"$CaptureIP",0)
$socket.bind($ipendpoint)

# Enable promiscuous mode
[void]$socket.iocontrol([net.sockets.iocontrolcode]::ReceiveAll,$byteIn,$byteOut)

# Initialize test variables
$tests = 0
$TestResult = "Noise"
$OneSuccess = 0

while ($tests -le $PingCount)
 {
 if (!$socket.Available)  # see if any packets are in the queue
  {
  start-sleep -milliseconds 500
  continue
  }

# Capture traffic
 $rcv = $socket.receive($byteData,0,$byteData.length,[net.sockets.socketflags]::None)

# Decode the header so we can read ICMP

 $MemoryStream = new-object System.IO.MemoryStream($byteData,0,$rcv)
 $BinaryReader = new-object System.IO.BinaryReader($MemoryStream)

# Set IP version & header length
 $VersionAndHeaderLength = $BinaryReader.ReadByte()

 # TOS
 $TypeOfService= $BinaryReader.ReadByte()

 # More values, and the Protocol Number for ICMP traffic
 # Convert network format of big-endian to host format of little-endian
 $TotalLength = NetworkToHostUInt16 $BinaryReader.ReadBytes(2)

 $Identification = NetworkToHostUInt16 $BinaryReader.ReadBytes(2)
```

```
 $FlagsAndOffset = NetworkToHostUInt16 $BinaryReader.ReadBytes(2)
 $TTL = $BinaryReader.ReadByte()
 $ProtocolNumber = $BinaryReader.ReadByte()
 $Checksum = [Net.IPAddress]::NetworkToHostOrder($BinaryReader.ReadInt16())

 # The source and destination IP addresses
 $SourceIPAddress = $BinaryReader.ReadUInt32()
 $DestinationIPAddress = $BinaryReader.ReadUInt32()

 # The source and destimation ports
 $sourcePort = [uint16]0
 $destPort = [uint16]0

 # Close the stream reader
 $BinaryReader.Close()
 $memorystream.Close()

 # Cast DCIP into an IPaddress type
 $DCIPP = [ipaddress] $DCIP
 $DestinationIPAddressP = [ipaddress] $DestinationIPAddress

 #Ping the DC at the end after starting the capture
 Test-Connection -Count 1 -ComputerName $DCIP -ea SilentlyContinue | Out-Null

 # This is the match logic - check to see if Destination IP from the Ping sent matches the DCIP entered by in
the ATA Console
 # The only way the ATA Gateway should see a destination of the DC is if Port Spanning is configured

  if ($DestinationIPAddressP -eq $DCIPP)  # is the destination IP eq to the DC IP?
  {
  $TestResult = "Port Spanning success!"
  $OneSuccess = 1
  } else {
   $TestResult = "Noise"
  }

 # Put source, destination, test result in Powershell object

 new-object psobject | add-member -pass noteproperty CaptureSource $([system.net.ipaddress]$SourceIPAddress) |
add-member -pass noteproperty CaptureDestination $([system.net.ipaddress]$DestinationIPAddress) | Add-Member -
pass NoteProperty Result $TestResult | Format-List | Out-Host
 #Count tests
 $tests ++
 }

 If ($OneSuccess -eq 1){
  Write-Host "Port Spanning Success!" -ForegroundColor Green
  Write-Host ""
  Write-Host "At least one packet which was addressed to the DC, was picked up by the Gateway." -
ForegroundColor Yellow
  Write-Host "A little noise is OK, but if you don't see a majority of successes, you might want to re-run." -
ForegroundColor Yellow
 } Else {
  Write-Host "No joy, all noise.  You may want to re-run, increase the number of Ping Counts, or check your
config." -ForegroundColor Red
 }

Write-Host ""
Write-Host "Press any key to continue..." -ForegroundColor Red
[void][System.Console]::ReadKey($true)
```

Validate port mirroring using Net Mon

1. Install Microsoft Network Monitor 3.4 on the ATA Gateway that you want to validate.

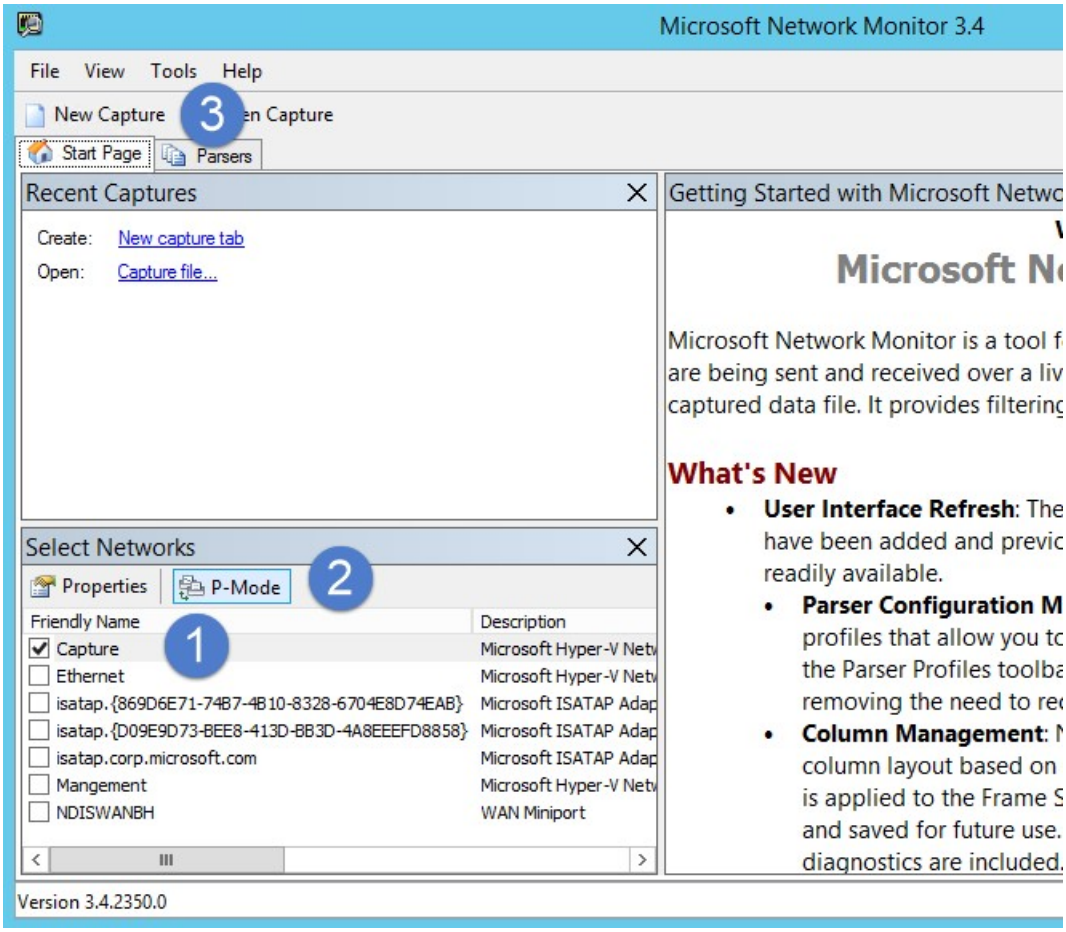
> **IMPORTANT**
>
> Do not install Microsoft Message Analyzer, or any other traffic capture software on the ATA Gateway.

2. Open Network Monitor and create a new capture tab.

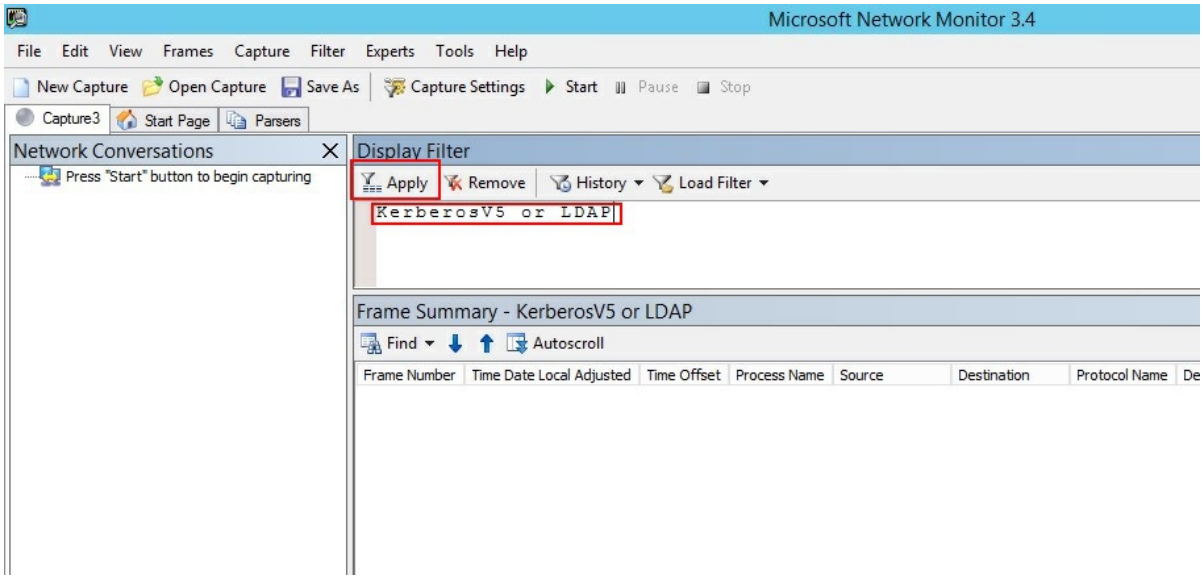
   a. Select only the **Capture** network adapter or the network adapter that is connected to the switch port that is configured as the port mirroring destination.

   b. Ensure that P-Mode is enabled.

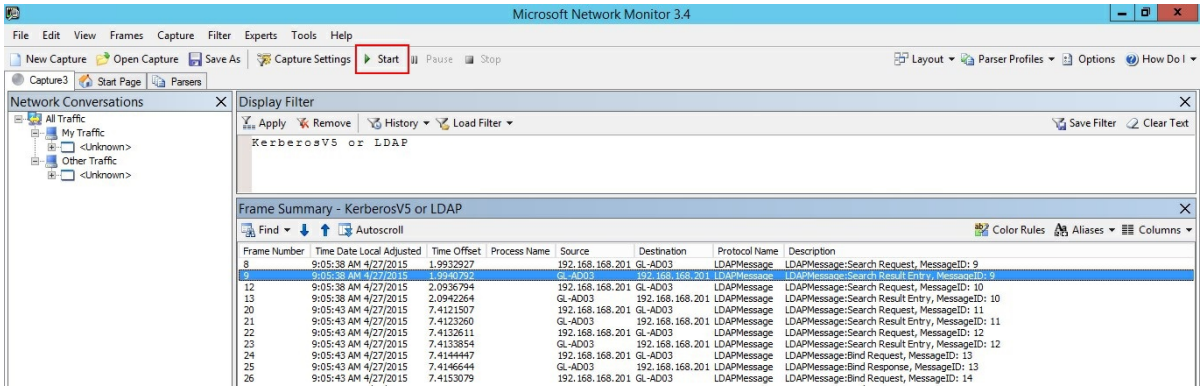
   c. Click **New Capture**.



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



4. Click **Start** to start the capture session. If you do not see traffic to and from the domain controller, review your port mirroring configuration.



> **NOTE**
>
> It is important to make sure you see traffic to and from the domain controllers.

5. If you only see traffic in one direction, you should work with your networking or virtualization teams to help troubleshoot your port mirroring configuration.

See Also

- Configure port mirroring
- Check out the ATA forum!

Configuring Windows Event Forwarding

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

> **NOTE**
> For ATA versions 1.8 and higher, event collection configuration is no longer necessary for ATA Lightweight Gateways. The ATA Lightweight Gateway now read events locally, without the need to configure event forwarding.

To enhance detection capabilities, ATA needs the following Windows events: 4776, 4732, 4733, 4728, 4729, 4756, 4757, 7045. These can either be read automatically by the ATA Lightweight Gateway or in case the ATA Lightweight Gateway is not deployed, it can be forwarded to the ATA Gateway in one of two ways, by configuring the ATA Gateway to listen for SIEM events or by configuring Windows Event Forwarding.

> **NOTE**
> If you are using Server Core, wecutil can be used to create and manage subscriptions to events that are forwarded from remote computers.

WEF configuration for ATA Gateway's with port mirroring

After configuring port mirroring from the domain controllers to the ATA Gateway, use the following instructions to configure Windows Event forwarding using Source Initiated configuration. This is one way to configure Windows Event forwarding.

Step 1: Add the network service account to the domain Event Log Readers Group.

In this scenario, assume that the ATA Gateway is a member of the domain.

1. Open Active Directory Users and Computers, navigate to the **BuiltIn** folder and double-click **Event Log Readers**.
2. Select **Members**.
3. If **Network Service** is not listed, click **Add**, type **Network Service** in the **Enter the object names to select** field. Then click **Check Names** and click **OK** twice.

After adding the **Network Service** to the **Event Log Readers** group, reboot the domain controllers for the change to take effect.

Step 2: Create a policy on the domain controllers to set the Configure target Subscription Manager setting.

> **NOTE**
> You can create a group policy for these settings and apply the group policy to each domain controller monitored by the ATA Gateway. The steps below modify the local policy of the domain controller.

1. Run the following command on each domain controller: *winrm quickconfig*
2. From a command prompt type *gpedit.msc*.
3. Expand **Computer Configuration > Administrative Templates > Windows Components >**

Event Forwarding

4. Double-click **Configure target Subscription Manager**.
   a. Select **Enabled**.
   b. Under **Options**, click **Show**.
   c. Under **SubscriptionManagers**, enter the following value and click **OK**:
   Server=http://:5985/wsman/SubscriptionManager/WEC,Refresh=10

   (For example: Server= `http://atagateway9.contoso.com:5985/wsman/SubscriptionManager/WEC,Refresh=10` *)*

   d. Click **OK**.
   e. From an elevated command prompt type *gpupdate /force*.

Step 3: Perform the following steps on the ATA Gateway

1. Open an elevated command prompt and type *wecutil qc*
2. Open **Event Viewer**.
3. Right-click **Subscriptions** and select **Create Subscription**.
   a. Enter a name and description for the subscription.
   b. For **Destination Log**, confirm that **Forwarded Events** is selected. For ATA to read the events, the destination log must be **Forwarded Events**.
   c. Select **Source computer initiated** and click **Select Computers Groups**.
      a. Click **Add Domain Computer**.
      b. Enter the name of the domain controller in the **Enter the object name to select** field. Then click **Check Names** and click **OK**.

      c. Click **OK**.
   d. Click **Select Events**.
      a. Click **By log** and select **Security**.
      b. In the **Includes/Excludes Event ID** field type the event number and click **OK**. For example, type 4776, like in the following sample.

   e. Right-click the created subscription and select **Runtime Status** to see if there are any issues with the status.
   f. After a few minutes, check to see that the events you set to be forwarded is showing up in the Forwarded Events on the ATA Gateway.

For more information, see: Configure the computers to forward and collect events

See Also

- Install ATA

- Check out the ATA forum!

ATA Database Management

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

If you need to move, backup or restore the ATA database, use these procedures for working with MongoDB.

Backing up the ATA database

Refer to the relevant MongoDB documentation.

Restoring the ATA database

Refer to the relevant MongoDB documentation.

Moving the ATA database to another drive

1. Stop the **Microsoft Advanced Threat Analytics Center** service.

   > **IMPORTANT**
   > Make sure the ATA Center service stopped before moving on to the next step.

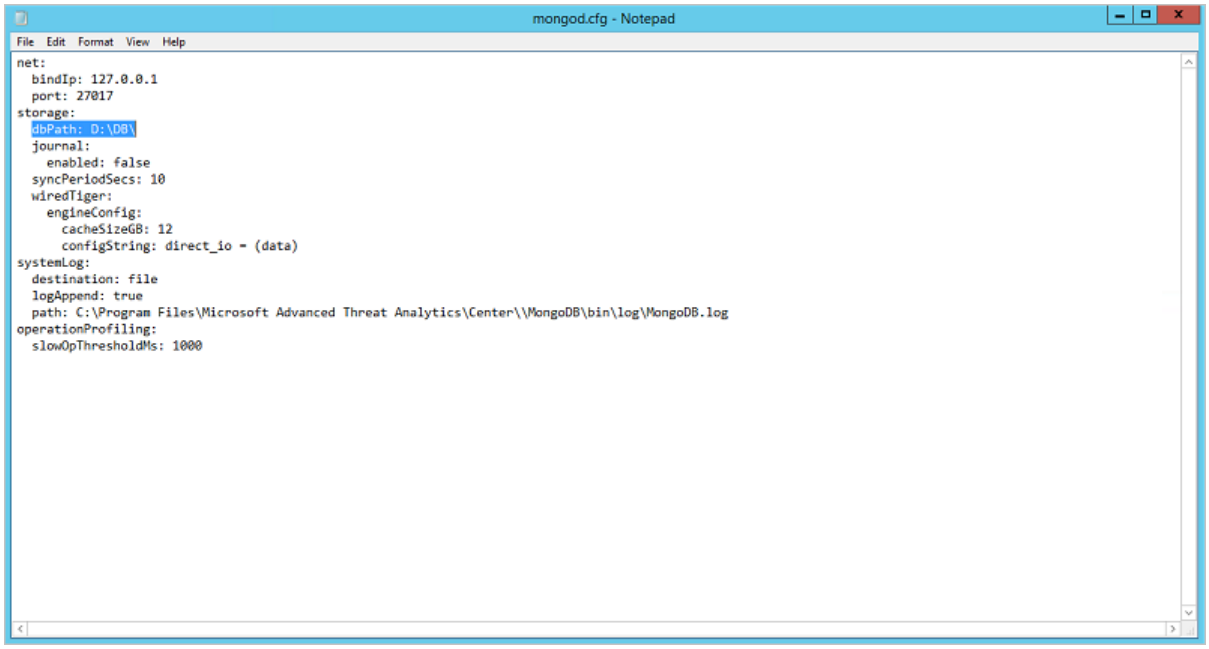
2. Stop the **MongoDB** service.

3. Open the Mongo configuration file located by default at: C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\mongod.cfg.

   Find the parameter `storage: dbPath`

4. Move the folder listed in the `dbPath` parameter to the new location.

5. Change the `dbPath` parameter inside the mongo configuration file to the new folder path and save and close the file.



6. Start the **MongoDB** service.
7. Start the **Microsoft Advanced Threat Analytics Center** service.

See Also

- ATA architecture
- ATA prerequisites
- Check out the ATA forum!

Working with ATA system health and events

7/20/2020 • 2 minutes to read • Edit Online

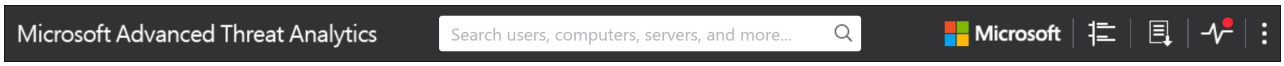
Applies to: Advanced Threat Analytics version 1.9

ATA Health Center

The ATA Health Center lets you know how your ATA service is performing and alerts you to problems.

Working with the ATA Health Center

The ATA Health Center lets you know that there's a problem by raising an alert (a red dot) above the Health Center icon in the menu bar.



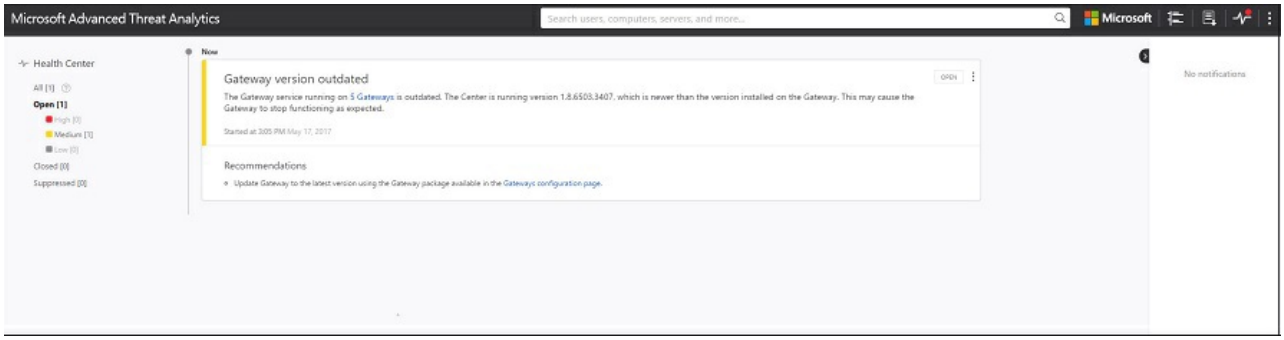
Managing ATA health

To check up on your system's overall health, click the Health Center icon in the menu bar 

- All open alerts can be managed by setting them to **Close**, **Suppress**, or **Delete** by clicking the three dots in the corner of the alert and making your selection.
- **Open**: All new suspicious activities appear in this list.
- **Close**: Is used to track suspicious activities that you identified, researched, and fixed for mitigated.

  > **NOTE**
  > ATA may reopen a closed activity if the same activity is detected again within a short period of time.

- **Suppress**: Suppressing an activity means you want to ignore it for now, and only be alerted again if there's a new instance. If there's a similar alert ATA doesn't reopen it. But if the alert stops for seven days, and is then seen again, you are alerted again.
- **Delete**: If you Delete an alert, it is deleted from the system, from the database and you will NOT be able to restore it. After you click delete, you'll be able to delete all suspicious activities of the same type.



See Also

- Working with suspicious activities

- Check out the ATA forum!

ATA Reports

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

The ATA reports section in the console enables you to generate reports that provide you with system status information, both system health and a report of the suspicious activities detected in your environment.

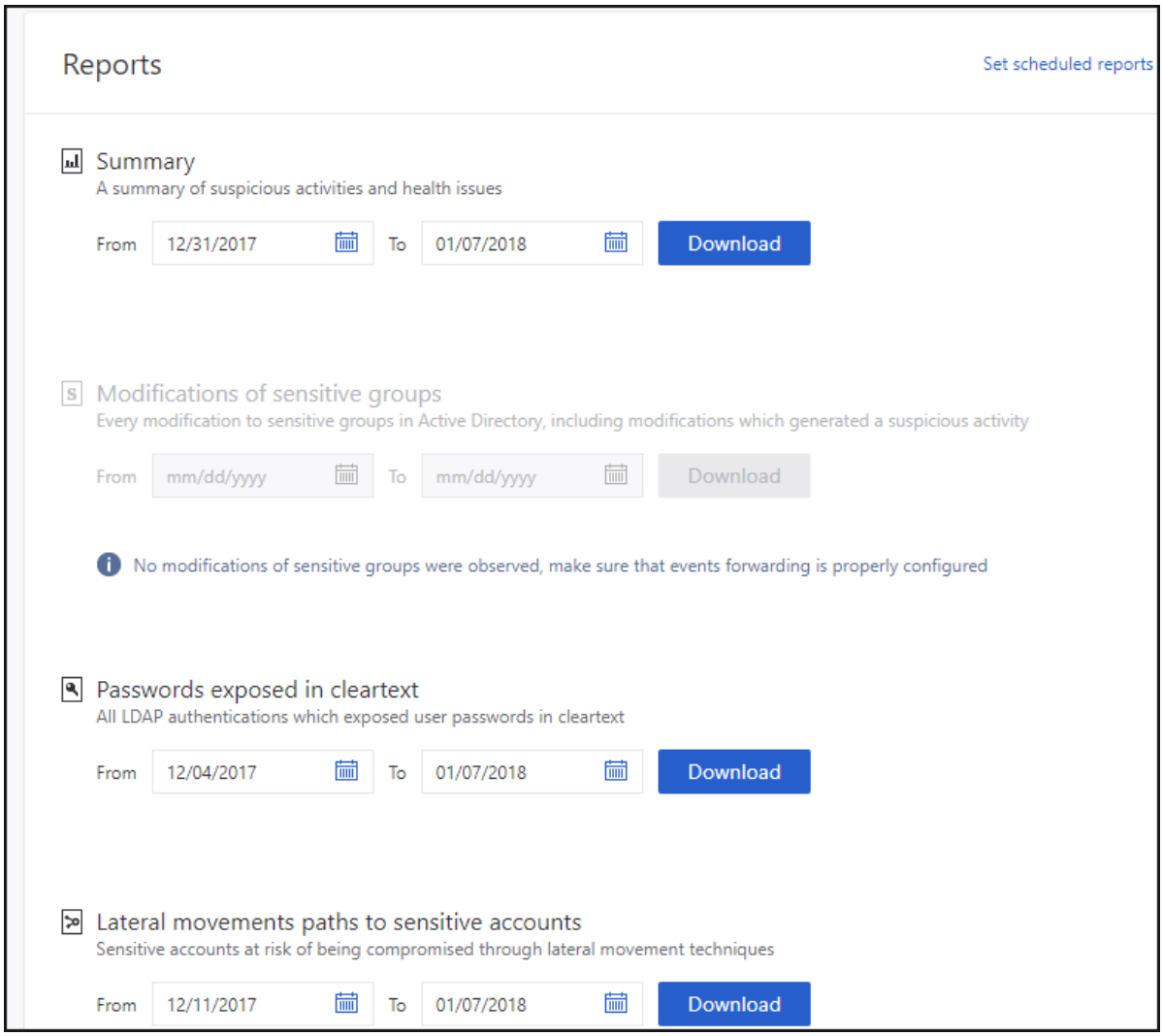
To access the reports page, click the report icon in the menu bar:  . The reports that are available are:

- **Summary report**: The Summary report presents a dashboard of the status in the system. You can view three tabs - one for a **Summary** of what was detected on your network, **Open suspicious activities** that lists the suspicious activities you should take care of, and **Open health issues** that lists ATA system health issues you should take care of. The suspicious activities listed are broken down by type, as are the health issues.
- **Modification of sensitive groups**: This report lists every time a modification is made to sensitive groups (such as admins).
- **Passwords exposed in cleartext**: Some services use the LDAP non-secure protocol to send account credentials in plain text. This can even happen for sensitive accounts. Attackers monitoring network traffic can catch and then reuse these credentials for malicious purposes. This report lists all source computer and account passwords that ATA detected as being sent in clear text.
- **Lateral movement paths to sensitive accounts**: This report lists the sensitive accounts that are exposed via lateral movement paths. For more information, see Lateral movement paths

There are two ways to generate a report: either on demand or by scheduling a report to be sent to your email periodically.

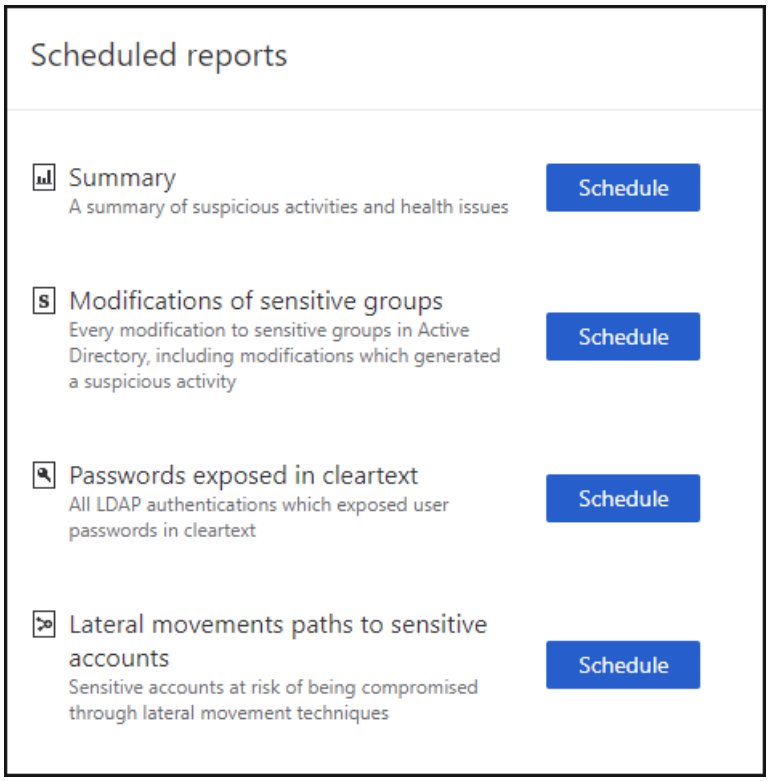
To generate a report on demand:

1. In the ATA console menu bar, click the report icon in the menu bar:  .
2. Under either your selected report type, set the **From** and **To** dates and click **Download**.



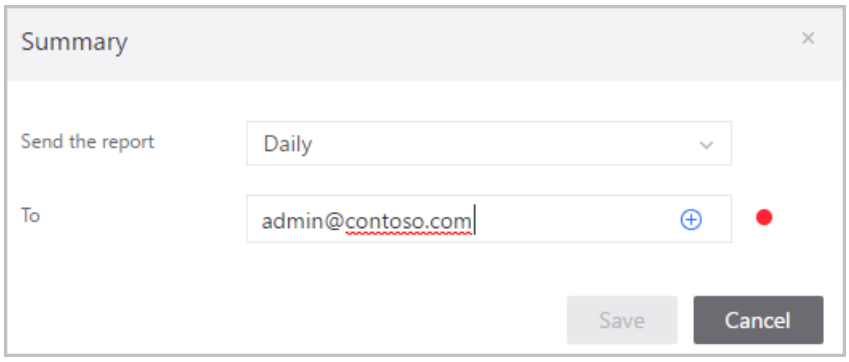
To set a scheduled report:

1. In the **Reports** page, click **Set scheduled reports**, or in the ATA Console configuration page, under Notifications and Reports, click **Scheduled reports**.



> **NOTE**
> The daily reports are designed to be sent shortly after midnight, UTC.

2. Click **Schedule** next to your selected report type, to set the frequency and email address for delivery of the reports, and click the plus sign next to the email addresses to add them, and click **Save**.



> **NOTE**
> Scheduled reports are delivered by email and can only be sent if you have already configured an email server under **Configuration** and then, under **Notifications and Reports**, select **Mail server**.

See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

ATA Role Groups

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

Role groups enable access management for ATA. Using role groups, you can segregate duties within your security team, and grant only the amount of access that users need to perform their jobs. This article explains access management and ATA role authorization, and helps you get up and running with role groups in ATA.

> **NOTE**
> Any local administrator on the ATA Center is automatically a Microsoft Advanced Threat Analytics Administrator.

Types of ATA Role Groups

ATA introduces three types of Role group: ATA Administrators, ATA Users, and ATA Viewers. The following table describes the type of access in ATA available per role. Depending on which role you assign, various screens and menu options in ATA are not available, as follows:

ACTIVITY	MICROSOFT ADVANCED THREAT ANALYTICS ADMINISTRATORS	MICROSOFT ADVANCED THREAT ANALYTICS USERS	MICROSOFT ADVANCED THREAT ANALYTICS VIEWERS
Login	Available	Available	Available
Provide Input for Suspicious Activities	Available	Available	Not available
Change status of Suspicious Activities	Available	Available	Not available
Share/Export suspicious activity via email/get link	Available	Available	Not available
Change status of Health Alerts	Available	Available	Not available
Update ATA Configuration	Available	Not available	Not available
Gateway – Add	Available	Not available	Not available
Gateway – Delete	Available	Not available	Not available
Monitored DC – Add	Available	Not available	Not available
Monitored DC – Delete	Available	Not available	Not available
View alerts and suspicious activities	Available	Available	Available

When users try to access a page that is not available for their role group, they are redirected to the ATA

unauthorized page.

Add \ Remove users - ATA Role Groups

ATA uses the local Windows groups as a basis for role groups. The role groups must be managed on the ATA Center server. To add or remove users, use the **Local Users and Groups** MMC (Lusrmgr.msc). On a domain joined machine, you can add domain accounts as well as local accounts.

Modifying the ATA Center configuration

7/20/2020 • 3 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

After the initial deployment, modifications to the ATA Center should be made carefully. Use the following procedures when updating the console URL, and the certificate.

The ATA Console URL

The URL is used in the following scenarios:

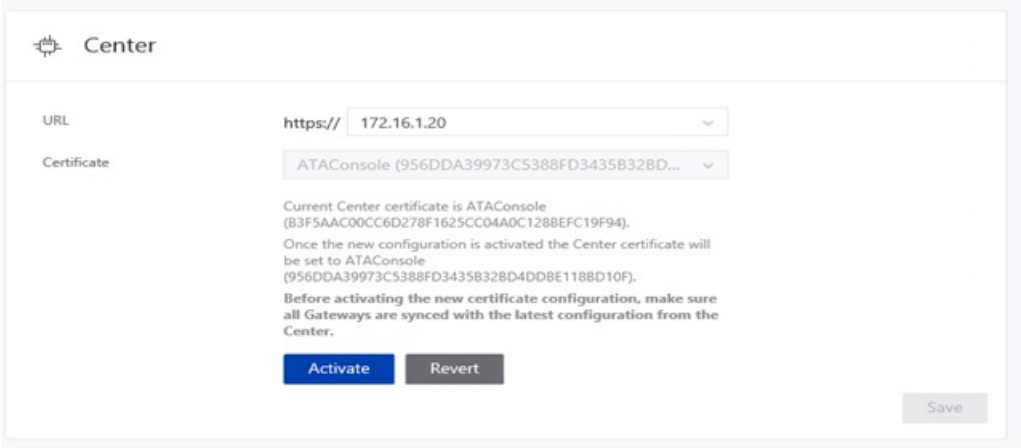
- This is the URL used by the ATA Gateways to communicate with the ATA Center.
- Installation of ATA Gateways – When an ATA Gateway is installed, it registers itself with the ATA Center. This registration process is accomplished by connecting to the ATA Console. If you enter an FQDN for the ATA Console 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.

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 still uses the original URL.

> **NOTE**
> If you entered a custom IP address, you cannot click **Activate** until you installed the IP address on the ATA Center.

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, in the Center configuration page, click the

Activate button to 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 an ATA Gateway was offline while you activated the new URL, and never got the updated configuration, manually update the configuration JSON file on the ATA Gateway.
- If you need to deploy a new ATA Gateway after activating the new URL, you need to download the ATA Gateway Setup package again.

The ATA Center certificate

WARNING

- The process of renewing an existing certificate is not supported. The only way to renew a certificate is by creating a new certificate and configuring ATA to use the new 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 that you 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.

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.

3. 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.

4. After all the ATA Gateways synced with the updated configuration, activate the new certificate that the ATA Center service is bound to. When you activate the new certificate, the ATA Center service binds to the new certificate. ATA Gateways 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 got the updated configuration, 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.

See Also

- Working with the ATA Console
- Check out the ATA forum!

Change ATA configuration - domain connectivity password

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

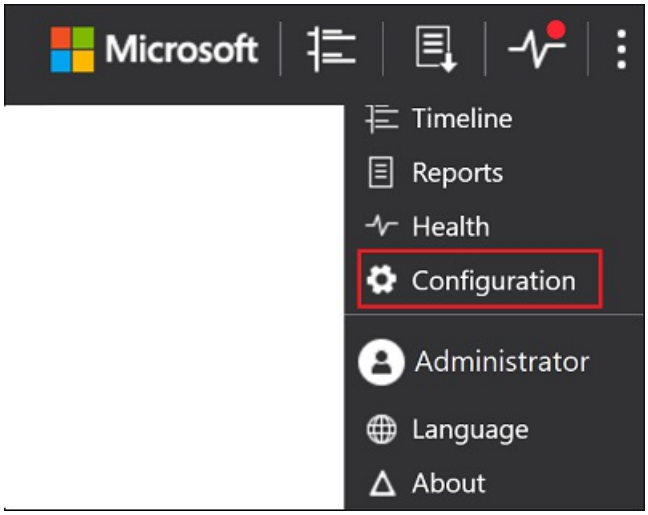
Change the domain connectivity password

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

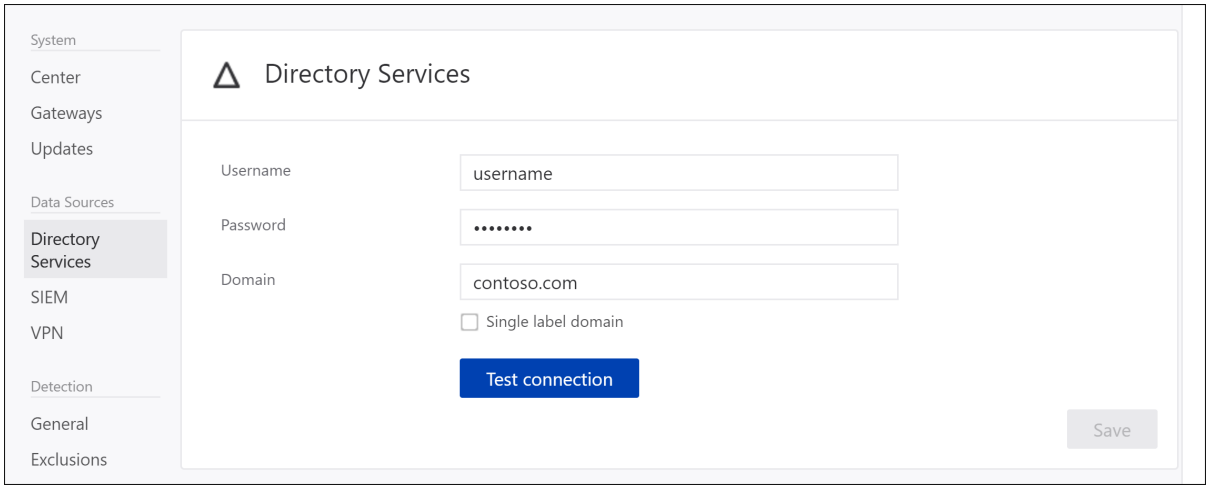
If you suspect that this happened, on the ATA Gateway, look at the Microsoft.Tri.Gateway-Errors.log file for the following errors: `The supplied credential is invalid.`

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

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



3. Select **Directory Services**.



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

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

5. Click **Save**.
6. After changing the password, manually check that the ATA Gateway service is running on the ATA Gateway servers.

See Also

- Working with the ATA Console
- Check out the ATA forum!

Excluding entities from detections

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

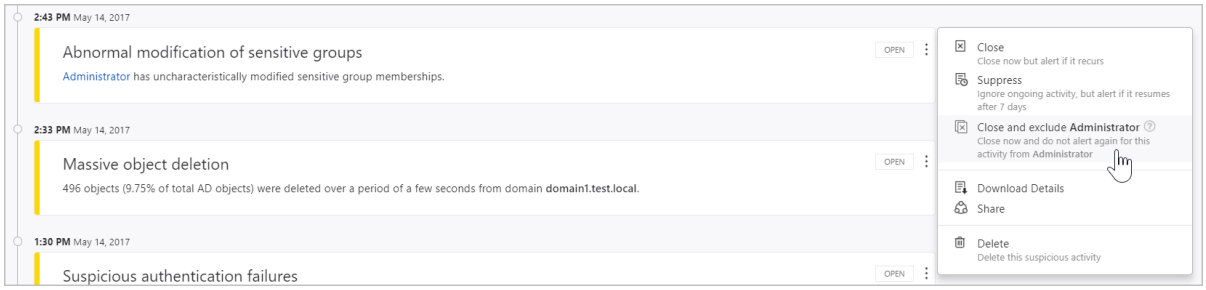
This article explains how to exclude entities from triggering alerts in order to minimize true benign positives but at the same time, make sure you catch the true positives. In order to keep ATA from being noisy about activities that, from specific users, may be part of your normal rhythm of business, you can quiet - or exclude - specific entities from raising alerts.

For example, if you have a security scanner that does DNS recon or an admin who remotely runs scripts on the domain controller - and these are sanctioned activities whose intent is part of the normal IT operations in your organization.

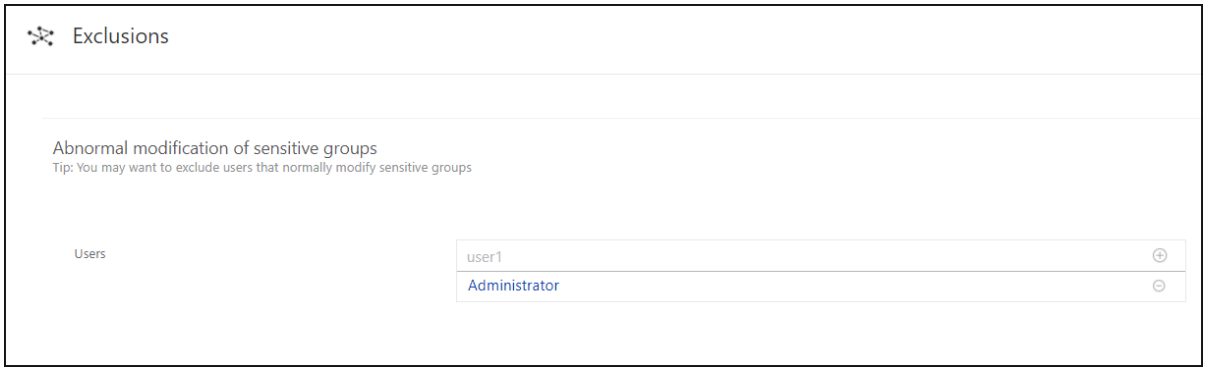
To exclude entities from raising alerts in ATA:

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, right-click the three dots at the end of the row for the suspicious activity on that entity, and select **Close and exclude**.
  This adds the user, computer, or IP address to the exclusions list for that suspicious activity. It closes the suspicious activity and it is no longer listed in the **Open** events list in the **Suspicious activity timeline**.



- **From the Configuration page**: To review or modify any exclusions: under **Configuration**, click **Exclusions** and then select the suspicious activity, such as **Sensitive account credentials exposed**.



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.

> **NOTE**
> For your protection, not all detections provide the possibility to set exclusions.

Some of the detections provide tips that help you decide what to exclude.

Each exclusion depends on the context, in some you can set users while for others you can set computers or IP addresses.

When you have the possibility of excluding an IP address or a computer, you can exclude one or the other - you don't need to provide both.

> **NOTE**
> The configuration pages can only be modified by ATA admins.

See Also

- Check out the ATA forum!
- Modifying ATA configuration

Export and Import the ATA Configuration

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

The configuration of ATA is stored in the "SystemProfile" collection in the database. This collection is backed up every 4 hours by the ATA Center service to files called: **SystemProfile_*timestamp*.json**. The 300 most recent versions are stored. This file is located in a subfolder called **Backup**. In the default ATA installed location it can be found here: *C:\Program Files\Microsoft Advanced Threat Analytics\Center\Backup\SystemProfile_*timestamp*.json*.

Note: It is recommended that you back up this file somewhere 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
```

See Also

- ATA architecture
- ATA prerequisites
- Check out the ATA forum!

Manage system-generated logs

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

NOTE

This article provides steps for how to delete personal data from the device or service and can be used to support your obligations under the GDPR. If you're looking for general info about GDPR, see the GDPR section of the Service Trust portal.

NOTE

Advanced Threat Analytics (ATA) collects anonymized system-generated log 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.

Data collected

Collected anonymized data includes the following parameters:

- 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:

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

  - Suspicious activity type
  - Suspicious activity ID
  - Status
  - Start and End Time
  - Input provided

- 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, that is, which pages in the ATA Console are visited.

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**.

See Also

- Troubleshooting ATA using the event log
- Check out the ATA forum!

Set ATA Notifications

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

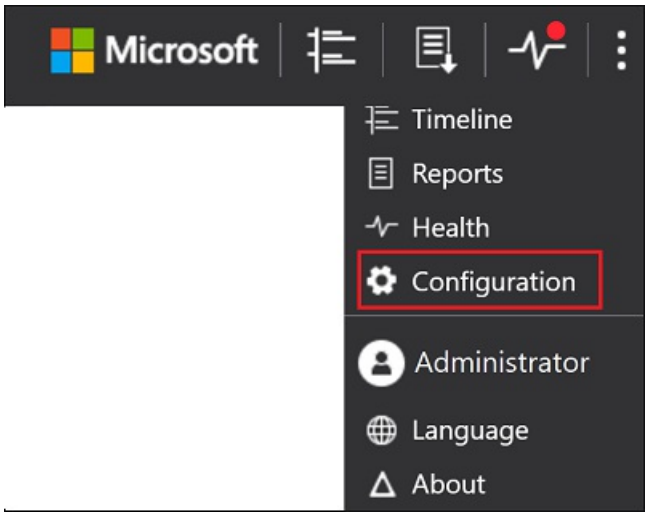
ATA can notify you when it detects a suspicious activity, either by email or by using ATA event forwarding and forwarding the event to your SIEM/syslog server. Before selecting which notifications you want to receive, you have to set up your email server and your Syslog server.

NOTE

- Email notifications include a link that takes 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 selected during the installation of the ATA Center. If you are going to configure email notifications, it is recommended to use an FQDN as the ATA Console URL.
- Notifications are sent from the ATA Center to either the SMTP server and the Syslog server.

To receive notifications, set the following parameters:

1. In the ATA Console, select the settings option on the toolbar and select **Configuration**.

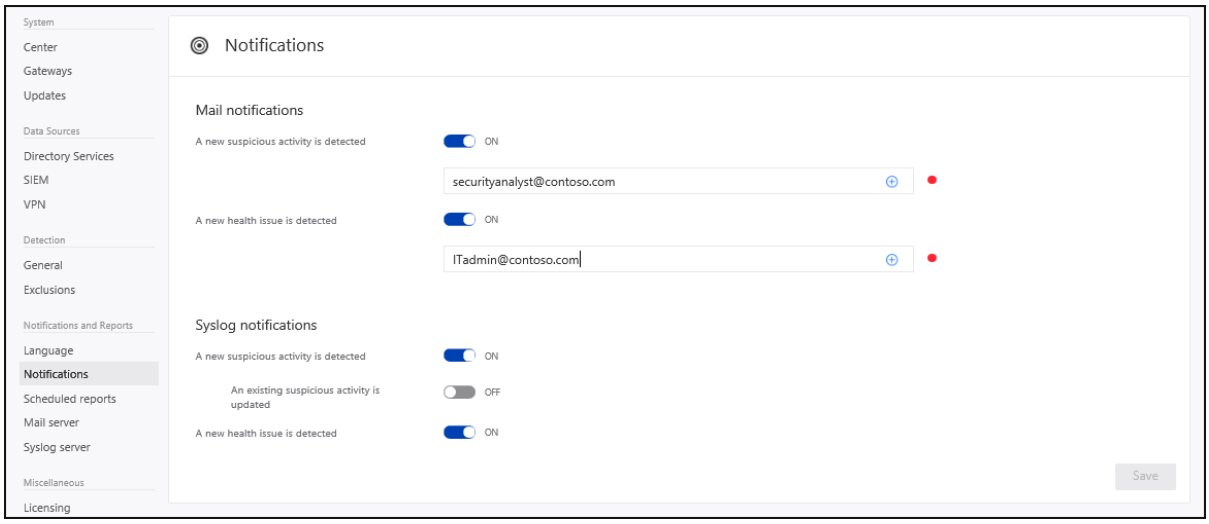


2. Under the **Notifications & Reports** section, select **Notifications**.
3. Under **Mail notifications**, specify which notifications should be sent via email - new suspicious activities and new health issues. You can set a separate email address for the suspicious activities to be sent to and for the health alerts so that, for example, suspicious activity notifications can be sent to your security analyst and your health alert notifications can be sent to your IT admin.

   NOTE

   Email alerts for suspicious activities are only sent when the suspicious activity is created.

4. Under **Syslog notifications**, specify which notifications should be sent to your Syslog server - new suspicious activities, updated suspicious activities, and new health issues.
5. Click **Save**.



See Also

Check out the ATA forum!

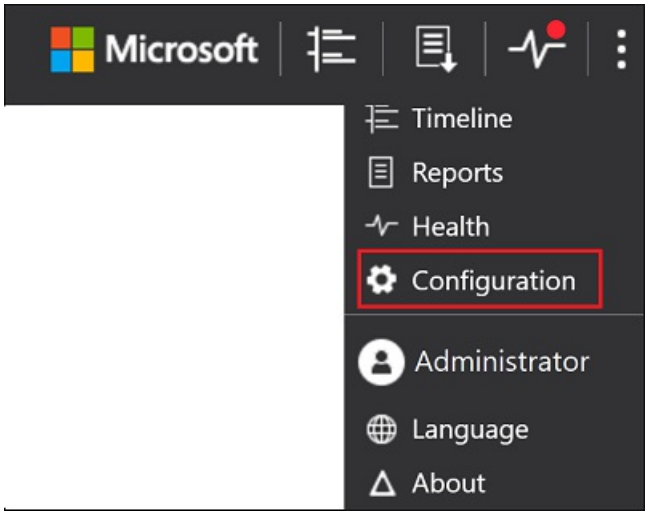
Provide ATA with your email server settings

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

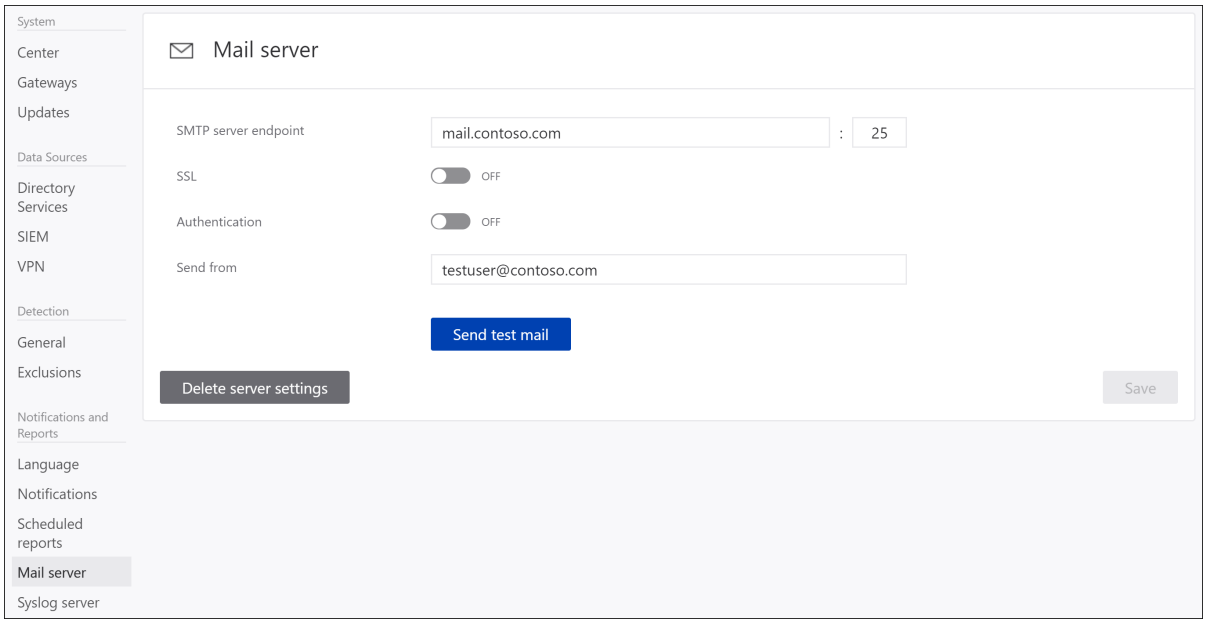
ATA can notify you when it detects a suspicious activity. For ATA to be able to send email notifications, you must first configure the **Email server settings**.

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**.



4. In the **notifications** section, under **Mail server**, enter the following information:

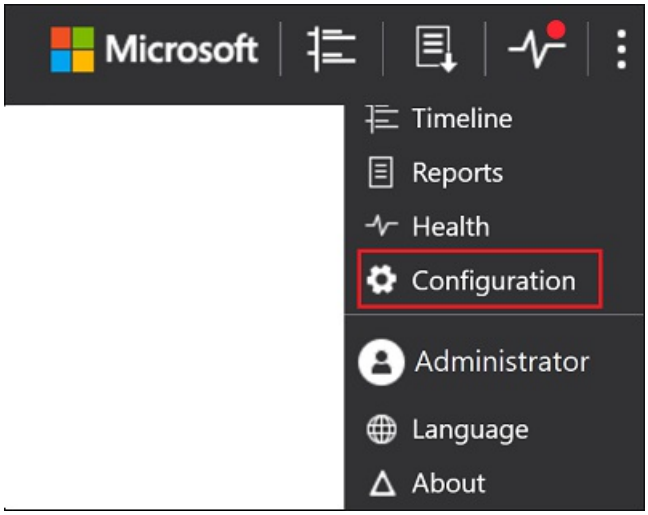
FIELD	DESCRIPTION	VALUE
SMTP server endpoint (required)	Enter the FQDN of your SMTP server and optionally change the port number (default 25).	For example: smtp.contoso.com
SSL	Toggle SSL if the SMTP server required SSL. **Note:** If you enable SSL, you also need to change the Port number.	Default is disabled
Authentication	Enable if your SMTP server requires authentication. **Note:** If you enable authentication, you must provide a user name and password of 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 from.	For example: ATA@contoso.com



Provide ATA with your Syslog server settings

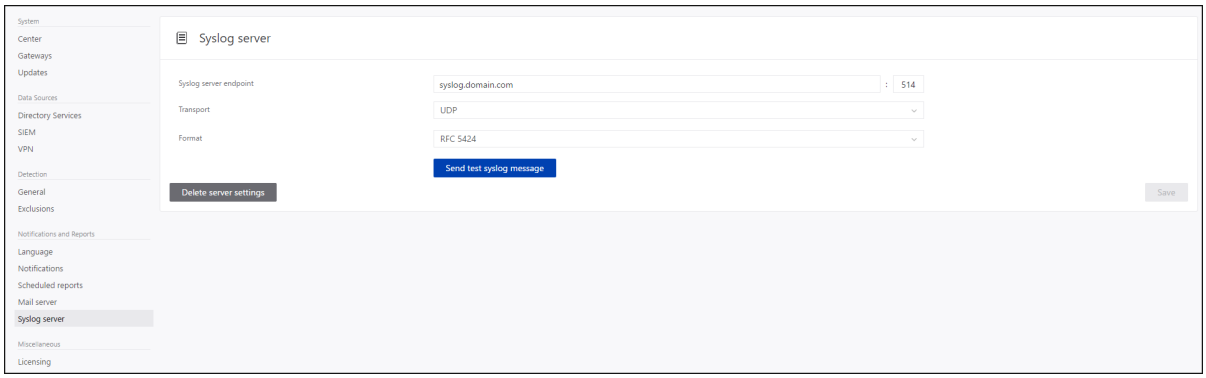
ATA can notify you when it detects a suspicious activity by sending the notification to your Syslog server. If you enable Syslog notifications, you can set the following for them.

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



5. 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.



See Also

Check out the ATA forum!

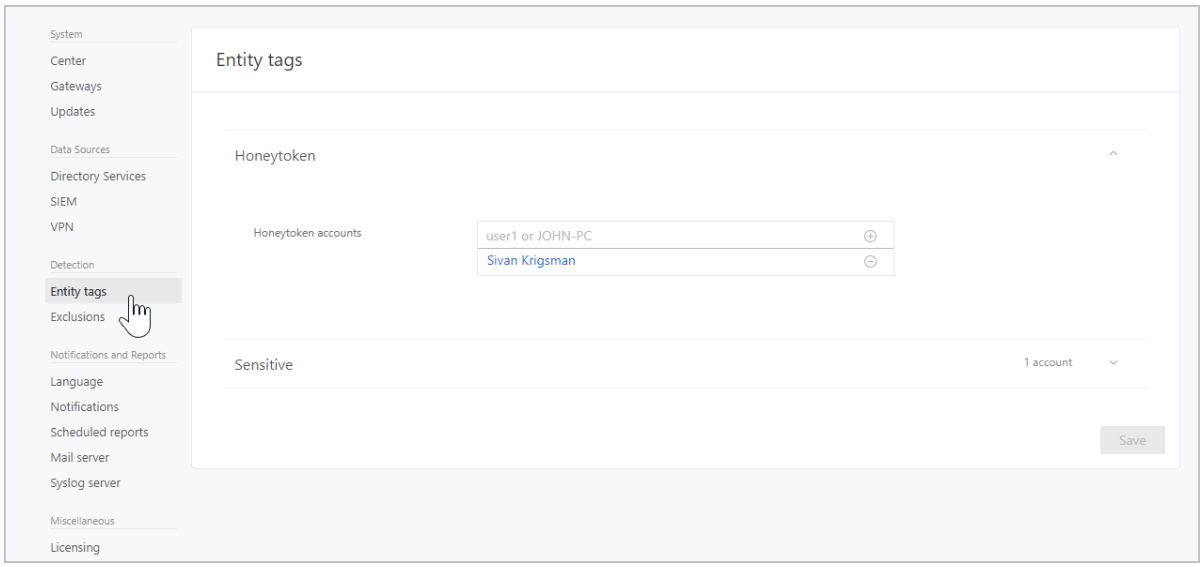
Tag sensitive accounts

7/20/2020 • 2 minutes to read • Edit Online

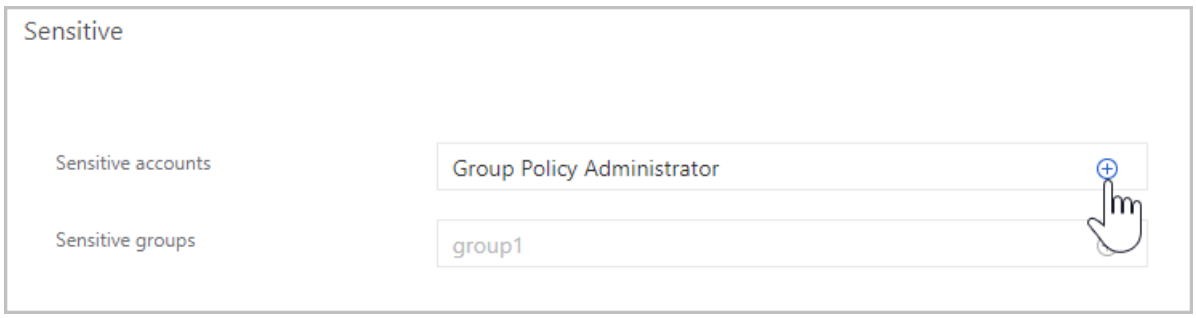
Applies to: Advanced Threat Analytics version 1.9

You can manually tag groups or accounts as sensitive to enhance detections. It is important to make sure this is updated because some ATA detections, such as sensitive group modification detection and lateral movement path, rely on which groups and accounts are considered sensitive. Previously, ATA automatically considered an entity *sensitive* if it was a member of a specific list of groups. You can now manually tag other users or groups as sensitive, such as board members, company executives, director of sales, etc., and ATA will consider them sensitive.

1. In the ATA console, click the **Configuration** cog in the menu bar.
2. Under **Detection,** click **Entity tags**.



3. In the **Sensitive** section, type the name of the **Sensitive accounts** and **Sensitive groups** and then click **+** sign to add them.



4. Click **Save**.
5. Go to the entity profile page by clicking on the entity name. Here you will be able to see why the entity is considered sensitive - whether it is because of membership in a group or because of manual tagging as sensitive.

Sensitive groups

The following list of groups are considered Sensitive by ATA. Any entity that is a member of these groups is considered sensitive:

- Administrators
- Power Users
- Account Operators
- Server Operators
- Print Operators
- Backup Operators
- Replicators
- Remote Desktop Users
- Network Configuration Operators
- Incoming Forest Trust Builders
- Domain Admins
- Domain Controllers
- Group Policy Creator Owners
- read-only Domain Controllers
- Enterprise Read-only Domain Controllers
- Schema Admins
- Enterprise Admins

See also

Check out the ATA forum!

Working with Suspicious Activities

7/20/2020 • 3 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

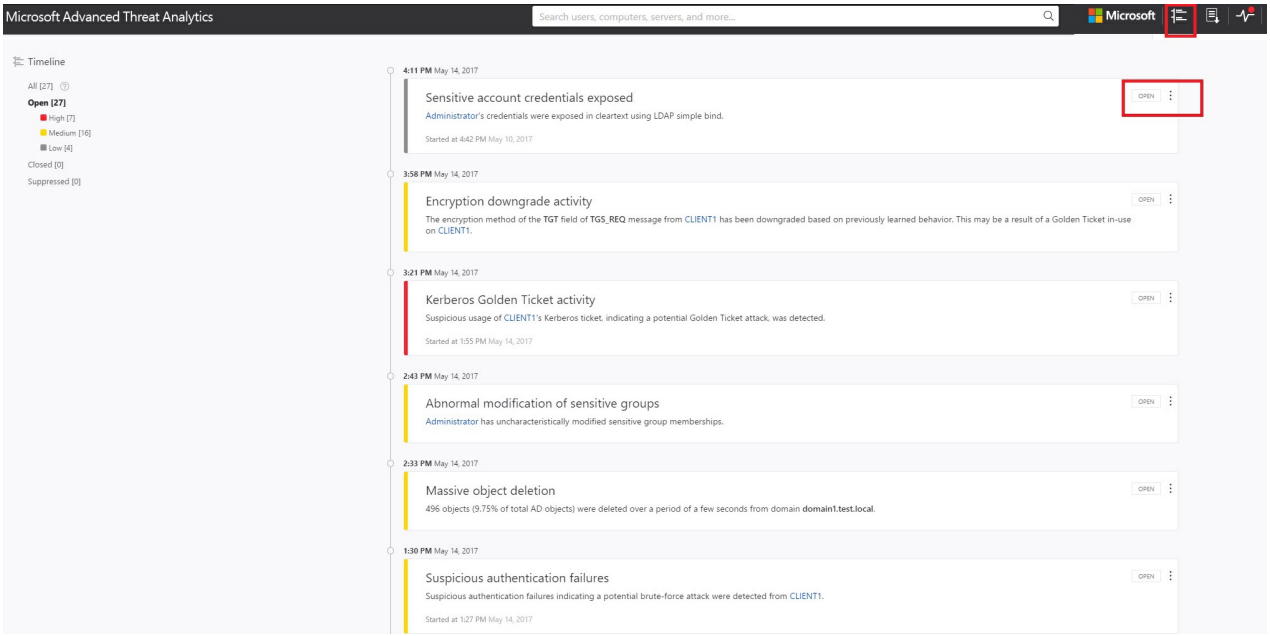
This article explains the basics of how to work with Advanced Threat Analytics.

Review suspicious activities on the attack time line

After logging in to the ATA Console, you are automatically taken to the open **Suspicious Activities Time Line**. Suspicious activities are listed in chronological order with the newest suspicious activities on the top of the time line. 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, closed, or suppressed.
- Ability to
  - Share the suspicious activity with other people in your organization via email.
  - Export the suspicious activity to Excel.

> **NOTE**
> - When you hover your mouse 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 that the entity is linked to.
> - If you click on an entity, it takes you to the entity profile of the user or computer.



Filter suspicious activities list

To filter the suspicious activities list:

1. In the **Filter by** pane on the left side of the screen, select one of the following options: **All**, **Open**, **Closed**, or **Suppressed**.
2. To further filter the list, select **High**, **Medium**, or **Low**.

Suspicious activity severity

- **Low**

  Indicates suspicious activities that can lead to attacks designed for malicious users or software to gain access to organizational data.

- **Medium**

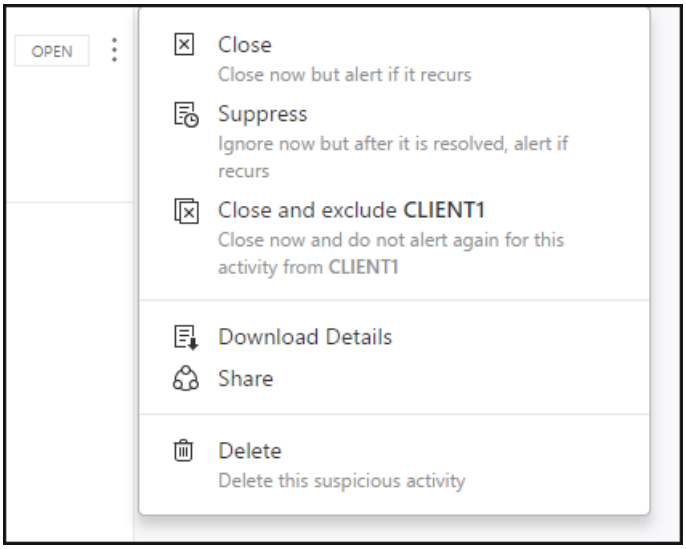
  Indicates suspicious activities that can put specific identities at risk for more severe attacks that could result in identity theft or privileged escalation

- **High**

  Indicates suspicious activities that can lead to identity theft, privilege escalation, or other high-impact attacks

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.



Suspicious activity status

- **Open**: All new suspicious activities appear in this list.
- **Close**: Is used to track suspicious activities that you identified, researched, and fixed for mitigated.

  > **NOTE**
  > If the same activity is detected again within a short period of time, ATA may reopen a closed activity.

- **Suppress**: Suppressing an activity means you want to ignore it for now, and only be alerted again if there's a new instance. This means that if there's a similar alert ATA doesn't reopen it. But if the alert stops for seven days, and is then seen again, you are alerted again.

- **Delete**: If you Delete an alert, it is deleted from the system, from the database and you will NOT be able to restore it. After you click delete, you'll be able to delete all suspicious activities of the same type.
- **Exclude**: The ability to exclude an entity from raising more of a certain type of alerts. For example, you can set ATA to exclude a specific entity (user or computer) from alerting again for a certain type of suspicious activity, such as a specific admin who runs remote code or a security scanner that does DNS reconnaissance. In addition to being able to add exclusions directly on the Suspicious activity as it is detected in the time line, you can also go to the Configuration page to **Exclusions**, and for each suspicious activity you can manually add and remove excluded entities or subnets (for example for Pass-the-Ticket).

> **NOTE**
> The configuration pages can only be modified by ATA admins.

Related Videos

- Joining the security community

See Also

- ATA suspicious activity playbook
- Check out the ATA forum!
- Modifying ATA configuration

Working with the ATA Console

7/20/2020 • 4 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

Use the ATA console to monitor and respond to suspicious activity detected by ATA.

Typing the `?` key provides keyboard shortcuts for ATA Portal accessibility.

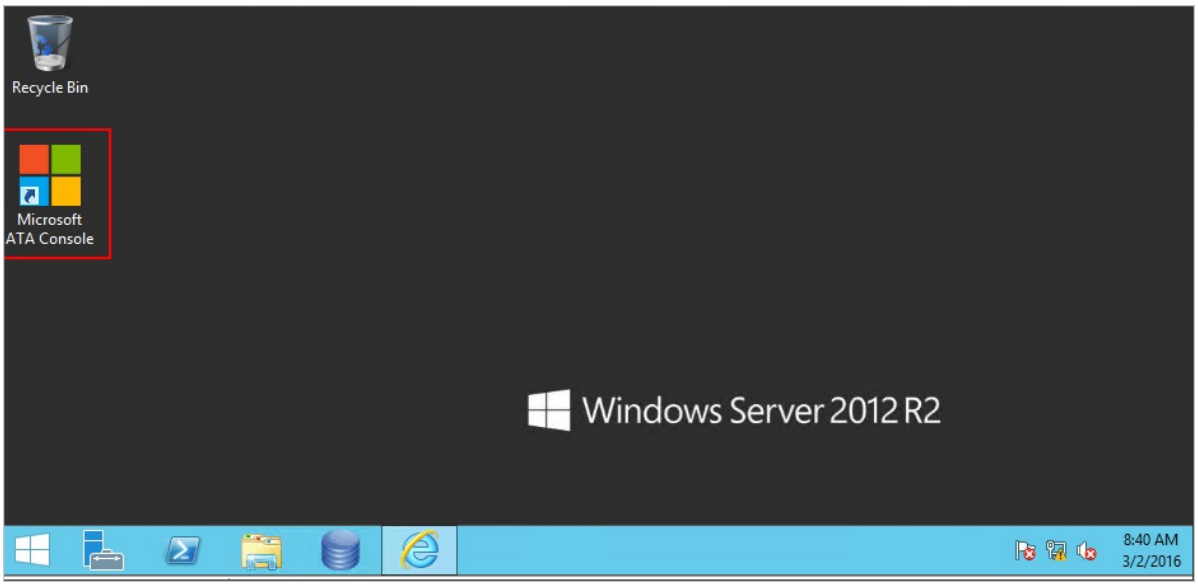
Enabling access to the ATA Console

To successfully log in to the ATA Console, you have to log in with a user who was assigned the proper ATA role to access the ATA Console. For more information about role-based access control (RBAC) in ATA, see Working with ATA role groups.

Logging into the ATA Console

> **NOTE**
> Starting with ATA 1.8, the log in process to the ATA Console is accomplished using single sign-on.

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.



> **NOTE**
> You can also open a browser from either the ATA Center or the ATA Gateway and browse to the IP address you 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 on to your computer, ATA uses that token to log you into the ATA Console. You can also log in using a smartcard. Your permissions in ATA correspond with your administrator role.

> **NOTE**
>
> Make sure to log on to the computer from which you want to access the ATA Console using your ATA admin username and password. Alternatively, you can run your browser as a different user or log out of Windows and log on with your ATA admin user. To prompt the ATA Console to ask for credentials, access the console using an IP address and you are prompted to enter credentials.

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 a localhost.

> **NOTE**
>
> In addition to logging each suspicious activity and health alert, every configuration change you make in the ATA Console is audited in the Windows Event Log on the ATA Center machine, under **Applications and services log** and then **Microsoft ATA**. Each login to the ATA console is audited as well.
> Configuration affecting the ATA Gateway is also logged in the Windows Event Log of the ATA Gateway machine.

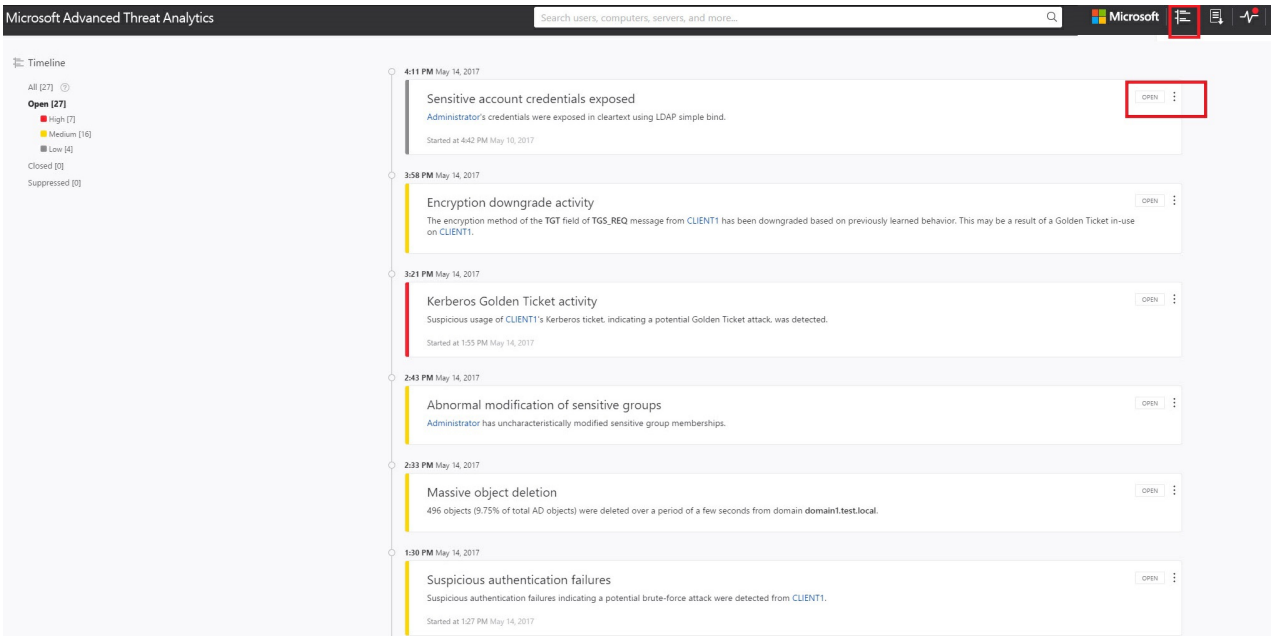
The ATA Console

The ATA Console provides you a quick view of all suspicious activities in chronological order. It enables you to drill into details of any activity and perform actions based on those activities. The console also displays alerts and notifications to highlight problems with the ATA network or new activities that are deemed suspicious.

These are the key elements of the ATA console.

Attack time line

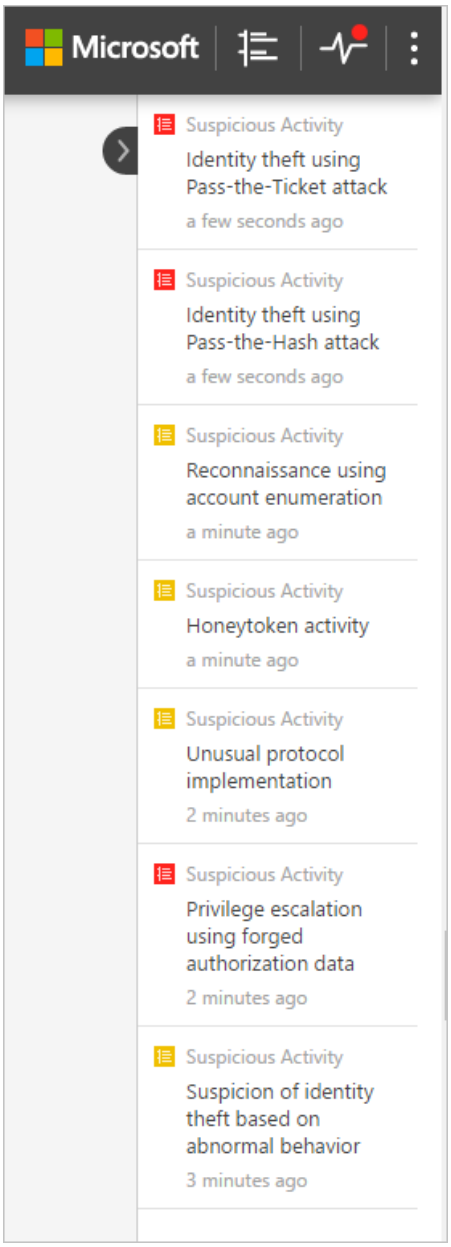
This is the default landing page you are taken to when you log in to the ATA Console. By default, all open suspicious activities are shown on the attack time line. You can filter the attack time line to show All, Open, Dismissed or Suppressed suspicious activities. You can also see the severity assigned to each activity.



For more information, see Working with suspicious activities.

Notification bar

When a new suspicious activity is detected, the notification bar opens automatically on the right-hand side. If there are new suspicious activities since the last time you logged in, the notification bar will open after you have successfully logged in. You can click the arrow on the right at any time to access the notification bar.



What's new

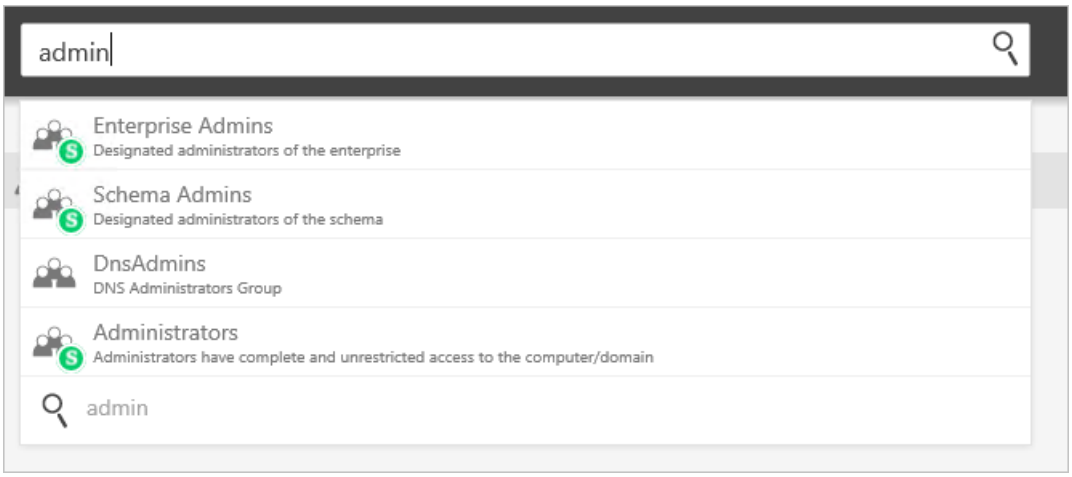
After a new version of ATA is released, the **What's new** window appears in the top right to let you know what was added in the latest version. It also provides you with a link to the version download.

Filtering panel

You can filter which suspicious activities are displayed in the attack time line or displayed in the entity profile suspicious activities tab based on Status and Severity.

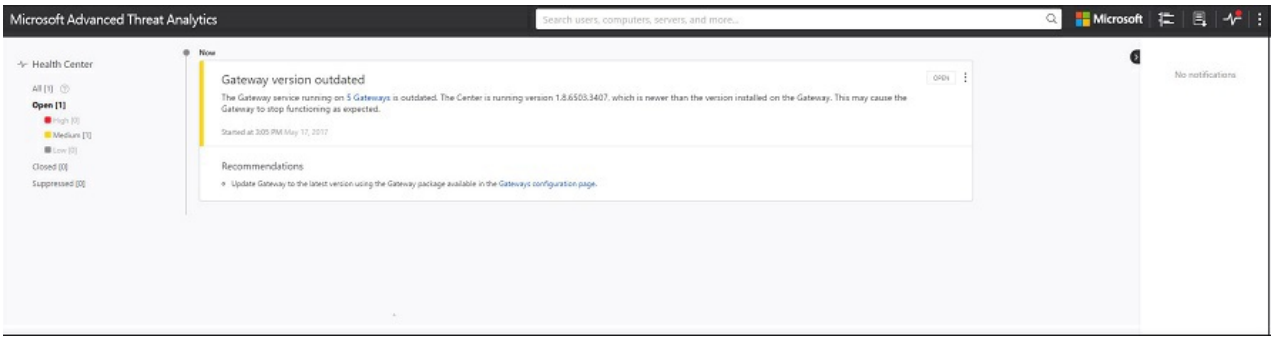
Search bar

In the top menu, you can find a search bar. You can search for a specific user, computer, or groups in ATA. To give it a try, just start typing.

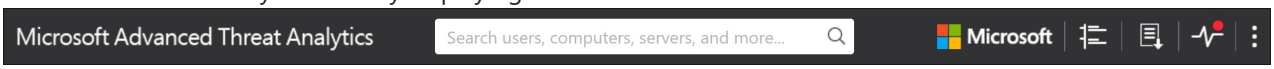


Health Center

The Health Center provides you with alerts when something isn't working properly in your ATA deployment.



Any time your system encounters a problem, such as a connectivity error or a disconnected ATA Gateway, the Health Center icon lets you know by displaying a red dot.



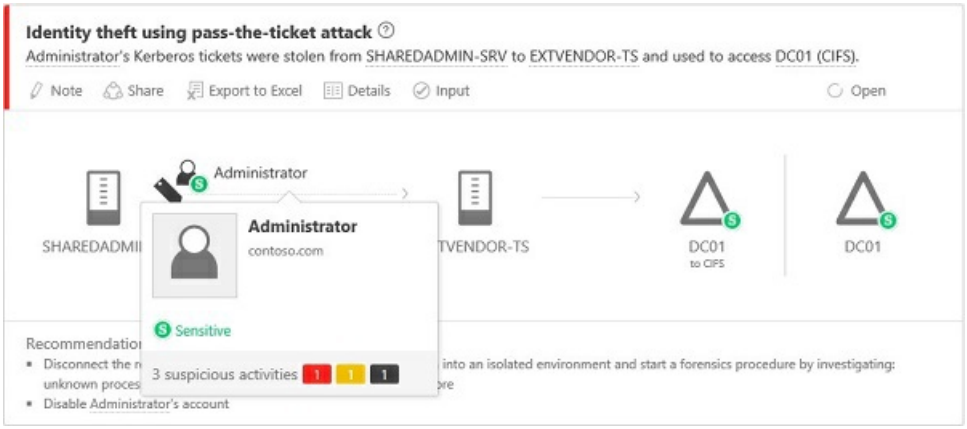
Sensitive groups

The following list of groups are considered **Sensitive** by ATA. Any entity that is a member of these groups is considered sensitive:

- Enterprise Read Only Domain Controllers
- Domain Admins
- Domain Controllers
- Schema Admins,
- Enterprise Admins
- Group Policy Creator Owners
- Read Only Domain Controllers
- Administrators
- Power Users
- Account Operators
- Server Operators
- Print Operators,
- Backup Operators,
- Replicators
- Remote Desktop Users
- Network Configuration Operators
- Incoming Forest Trust Builders
- DNS Admins

Mini profile

If you hover your mouse over an entity, anywhere in the console where there is a single entity presented, such as a user, or a computer, a mini profile automatically opens displaying the following information if available:



- Name
- Picture
- Email
- Telephone
- Number of suspicious activities by severity

See Also

Check out the ATA forum!

Investigating entity profiles

7/20/2020 • 3 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

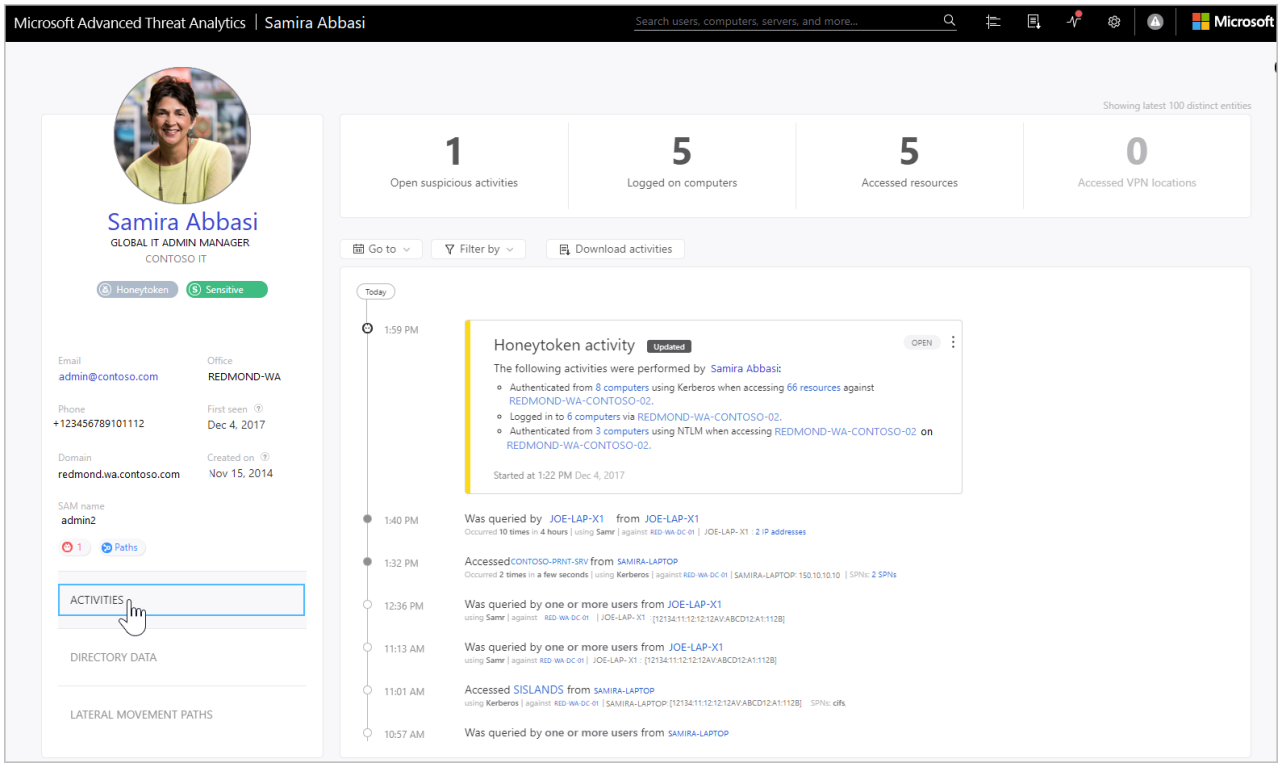
The entity profile provides you with a dashboard designed for full deep-dive investigation of users, computers, devices and the resources they have access to and their history. The profile page takes advantage of the new ATA logical activity translator which can look at a group of activities occurring (aggregated up to a minute) and group them into a single logical activity to give you a better understanding of the actual activities of your users.

To access an entity profile page, click on the name of the entity, such as a username, in the suspicious activity timeline.

The left menu provides you with all the Active Directory information available on the entity - email address, domain, first seen date. If the entity is sensitive it will tell you why. For example, is the user tagged as sensitive or the member of a sensitive group? If it's a sensitive user you'll see the icon under the user's name.

View entity activities

To view all the activities performed by the user, or performed on an entity, click on the **Activities** tab.

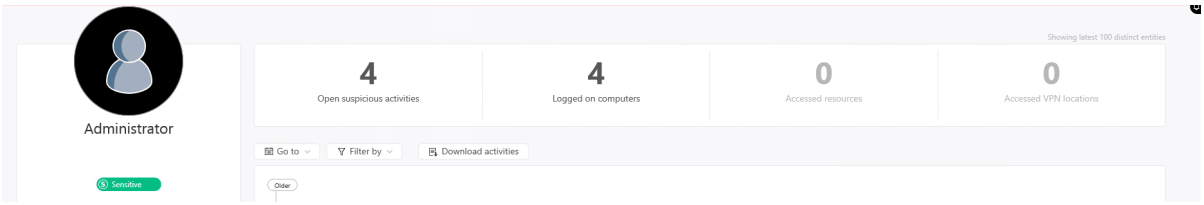


By default, the main pane of the entity profile displays a timeline of the entity's activities with a history of up to 6 months back, from which you can also drill down into the entities accessed by the user, or for entities, users who accessed the entity.

At the top, you can view the summary tiles that give you a quick overview of what you need to understand in a glance about your entity. These tiles change based on what type of entity it is, for a user, you will see:

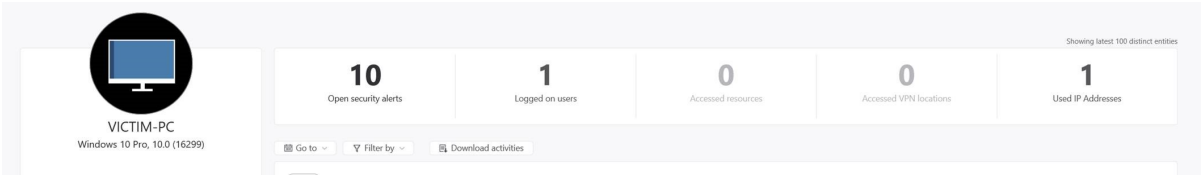
- How many open suspicious activities there are for the user
- How many computers the user logged onto

- How many resources the user accessed
- From which locations the user logged into VPN



For computers you can see:

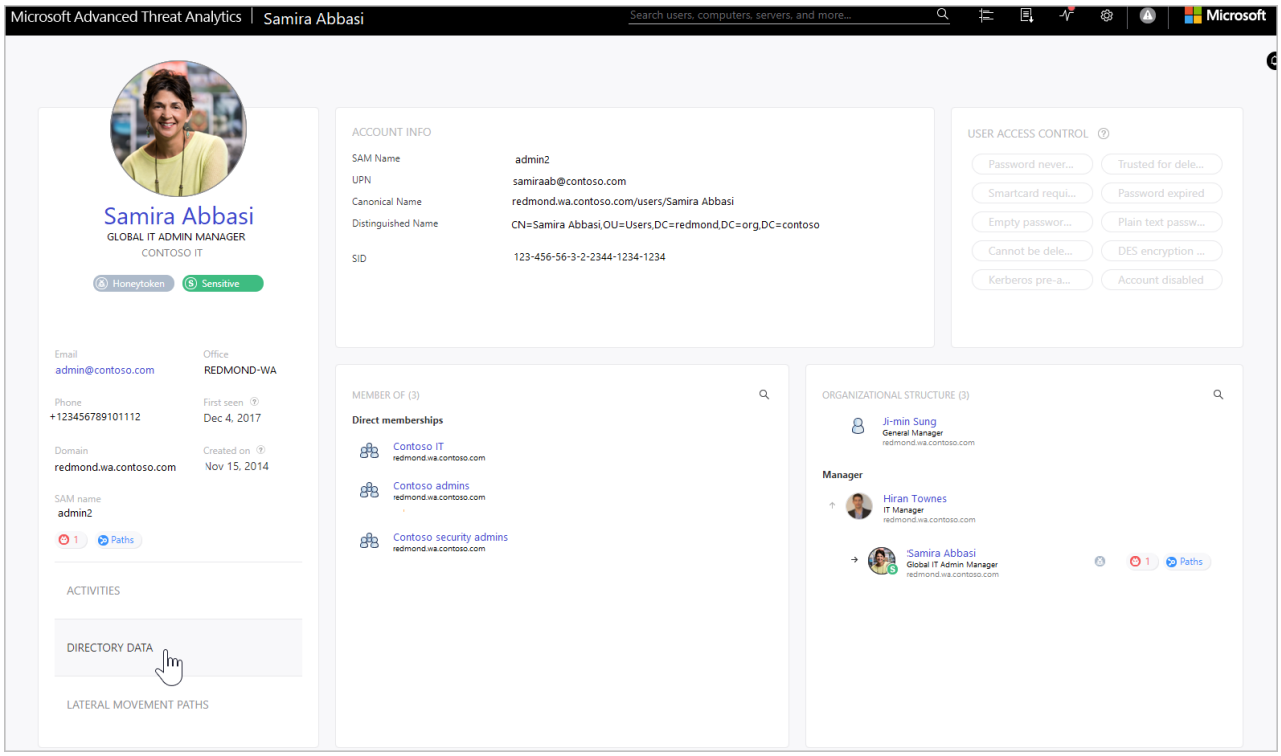
- How many open suspicious activities there are for the machine
- How many users logged into the machine
- How many resources the computer accessed
- How many locations VPN was accessed from on the computer
- A list of which IP addresses the computer has used



Using the **Filter by** button above the activity timeline, you can filter the activities by activity type. You can also filter out a specific (noisy) type of activity. This is really helpful for investigation when you want to understand the basics of what an entity is doing in the network. You can also go to a specific date, and you can export the activities as filtered to Excel. The exported file provides a page for directory services changes (things that changed in Active Directory for the account) and a separate page for activities.

View directory data

The **Directory data** tab provides the static information available from Active Directory, including user access control security flags. ATA also displays group memberships for the user so that you can tell if the user has a direct membership or a recursive membership. For groups, ATA lists members of the group.

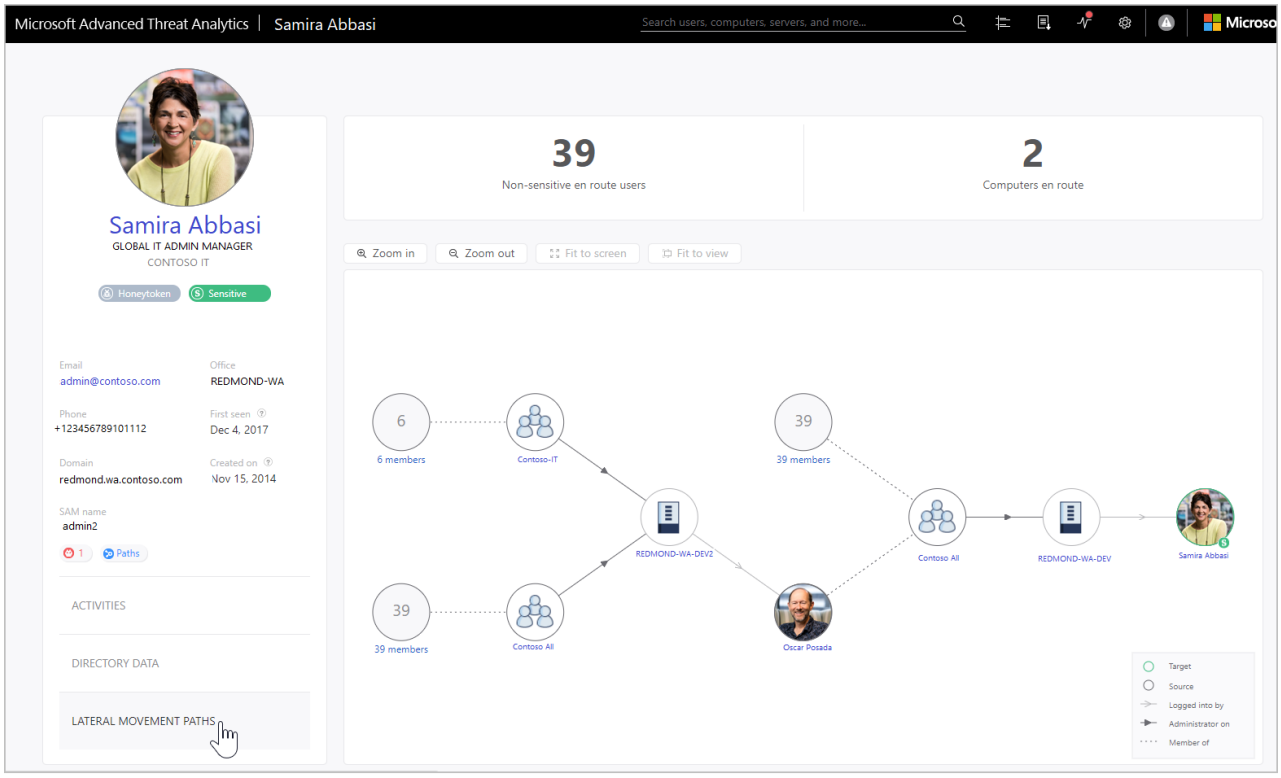


In the **User access control** section, ATA surfaces security settings that may need your attentions. You can see important flags about the user, such as can the user press enter to bypass the password, does the user have a password that never expires, etc.

View lateral movement paths

By clicking the **Lateral movement paths** tab you can view a fully dynamic and clickable map that provides you with a visual representation of the lateral movement paths to and from this user that can be used to infiltrate your network.

The map provides you with a list of how many hops between computers or users an attacker would have to and from this user to compromise a sensitive account, and if the user themselves has a sensitive account, you can see how many resources and accounts are directly connected. For more information, see Lateral movement paths.



See Also

Check out the ATA forum!

Investigate lateral movement paths with ATA

7/20/2020 • 3 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

Even when you do your best to protect your sensitive users, and your admins have complex passwords that they change frequently, their machines are hardened, and their data is stored securely, attackers can still use lateral movement paths to access sensitive accounts. In lateral movement attacks, the attacker takes advantage of instances when sensitive users sign in to a machine where a non-sensitive user has local rights. Attackers can then move laterally, accessing the less sensitive user and then moving across the computer to gain credentials for the sensitive user.

What is a lateral movement path?

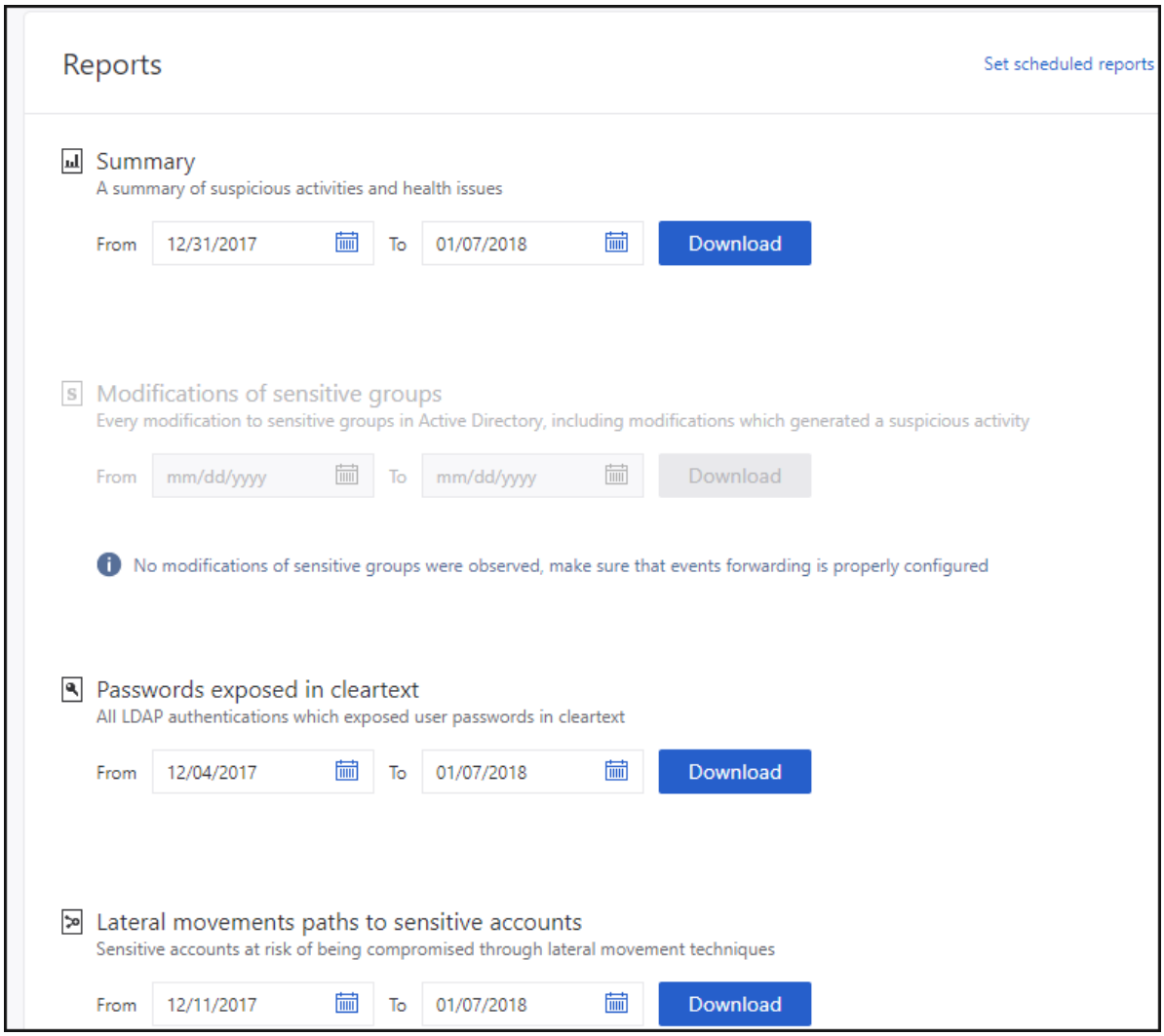
Lateral movement is when an attacker uses non-sensitive accounts to gain access to sensitive accounts. This can be done using the methods described in the Suspicious activity guide. Attackers use lateral movement to identify the administrators in your network and learn which machines they can access. With this information, and further moves, the attacker can take advantage of the data on your domain controllers.

ATA enables you to take preemptive action on your network to prevent attackers from succeeding at lateral movement.

Discovery your at-risk sensitive accounts

To discover which sensitive accounts in your network are vulnerable because of their connection to non-sensitive accounts or resources, in a specific timeframe, follow these steps:

1. In the ATA console menu, click the reports icon  .
2. Under **Lateral movements paths to sensitive accounts**, if there are no lateral movement paths found, the report is grayed out. If there are lateral movement paths, then the dates of the report automatically select the first date when there is relevant data.

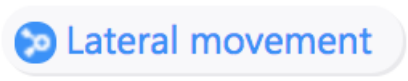


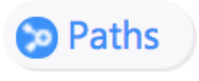
3. Click **Download**.

4. The Excel file that is created provides you with details about your sensitive accounts at risk. The **Summary** tab provides graphs that detail the number of sensitive accounts, computers, and averages for at-risk resources. The **Details** tab provides a list of the sensitive accounts that you should be concerned about. Note that the paths are paths that existed previously, and may not be available today.

Investigate

Now that you know which sensitive accounts are at risk, you can deep dive in ATA to learn more and take preventative measures.

1. In the ATA console, search for the Lateral movement badge that's added to the entity profile when the entity is in a lateral movement path 

or 

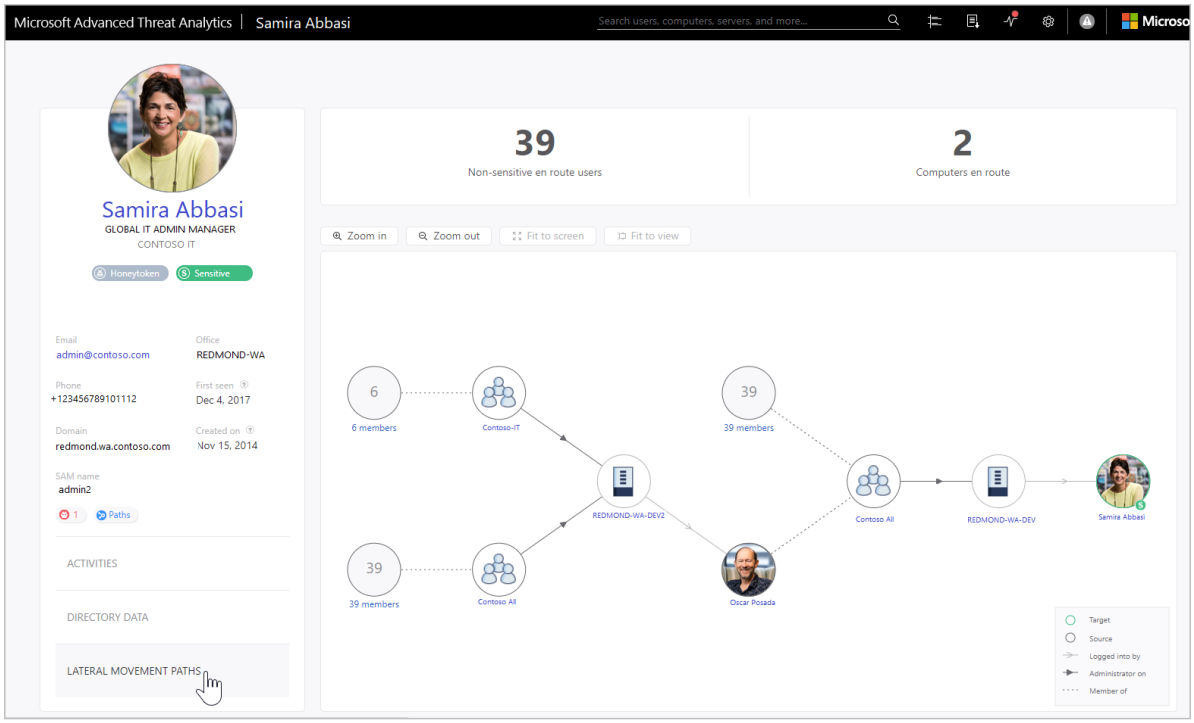
. This is available if there was a lateral movement path in the last two days.

2. In the user profile page that opens, click the **Lateral movement paths** tab.

3. The graph that is displayed provides a map of the possible paths to the sensitive user. The graph shows connections that have been made over the last two days.

4. Review the graph to see what you can learn about exposure of your sensitive user's credentials. For example, in this map, you can follow the **Logged into by** gray arrows to see where Samira signed in with their privileged credentials. In this case, Samira's sensitive credentials were saved on the computer REDMOND-WA-DEV. Then, see which other users signed in to which computers that created the most

exposure and vulnerability. You can see this by looking at the **Administrator on** black arrows to see who has admin privileges on the resource. In this example, everyone in the group **Contoso All** has the ability to access user credentials from that resource.



Preventative best practices

- The best way to prevent lateral movement is to make sure that sensitive users use their administrator credentials only when they sign in to hardened computers where there is no non-sensitive user who has admin rights on the same computer. In the example, make sure that if Samira needs access to REDMOND-WA-DEV, they sign in with a username and password other than their admin credentials, or remove the Contoso All group from the local administrators group on REDMOND-WA-DEV.
- It is also recommended that you make sure that no one has unnecessary local administrative permissions. In the example, check to see if everyone in Contoso All really needs admin rights on REDMOND-WA-DEV.
- Make sure people only have access to necessary resources. In the example, Oscar Posada significantly widens Samira's exposure. Is it necessary that they be included in the group **Contoso All**? Are there subgroups that you could create to minimize exposure?

> **TIP**
> If activity is not detected during the last two days, the graph does not appear, but the lateral movement path report is still available to provide information about lateral movement paths over the last 60 days.

> **TIP**
> For instructions about how to set your servers to allow ATA to perform the SAM-R operations needed for lateral movement path detection, configure SAM-R.

See also

- Work with suspicious activities
- Check out the ATA forum!

ATA SIEM log reference

7/20/2020 • 6 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

ATA can forward security and health alert events to your SIEM. Alerts are forwarded in the CEF format. A sample of each type of security alert log to be sent to your SIEM, is below.

Sample ATA security alerts in CEF format

The following fields and their values are forwarded to your SIEM:

- start – Time the alert started
- suser – Account (normally user account), involved in the alert
- shost – Source machine of the alert
- outcome – Alerts with defined activity success or failure performed in the alert
- msg – Alert description
- cnt – Alerts with a count of the number of times the alert happened (for example brute force has an amount of guessed passwords)
- app – Alert protocol
- externalId – Event ID ATA writes to the event log that corresponds to the alert*
- cs#label & cs# – Customer strings that CEF allows to use the cs#label is the name of the new field, and cs# is the value, for example: cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5909ae198ca1ec04d05e65fa

In this example, cs1 is a field that has a URL to the alert.

*If you create scripts or automation based on logs, use the permanent externalID of each log in place of using the log names, as log names are subject to change without notice.

ALERT NAMES	ALERT EVENT IDS
2001	Suspicion of identity theft based on abnormal behavior
2002	Unusual protocol implementation
2003	Reconnaissance using account enumeration
2004	Brute force attack using LDAP simple bind
2006	Malicious replication of Directory Services
2007	Reconnaissance using DNS
2008	Encryption downgrade activity
2009	Encryption downgrade activity (potential golden ticket)
2010	Encryption downgrade activity (potential overpass-the-hash)

ALERT NAMES	ALERT EVENT IDS
2011	Encryption downgrade activity (potential skeleton key)
2012	Reconnaissance using SMB session enumeration
2013	Privilege escalation using forged authorization data
2014	Honeytoken activity
2016	Massive object deletion
2017	Identity theft using Pass-the-Hash attack
2018	Identity theft using Pass-the-Ticket attack
2019	Remote execution attempt detected
2020	Malicious data protection private information request
2021	Reconnaissance using Directory Services queries
2022	Kerberos Golden Ticket activity
2023	Suspicious authentication failures
2024	Abnormal modification of sensitive groups
2026	Suspicious service creation

Sample logs

Priorities: 3=Low 5=Medium 10=High

Abnormal modification of sensitive groups

1 2018-12-12T16:53:22.925757+00:00 CENTER ATA 4688 AbnormalSensitiveGroupMembership CEF:0|Microsoft|ATA|1.9.0.0|AbnormalSensitiveGroupMembershipChangeSuspiciousActivity|Abnormal modification of sensitive groups|5|start=2018-12-12T18:52:58.0000000Z app=GroupMembershipChangeEvent suser=krbtgt msg=krbtgt has uncharacteristically modified sensitive group memberships. externalId=2024 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c113d028ca1ec1250ca0491

Brute force attack using LDAP simple bind

12-12-2018 19:52:18 Auth.Warning 192.168.0.222 1 2018-12-12T17:52:18.899690+00:00 CENTER ATA 4688 LdapBruteForceSuspiciousActivity ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|LdapBruteForceSuspiciousActivity|Brute force attack using LDAP simple bind|5|start=2018-12-12T17:52:10.2350665Z app=Ldap msg=10000 password guess attempts were made on 100 accounts from W2012R2-000000-Server. One account password was successfully guessed. externalId=2004 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114acb8ca1ec1250cacdcb

Encryption downgrade activity (Golden Ticket)

12-12-2018 20:12:35 Auth.Warning 192.168.0.222 1 2018-12-12T18:12:35.105942+00:00 CENTER ATA 4688 EncryptionDowngradeSuspiciousAct
‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|EncryptionDowngradeSuspiciousActivity|Encryption downgrade activity|5|start=2018-12-12T18:10:35.0334169Z app=Kerberos msg=The encryption method of the TGT field of

TGS_REQ message from W2012R2-000000-Server has been downgraded based on previously learned behavior. This may be a result of a Golden Ticket in-use on W2012R2-000000-Server. externalId=2009 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114f938ca1ec1250cafcfa

Encryption downgrade activity (overpass-the-hash)

12-12-2018 19:00:31 Auth.Warning 192.168.0.222 1 2018-12-12T17:00:31.963485+00:00 CENTER ATA 4688 EncryptionDowngradeSuspiciousAct ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|EncryptionDowngradeSuspiciousActivity|Encryption downgrade activity|5|start=2018-12-12T17:00:31.2975188Z app=Kerberos msg=The encryption method of the Encrypted_Timestamp field of AS_REQ message from W2012R2-000000-Server has been downgraded based on previously learned behavior. This may be a result of a credential theft using Overpass-the-Hash from W2012R2-000000-Server. externalId=2010 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c113eaf8ca1ec1250ca0883

Encryption downgrade activity (Skeleton Key)

12-12-2018 20:07:24 Auth.Warning 192.168.0.222 1 2018-12-12T18:07:24.065140+00:00 CENTER ATA 4688 EncryptionDowngradeSuspiciousAct ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|EncryptionDowngradeSuspiciousActivity|Encryption downgrade activity|5|start=2018-12-12T18:07:24.0222746Z app=Kerberos msg=The encryption method of the ETYPE_INFO2 field of KRB_ERR message from W2012R2-000000-Server has been downgraded based on previously learned behavior. This may be a result of a Skeleton Key on DC1. externalId=2011 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114e5c8ca1ec1250cafafe

Honeytoken activity

12-12-2018 19:51:52 Auth.Warning 192.168.0.222 1 2018-12-12T17:51:52.659618+00:00 CENTER ATA 4688 HoneytokenActivitySuspiciousActi ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|HoneytokenActivitySuspiciousActivity|Honeytoken activity|5|start=2018-12-12T17:51:52.5855994Z app=Kerberos suser=USR78982 msg=The following activities were performed by USR78982 LAST78982:\r\nAuthenticated from CLIENT1 using NTLM when accessing domain1.test.local\cifs on DC1. externalId=2014 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114ab88ca1ec1250ca7f76

Identity theft using Pass-the-Hash attack

12-12-2018 19:56:02 Auth.Error 192.168.0.222 1 2018-12-12T17:56:02.047236+00:00 CENTER ATA 4688 PassTheHashSuspiciousActivity ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|PassTheHashSuspiciousActivity|Identity theft using Pass-the-Hash attack|10|start=2018-12-12T17:54:01.9582400Z app=Ntlm suser=USR46829 LAST46829 msg=USR46829 LAST46829's hash was stolen from one of the computers previously logged into by USR46829 LAST46829 and used from W2012R2-000000-Server. externalId=2017 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114bb28ca1ec1250caf673

Identity theft using Pass-the-Ticket attack

12-12-2018 22:03:51 Auth.Error 192.168.0.222 1 2018-12-12T20:03:51.643633+00:00 CENTER ATA 4688 PassTheTicketSuspiciousActivity ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|PassTheTicketSuspiciousActivity|Identity theft using Pass-the-Ticket attack|10|start=2018-12-12T17:54:12.9960662Z app=Kerberos suser=Birdie Lamb msg=Birdie Lamb (Software Engineer)'s Kerberos tickets were stolen from W2012R2-000106-Server to W2012R2-000051-Server and used to access domain1.test.local\host. externalId=2018 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114b458ca1ec1250caf5b7

Kerberos Golden Ticket activity

12-12-2018 19:53:26 Auth.Error 192.168.0.222 1 2018-12-12T17:53:26.869091+00:00 CENTER ATA 4688 GoldenTicketSuspiciousActivity ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|GoldenTicketSuspiciousActivity|Kerberos Golden Ticket activity|10|start=2018-12-13T06:51:26.7290524Z app=Kerberos suser=Sonja Chadsey msg=Suspicious usage of Sonja Chadsey (Software Engineer)'s Kerberos ticket, indicating a potential Golden Ticket attack, was detected. externalId=2022 cs1Label=url

cs1=https://192.168.0.220/suspiciousActivity/5c114b168ca1ec1250caf556

Malicious data protection private information request

12-12-2018 20:03:49 Auth.Error 192.168.0.222 1 2018-12-12T18:03:49.814620+00:00 CENTER ATA 4688 RetrieveDataProtectionBackupKeyS
‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|RetrieveDataProtectionBackupKeySuspiciousActivity|Malicious data protection private information request|10|start=2018-12-12T17:58:56.3537533Z app=LsaRpc shost=W2012R2-000000-Server msg=An unknown user performed 1 successful attempt from W2012R2-000000-Server to retrieve DPAPI domain backup key from DC1. externalId=2020 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114d858ca1ec1250caf983

Malicious replication of Directory Services

12-12-2018 19:56:49 Auth.Error 192.168.0.222 1 2018-12-12T17:56:49.312648+00:00 CENTER ATA 4688 DirectoryServicesReplicationSusp
‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|DirectoryServicesReplicationSuspiciousActivity|Malicious replication of Directory Services|10|start=2018-12-12T17:52:34.3287329Z app=Drsr shost=W2012R2-000000-Server msg=Malicious replication requests were successfully performed from W2012R2-000000-Server against DC1. outcome=Success externalId=2006 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114be18ca1ec1250caf6b8

Privilege escalation using forged authorization data

12-12-2018 19:51:15 Auth.Error 192.168.0.222 1 2018-12-12T17:51:15.658608+00:00 CENTER ATA 4688 ForgedPacSuspiciousActivity ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|ForgedPacSuspiciousActivity|Privilege escalation using forged authorization data|10|start=2018-12-12T17:51:15.0261128Z app=Kerberos suser=triservice msg=triservice attempted to escalate privileges against DC1 from W2012R2-000000-Server by using forged authorization data. externalId=2013 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114a938ca1ec1250ca7f48

Reconnaissance using Directory Services queries

12-12-2018 20:23:52 Auth.Warning 192.168.0.222 1 2018-12-12T18:23:52.155531+00:00 CENTER ATA 4688 SamrReconnaissanceSuspiciousActi
‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|SamrReconnaissanceSuspiciousActivity|Reconnaissance using Directory Services queries|5|start=2018-12-12T18:04:12.9868815Z app=Samr shost=W2012R2-000000-Server msg=The following directory services queries using SAMR protocol were attempted against DC1 from W2012R2-000000-Server:\r\nSuccessful query about Incoming Forest Trust Builders (Members of this group can create incoming, one-way trusts to this forest) in domain1.test.local externalId=2021 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114e758ca1ec1250cafb2e

Reconnaissance using account enumeration

1 2018-12-12T16:57:09.661680+00:00 CENTER ATA 4688 AccountEnumerationSuspiciousActi CEF:0|Microsoft|ATA|1.9.0.0|AccountEnumerationSuspiciousActivity|Reconnaissance using account enumeration|5|start=2018-12-12T16:57:09.1706828Z app=Kerberos shost=W2012R2-000000-Server msg=Suspicious account enumeration activity using Kerberos protocol, originating from W2012R2-000000-Server, was detected. The attacker performed a total of 100 guess attempts for account names, 1 guess attempt matched existing account names in Active Directory. externalId=2003 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c113de58ca1ec1250ca06d8

Reconnaissance using DNS

1 2018-12-12T16:57:20.743634+00:00 CENTER ATA 4688 DnsReconnaissanceSuspiciousActiv CEF:0|Microsoft|ATA|1.9.0.0|DnsReconnaissanceSuspiciousActivity|Reconnaissance using DNS|5|start=2018-12-12T16:57:20.2556472Z app=Dns shost=W2012R2-000000-Server msg=Suspicious DNS activity was observed, originating from W2012R2-000000-Server (which is not a DNS server) against DC1. externalId=2007 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c113df08ca1ec1250ca074c

Reconnaissance using SMB session enumeration

12-12-2018 19:50:51 Auth.Warning 192.168.0.222 1 2018-12-12T17:50:51.090247+00:00 CENTER ATA 4688 EnumerateSessionsSuspiciousActiv
‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|EnumerateSessionsSuspiciousActivity|Reconnaissance using SMB session enumeration|5|start=2018-12-12T17:00:42.7234229Z app=SrvSvc shost=W2012R2-000000-Server msg=SMB session enumeration attempts failed from W2012R2-000000-Server against DC1. No accounts were exposed. externalId=2012 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114a788ca1ec1250ca7735

Remote execution attempt detected

12-12-2018 19:58:45 Auth.Warning 192.168.0.222 1 2018-12-12T17:58:45.082799+00:00 CENTER ATA 4688 RemoteExecutionSuspiciousActivit ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|RemoteExecutionSuspiciousActivity|Remote execution attempt detected|5|start=2018-12-12T17:54:23.9523766Z shost=W2012R2-000000-Server msg=The following remote execution attempts were performed on DC1 from W2012R2-000000-Server:\r\nFailed remote scheduling of one or more tasks. externalId=2019 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114c548ca1ec1250caf783

Unusual protocol implementation

1 2018-12-12T16:50:46.930234+00:00 CENTER ATA 4688 AbnormalProtocolSuspiciousActivi CEF:0|Microsoft|ATA|1.9.0.0|AbnormalProtocolSuspiciousActivity|Unusual protocol implementation|5|start=2018-12-12T16:48:46.6480337Z app=Ntlm shost=W2012R2-000000-Server outcome=Success msg=triservice successfully authenticated from W2012R2-000000-Server against DC1 using an unusual protocol implementation. This may be a result of malicious tools used to execute attacks such as Pass-the-Hash and brute force. externalId=2002 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c113c668ca1ec1250ca0397

Suspicion of identity theft based on abnormal behavior

1 2018-12-12T16:50:35.746877+00:00 CENTER ATA 4688 AbnormalBehaviorSuspiciousActivi CEF:0|Microsoft|ATA|1.9.0.0|AbnormalBehaviorSuspiciousActivity|Suspicion of identity theft based on abnormal behavior|5|start=2018-12-12T16:48:35.5501183Z app=Kerberos suser=USR45964 msg=USR45964 LAST45964 exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:\r\nPerformed interactive login from 30 abnormal workstations.\r\nRequested access to 30 abnormal resources. externalId=2001 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c113c5b8ca1ec1250ca0355

Suspicious authentication failures

12-12-2018 19:50:34 Auth.Warning 192.168.0.222 1 2018-12-12T17:04:25.214067+00:00 CENTER ATA 4688 BruteForceSuspiciousActivity ‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|BruteForceSuspiciousActivity|Suspicious authentication failures|5|start=2018-12-12T17:03:58.5892462Z app=Kerberos shost=W2012R2-000106-Server msg=Suspicious authentication failures indicating a potential brute-force attack were detected from W2012R2-000106-Server. externalId=2023 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c113f988ca1ec1250ca5810

Suspicious service creation

12-12-2018 19:53:49 Auth.Warning 192.168.0.222 1 2018-12-12T17:53:49.913034+00:00 CENTER ATA 4688 MaliciousServiceCreationSuspicio
‹ø¨CEF:0|Microsoft|ATA|1.9.0.0|MaliciousServiceCreationSuspiciousActivity|Suspicious service creation|5|start=2018-12-12T19:53:49.0000000Z app=ServiceInstalledEvent shost=W2012R2-000000-Server msg=triservice created FakeService in order to execute potentially malicious commands on W2012R2-000000-Server. externalId=2026 cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5c114b2d8ca1ec1250caf577

Health alerts

GatewayDisconnectedMonitoringAlert

1 2018-12-12T16:52:41.520759+00:00 CENTER ATA 4688 GatewayDisconnectedMonitoringAle CEF:0|Microsoft|ATA|1.9.0.0|GatewayDisconnectedMonitoringAlert|GatewayDisconnectedMonitoringAlert|5|external

Id=1011 cs1Label=url cs1=https://192.168.0.220/monitoring msg=There has not been communication from the Gateway CENTER for 5 minutes. Last communication was on 12/12/2018 4:47:03 PM UTC.

GatewayStartFailureMonitoringAlert

1 2018-12-12T15:36:59.701097+00:00 CENTER ATA 1372 GatewayStartFailureMonitoringAle CEF:0|Microsoft|ATA|1.9.0.0|GatewayStartFailureMonitoringAlert|GatewayStartFailureMonitoringAlert|5|externalId=1018 cs1Label=url cs1=https://192.168.0.220/monitoring msg=The Gateway service on DC1 failed to start. It was last seen running on 12/12/2018 3:04:12 PM UTC.

> **NOTE**
> All health alerts are sent with the same template as above.

See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

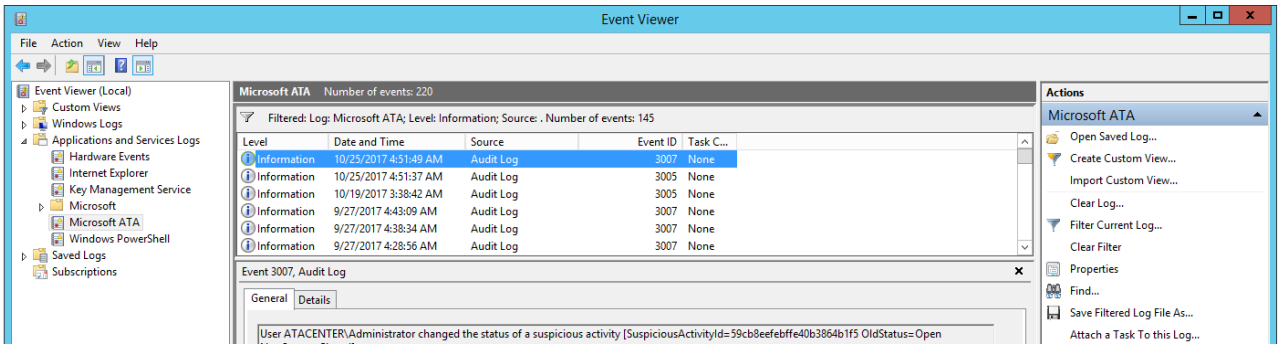
ATA event ID reference

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

The ATA Center event viewer logs events for ATA. This article provides a list of event IDs and provides a description of each.

The events can be found here:



ATA health events

EVENT ID	ALERT NAME
1001	Center running out of disk space
1003	Center overloaded
1004	Center certificate about to expire / Center certificate expired
1005	MongoDB is down
1006	Read-only user password to expire shortly / Read-only user password expired
1007	Domain synchronizer not assigned
1008	Some or All of the capture network adapters on a Gateway are not available
1009	A capture network adapter on a Gateway no longer exists
1010	Some domain controllers are unreachable by a Gateway / All domain controllers are unreachable by a Gateway
1011	Gateway stopped communicating
1012	Some forwarded events are not being analyzed
1013	Some network traffic is not being analyzed

EVENT ID	ALERT NAME
1014	Failure sending mail
1015	Failure connecting to the SIEM server using Syslog
1016	Gateway version outdated
1017	No traffic received from domain controller
1018	Gateway service failed to start
1019	Lightweight Gateway reached a memory resource limit
1020	Gateway is not processing Radius events
1021	Gateway is not processing Syslog events
1022	Geolocation service is unavailable

ATA security alert events

EVENT ID	ALERT NAME
2001	Suspicion of identity theft based on abnormal behavior
2002	Unusual protocol implementation
2003	Reconnaissance using account enumeration
2004	Brute force attack using LDAP simple bind
2006	Malicious replication of Directory Services
2007	Reconnaissance using DNS
2008	Encryption downgrade activity
2009	Encryption downgrade activity (potential golden ticket)
2010	Encryption downgrade activity (potential overpass-the-hash)
2011	Encryption downgrade activity (potential skeleton key)
2012	Reconnaissance using SMB session enumeration
2013	Privilege escalation using forged authorization data
2014	Honeytoken activity
2016	Massive object deletion

EVENT ID	ALERT NAME
2017	Identity theft using Pass-the-Hash attack
2018	Identity theft using Pass-the-Ticket attack
2019	Remote execution attempt detected
2020	Malicious data protection private information request
2021	Reconnaissance using Directory Services queries
2022	Kerberos Golden Ticket activity
2023	Suspicious authentication failures
2024	Abnormal modification of sensitive groups
2026	Suspicious service creation

ATA auditing events

EVENT ID	ALERT NAME
3001	Change to ATA configuration
3002	ATA Gateway added
3003	ATA Gateway deleted
3004	ATA license activated
3005	Log in to ATA console
3006	Manual change to health activity status
3007	Manual change to suspicious activity status

See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

Advanced Threat Analytics suspicious activity guide

7/20/2020 • 28 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

Following proper investigation, any suspicious activity can be classified as:

- **True positive**: A malicious action detected by ATA.
- **Benign true positive**: An action detected by ATA that is real but not malicious, such as a penetration test.
- **False positive**: A false alarm, meaning the activity didn't happen.

For more information on how to work with ATA alerts, see Working with suspicious activities.

For questions or feedback, contact the ATA team at ATAEval@microsoft.com.

Abnormal modification of sensitive groups

Description

Attackers add users to highly privileged groups. They do so to gain access to more resources and gain persistency. Detections rely on profiling the user group modification activities, and alerting when an abnormal addition to a sensitive group is seen. Profiling is continuously performed by ATA. The minimum period before an alert can be triggered is one month per domain controller.

For a definition of sensitive groups in ATA, see Working with the ATA console.

The detection relies on events audited on domain controllers. To make sure your domain controllers audit the needed events, use the tool referenced in ATA Auditing (AuditPol, Advanced Audit Settings Enforcement, Lightweight Gateway Service discovery).

Investigation

1. Is the group modification legitimate?
   Legitimate group modifications that rarely occur, and were not learned as "normal", might cause an alert, which would be considered a benign true positive.
2. If the added object was a user account, check which actions the user account took after being added to the admin group. Go to the user's page in ATA to get more context. Were there any other suspicious activities associated with the account before or after the addition took place? Download the **Sensitive group modification** report to see what other modifications were made and by whom during the same time period.

Remediation

Minimize the number of users who are authorized to modify sensitive groups.

Set up Privileged Access Management for Active Directory if applicable.

Broken trust between computers and domain

> **NOTE**
> The Broken trust between computers and domain alert was deprecated and only appears in ATA versions prior to 1.9.

Description

Broken trust means that Active Directory security requirements may not be in effect for these computers. This is considered a baseline security and compliance failure and a soft target for attackers. In this detection, an alert is triggered if more than five Kerberos authentication failures are seen from a computer account within 24 hours.

Investigation

Is the computer being investigated allowing domain users to log on?

- If yes, you may ignore this computer in the remediation steps.

Remediation

Rejoin the machine back to the domain if necessary or reset the machine's password.

Brute force attack using LDAP simple bind

Description

> **NOTE**
> The main difference between **Suspicious authentication failures** and this detection is that in this detection, ATA can determine whether different passwords were in use.

In a brute-force attack, an attacker attempts to authenticate with many different passwords for different accounts until a correct password is found for at least one account. Once found, an attacker can log in using that account.

In this detection, an alert is triggered when ATA detects a massive number of simple bind authentications. This can be either *horizontally* with a small set of passwords across many users; or *vertically"* with a large set of passwords on just a few users; or any combination of these two options.

Investigation

1. If there are many accounts involved, click **Download details** to view the list in an Excel spreadsheet.
2. Click on the alert to go to its dedicated page. Check if any login attempts ended with a successful authentication. The attempts would appear as **Guessed accounts** on the right side of the infographic. If yes, are any of the **Guessed accounts** normally used from the source computer? If yes, **Suppress** the suspicious activity.
3. If there are no **Guessed accounts**, are any of the **Attacked accounts** normally used from the source computer? If yes, **Suppress** the suspicious activity.

Remediation

Complex and long passwords provide the necessary first level of security against brute-force attacks.

Encryption downgrade activity

Description

Encryption downgrade is a method of weakening Kerberos by downgrading the encryption level of different fields of the protocol that are normally encrypted using the highest level of encryption. A weakened encrypted field can

be an easier target to offline brute force attempts. Various attack methods utilize weak Kerberos encryption cyphers. In this detection, ATA learns the Kerberos encryption types used by computers and users, and alerts you when a weaker cypher is used that: (1) is unusual for the source computer and/or user; and (2) matches known attack techniques.

There are three detection types:

1. Skeleton Key – is malware that runs on domain controllers and allows authentication to the domain with any account without knowing its password. This malware often uses weaker encryption algorithms to hash the user's passwords on the domain controller. In this detection, the encryption method of the KRB_ERR message from the domain controller to the account asking for a ticket was downgraded compared to the previously learned behavior.

2. Golden Ticket – In a Golden Ticket alert, the encryption method of the TGT field of TGS_REQ (service request) message from the source computer was downgraded compared to the previously learned behavior. This is not based on a time anomaly (as in the other Golden Ticket detection). In addition, there was no Kerberos authentication request associated with the previous service request detected by ATA.

3. Overpass-the-Hash – An attacker can use a weak stolen hash in order to create a strong ticket, with a Kerberos AS request. In this detection, the AS_REQ message encryption type from the source computer was downgraded compared to the previously learned behavior (that is, the computer was using AES).

Investigation

First check the description of the alert to see which of the above three detection types you're dealing with. For further information, download the Excel spreadsheet.

1. Skeleton Key – You can check if Skeleton Key has affected your domain controllers by using the the scanner written by the ATA team. If the scanner finds malware on 1 or more of your domain controllers, it is a true positive.
2. Golden Ticket – In the Excel spreadsheet, go to the **Network activity** tab. You will see that the relevant downgraded field is **Request Ticket Encryption Type**, and **Source Computer Supported Encryption Types** lists stronger encryption methods. a. Check the source computer and account, or if there are multiple source computers and accounts check if they have something in common (for example, all the marketing personnel use a specific app that might be causing the alert to be triggered). There are cases in which a custom application that is rarely used is authenticating using a lower encryption cipher. Check if there are any such custom apps on the source computer. If so, it is probably a benign true positive and you can **Suppress** it. b. Check the resource accessed by those tickets, if there is one resource they are all accessing, validate it, make sure it is a valid resource they supposed to access. In addition, verify if the target resource supports strong encryption methods. You can check this in Active Directory by checking the attribute `msDS-SupportedEncryptionTypes`, of the resource service account.
3. Overpass-the-Hash – In the Excel spreadsheet, go to the **Network activity** tab. You will see that the relevant downgraded field is **Encrypted Timestamp Encryption Type** and **Source Computer Supported Encryption Types** contains stronger encryption methods. a. There are cases in which this alert might be triggered when users log in using smartcards if the smartcard configuration was changed recently. Check if there were changes like this for the account(s) involved. If so, this is probably a benign true positive and you can **Suppress** it. b. Check the resource accessed by those tickets, if there is one resource they are all accessing, validate it, make sure it is a valid resource they supposed to access. In addition, verify if the target resource supports strong encryption methods. You can check this in Active Directory by checking the attribute `msDS-SupportedEncryptionTypes`, of the resource service account.

Remediation

1. Skeleton Key – Remove the malware. For more information, see Skeleton Key Malware Analysis.

2. Golden Ticket – Follow the instructions of the Golden Ticket suspicious activities.

Also, because creating a Golden Ticket requires domain admin rights, implement Pass the hash recommendations.

3. Overpass-the-Hash – If the involved account is not sensitive, then reset the password of that account. This prevents the attacker from creating new Kerberos tickets from the password hash, although the existing tickets can still be used until they expire. If it's a sensitive account, you should consider resetting the KRBTGT account twice as in the Golden Ticket suspicious activity. Resetting the KRBTGT twice invalidates all Kerberos tickets in this domain so plan before doing so. See guidance in KRBTGT Account Password Reset Scripts now available for customers. Also see using the Reset the KRBTGT account password/keys tool. Since this is a lateral movement technique, follow the best practices of Pass the hash recommendations.

Honeytoken activity

Description

Honeytoken accounts are decoy accounts set up to identify and track malicious activity that involves these accounts. Honeytoken accounts should be left unused, while having an attractive name to lure attackers (for example, SQL-Admin). Any activity from them might indicate malicious behavior.

For more information on honey token accounts, see Install ATA - Step 7.

Investigation

1. Check whether the owner of the source computer used the Honeytoken account to authenticate, using the method described in the suspicious activity page (for example, Kerberos, LDAP, NTLM).
2. Browse to the source computer(s) profile page(s) and check which other accounts authenticated from them. Check with the owners of those accounts if they used the Honeytoken account.
3. This could be a non-interactive login, so make sure to check for applications or scripts that are running on the source computer.

If after performing steps 1 through 3, if there's no evidence of benign use, assume this is malicious.

Remediation

Make sure Honeytoken accounts are used only for their intended purpose, otherwise they might generate many alerts.

Identity theft using Pass-the-Hash attack

Description

Pass-the-Hash is a lateral movement technique in which attackers steal a user's NTLM hash from one computer and use it to gain access to another computer.

Investigation

Was the hash used from a computer owned or used regularly by the targeted user? If yes, the alert is a false positive, if not, it is probably a true positive.

Remediation

1. If the involved account is not sensitive, reset the password of that account. Resetting the password prevents the attacker from creating new Kerberos tickets from the password hash. Existing tickets are still usable until they expire.
2. If the involved account is sensitive, consider resetting the KRBTGT account twice, as in the Golden Ticket suspicious activity. Resetting the KRBTGT twice invalidates all domain Kerberos tickets, so plan around the

impact before doing so. See the guidance in KRBTGT Account Password Reset Scripts now available for customers, also refer to using the Reset the KRBTGT account password/keys tool. As this is typically a lateral movement technique, follow the best practices of Pass the hash recommendations.

Identity theft using Pass-the-Ticket attack

Description

Pass-the-Ticket is a lateral movement technique in which attackers steal a Kerberos ticket from one computer and use it to gain access to another computer by reusing the stolen ticket. In this detection, a Kerberos ticket is seen used on two (or more) different computers.

Investigation

1. Click the **Download details** button to view the full list of IP addresses involved. Is the IP address of one or both computers part of a subnet allocated from an undersized DHCP pool, for example, VPN or WiFi? Is the IP address shared? For example, by a NAT device? If the answer to any of these questions is yes, the alert is a false positive.
2. Is there a custom application that forwards tickets on behalf of users? If so, it is a benign true positive.

Remediation

1. If the involved account is not sensitive, then reset the password of that account. Password resent prevents the attacker from creating new Kerberos tickets from the password hash. Any existing tickets remain usable until expired.
2. If it's a sensitive account, you should consider resetting the KRBTGT account twice as in the Golden Ticket suspicious activity. Resetting the KRBTGT twice invalidates all Kerberos tickets in this domain so plan before doing so. See the guidance in KRBTGT Account Password Reset Scripts now available for customers, also see using the Reset the KRBTGT account password/keys tool. Since this is a lateral movement technique, follow the best practices in Pass the hash recommendations.

Kerberos Golden Ticket activity

Description

Attackers with domain admin rights can compromise your KRBTGT account. Attackers can use the KRBTGT account to create a Kerberos ticket granting ticket (TGT) providing authorization to any resource. The ticket expiration can be set to any arbitrary time. This fake TGT is called a "Golden Ticket" and allows attackers to achieve and maintain persistency in your network.

In this detection, an alert is triggered when a Kerberos ticket granting ticket (TGT) is used for more than the allowed time permitted as specified in the Maximum lifetime for user ticket security policy.

Investigation

1. Was there any recent (within the last few hours) change made to the **Maximum lifetime for user ticket** setting in group policy? If yes, then **Close** the alert (it was a false positive).
2. Is the ATA Gateway involved in this alert a virtual machine? If yes, did it recently resume from a saved state? If yes, then **Close** this alert.
3. If the answer to the above questions is no, assume this is malicious.

Remediation

Change the Kerberos Ticket Granting Ticket (KRBTGT) password twice according to the guidance in KRBTGT Account Password Reset Scripts now available for customers, using the Reset the KRBTGT account password/keys

tool. Resetting the KRBTGT twice invalidates all Kerberos tickets in this domain so plan before doing so.
Also, because creating a Golden Ticket requires domain admin rights, implement Pass the hash recommendations.

Malicious data protection private information request

Description

The Data Protection API (DPAPI) is used by Windows to securely protect passwords saved by browsers, encrypted files, and other sensitive data. Domain controllers hold a backup master key that can be used to decrypt all secrets encrypted with DPAPI on domain-joined Windows machines. Attackers can use that master key to decrypt any secrets protected by DPAPI on all domain-joined machines. In this detection, an alert is triggered when the DPAPI is used to retrieve the backup master key.

Investigation

1. Is the source computer running an organization-approved advanced security scanner against Active Directory?
2. If yes and it should always be doing so,**Close and exclude** the suspicious activity.
3. If yes and it should not do this,**Close the suspicious activity.

Remediation

To use DPAPI, an attacker needs domain admin rights. Implement Pass the hash recommendations.

Malicious replication of Directory Services

Description

Active Directory replication is the process by which changes that are made on one domain controller are synchronized with all other domain controllers. Given necessary permissions, attackers can initiate a replication request, allowing them to retrieve the data stored in Active Directory, including password hashes.

In this detection, an alert is triggered when a replication request is initiated from a computer that is not a domain controller.

Investigation

1. Is the computer in question a domain controller? For example, a newly promoted domain controller that had replication issues. If yes, **Close** the suspicious activity.
2. Is the computer in question supposed to be replicating data from Active Directory? For example, Azure AD Connect. If yes, **Close and exclude** the suspicious activity.
3. Click on the source computer or account to go to its profile page. Check what happened around the time of the replication, searching for unusual activities, such as: who was logged in, which resources where accessed.

Remediation

Validate the following permissions:

- Replicate directory changes
- Replicate directory changes all

For more information, see Grant Active Directory Domain Services permissions for profile synchronization in SharePoint Server 2013. You can leverage AD ACL Scanner or create a Windows PowerShell script to determine who in the domain has these permissions.

Massive object deletion

Description

In some scenarios, attackers perform denial of service (DoS) attacks rather than only stealing information. Deleting a large number of accounts is one method of attempting a DoS attack.

In this detection, an alert is triggered any time more than 5% of all accounts are deleted. The detection requires read access to the deleted object container.
For information about configuring read-only permissions on the deleted object container, see **Changing permissions on a deleted object container** in View or Set Permissions on a Directory Object.

Investigation

Review the list of deleted accounts and determine if there is a pattern or a business reason that justifies a large-scale deletion.

Remediation

Remove permissions for users who can delete accounts in Active Directory. For more information, see View or Set Permissions on a Directory Object.

Privilege escalation using forged authorization data

Description

Known vulnerabilities in older versions of Windows Server allow attackers to manipulate the Privileged Attribute Certificate (PAC). PAC is a field in the Kerberos ticket that has user authorization data (in Active Directory this is group membership) and grants attackers additional privileges.

Investigation

1. Click on the alert to access the details page.
2. Is the destination computer (under the **ACCESSED** column) patched with MS14-068 (domain controller) or MS11-013 (server)? If yes, **Close** the suspicious activity (it is a false positive).
3. If the destination computer is not patched, does the source computer run (under the **FROM** column) an OS/application known to modify the PAC? If yes, **Suppress** the suspicious activity (it is a benign true positive).
4. If the answer to the two previous questions was no, assume this activity is malicious.

Remediation

Make sure all domain controllers with operating systems up to Windows Server 2012 R2 are installed with KB3011780 and all member servers and domain controllers up to 2012 R2 are up-to-date with KB2496930. For more information, see Silver PAC and Forged PAC.

Reconnaissance using account enumeration

Description

In account enumeration reconnaissance, an attacker uses a dictionary with thousands of user names, or tools such as KrbGuess to attempt to guess user names in your domain. The attacker makes Kerberos requests using these names in order to try to find a valid username in your domain. If a guess successfully determines a username, the attacker will get the Kerberos error **Preauthentication required** instead of **Security principal unknown**.

In this detection, ATA can detect where the attack came from, the total number of guess attempts and how many

were matched. If there are too many unknown users, ATA will detect it as a suspicious activity.

Investigation

1. Click on the alert to get to its details page.
2. Should this host machine query the domain controller as to whether accounts exist (for example, Exchange servers)?
   Is there a script or application running on the host that could generate this behavior?
   If the answer to either of these questions is yes, **Close** the suspicious activity (it is a benign true positive) and exclude that host from the suspicious activity.
3. Download the details of the alert in an Excel spreadsheet to conveniently see the list of account attempts, divided into existing and non-existing accounts. If you look at the non-existing accounts sheet in the spreadsheet and the accounts look familiar, they may be disabled accounts or employees who left the company. In this case, it is unlikely that the attempt is coming from a dictionary. Most likely, it's an application or script that is checking to see which accounts still exist in Active Directory, meaning that it's a benign true positive.
4. If the names are largely unfamiliar, did any of the guess attempts match existing account names in Active Directory? If there are no matches, the attempt was futile, but you should pay attention to the alert to see if it gets updated over time.
5. If any of the guess attempts match existing account names, the attacker knows of the existence of accounts in your environment and can attempt to use brute force to access your domain using the discovered user names. Check the guessed account names for additional suspicious activities. Check to see if any of the matched accounts are sensitive accounts.

Remediation

Complex and long passwords provide the necessary first level of security against brute-force attacks.

Reconnaissance using Directory Services queries

Description

Directory services reconnaissance is used by attackers to map the directory structure and target privileged accounts for later steps in an attack. The Security Account Manager Remote (SAM-R) protocol is one of the methods used to query the directory to perform such mapping.

In this detection, no alerts would be triggered in the first month after ATA is deployed. During the learning period, ATA profiles which SAM-R queries are made from which computers, both enumeration and individual queries of sensitive accounts.

Investigation

1. Click on the alert to get to its details page. Check which queries were performed (for example, Enterprise admins, or Administrator) and whether or not they were successful.
2. Are such queries supposed to be made from the source computer in question?
3. If yes and the alert gets updated, **Suppress** the suspicious activity.
4. If yes and it should not do this anymore, **Close** the suspicious activity.
5. If there's information on the involved account: are such queries supposed to be made by that account or does that account normally log in to the source computer?
   - If yes and the alert gets updated, **Suppress** the suspicious activity.

- If yes and it should not do this anymore, **Close** the suspicious activity.
- If the answer was no to all of the above, assume this is malicious.

6. If there is no information about the account that was involved, you can go to the endpoint and check which account was logged in at the time of the alert.

Remediation

Use the SAMRi10 tool to harden your environment against this technique. If the tool is not applicable to your domain controller:

1. Is the computer running a vulnerability scanning tool?
2. Investigate whether the specific queried users and groups in the attack are privileged or high value accounts (that is, CEO, CFO, IT management, etc.). If so, look at other activity on the endpoint as well and monitor computers that the queried accounts are logged into, as they are probably targets for lateral movement.

Reconnaissance using DNS

Description

Your DNS server contains a map of all the computers, IP addresses, and services in your network. This information is used by attackers to map your network structure and target interesting computers for later steps in their attack.

There are several query types in the DNS protocol. ATA detects the AXFR (Transfer) request originating from non-DNS servers.

Investigation

1. Is the source machine (**Originating from...**) a DNS server? If yes, then this is probably a false positive. To validate, click on the alert to get to its details page. In the table, under **Query**, check which domains were queried. Are these existing domains? If yes, then **Close** the suspicious activity (it is a false positive). In addition, make sure UDP port 53 is open between the ATA Gateway and the source computer to prevent future false positives.
2. Is the source machine running a security scanner? If yes, **Exclude** the entities in ATA, either directly with **Close and exclude** or via the **Exclusion** page (under **Configuration** – available for ATA admins).
3. If the answer to all the preceding questions is no, keep investigating focusing on the source computer. Click on the source computer to go to its profile page. Check what happened around the time of the request, searching for unusual activities, such as: who was logged in, which resources where accessed.

Remediation

Securing an internal DNS server to prevent reconnaissance using DNS from occurring can be accomplished by disabling or restricting zone transfers only to specified IP addresses. For more information on restricting zone transfers, see Restrict Zone Transfers. Modifying zone transfers is one task among a checklist that should be addressed for securing your DNS servers from both internal and external attacks.

Reconnaissance using SMB session enumeration

Description

Server Message Block (SMB) enumeration enables attackers to get information about where users recently logged on. Once attackers have this information, they can move laterally in the network to get to a specific sensitive account.

In this detection, an alert is triggered when an SMB session enumeration is performed against a domain controller.

Investigation

1. Click on the alert to get to its details page. Check the account/s that performed the operation and which accounts were exposed, if any.
    - Is there some kind of security scanner running on the source computer? If yes, **Close and exclude** the suspicious activity.
2. Check which involved user/s performed the operation. Do they normally log into the source computer or are they administrators who should perform such actions?
3. If yes and the alert gets updated, **Suppress** the suspicious activity.
4. If yes and it should not get updated, **Close** the suspicious activity.
5. If the answer to all the above is no, assume the activity is malicious.

Remediation

Use the Net Cease tool to harden your environment against this type of attack.

Remote execution attempt detected

Description

Attackers who compromise administrative credentials or use a zero-day exploit can execute remote commands on your domain controller. This can be used for gaining persistence, collecting information, denial of service (DOS) attacks or any other reason. ATA detects PSexec and Remote WMI connections.

Investigation

1. This is common for administrative workstations as well as for IT team members and service accounts that perform administrative tasks against domain controllers. If this is this the case, and the alert gets updated because the same admin or computer is performing the task, **Suppress** the alert.
2. Is the computer in question allowed to perform this remote execution against your domain controller?
    - Is the account in question allowed to perform this remote execution against your domain controller?
    - If the answer to both questions is yes, then **Close** the alert.
3. If the answer to either questions is no, this activity should be considered a true positive. Try to find the source of the attempt by checking computer and account profiles. Click on the source computer or account to go to its profile page. Check what happened around the time of these attempts, searching for unusual activities, such as: who was logged in, which resources where accessed.

Remediation

1. Restrict remote access to domain controllers from non-Tier 0 machines.
2. Implement privileged access to allow only hardened machines to connect to domain controllers for admins.

Sensitive account credentials exposed & Services exposing account credentials

> **NOTE**
> This suspicious activity was deprecated and only appears in ATA versions prior to 1.9. For ATA 1.9 and later, see Reports.

Description

Some services send account credentials in plain text. This can even happen for sensitive accounts. Attackers monitoring network traffic can catch and then reuse these credentials for malicious purposes. Any clear text

password for a sensitive account triggers the alert, while for non-sensitive accounts the alert is triggered if five or more different accounts send clear text passwords from the same source computer.

Investigation

Click on the alert to get to its details page. See which accounts were exposed. If there are many such accounts, click **Download details** to view the list in an Excel spreadsheet.

Usually there's a script or legacy application on the source computers that uses LDAP simple bind.

Remediation

Verify the configuration on the source computers and make sure not to use LDAP simple bind. Instead of using LDAP simple binds you can use LDAP SALS or LDAPS.

Suspicious authentication failures

Description

In a brute-force attack, an attacker attempts to authenticate with many different passwords for different accounts until a correct password is found for at least one account. Once found, an attacker can log in using that account.

In this detection, an alert is triggered when many authentication failures using Kerberos or NTLM occurred, this can be either horizontally with a small set of passwords across many users; or vertically with a large set of passwords on just a few users; or any combination of these two options. The minimum period before an alert can be triggered is one week.

Investigation

1. Click **Download details** to view the full information in an Excel spreadsheet. You can get the following information:
   - List of the attacked accounts
   - List of guessed accounts in which login attempts ended with successful authentication
   - If the authentication attempts were performed using NTLM, you will see relevant event activities
   - If the authentication attempts were performed using Kerberos, you will see relevant network activities
2. Click on the source computer to go to its profile page. Check what happened around the time of these attempts, searching for unusual activities, such as: who was logged in, which resources where accessed.
3. If the authentication was performed using NTLM, and you see that the alert occurs many times, and there is not enough information available about the server that the source machine tried to access, you should enable **NTLM auditing** on the involved domain controllers. To do this, turn on event 8004. This is the NTLM authentication event that includes information about the source computer, user account, and **server** that the source machine tried to access. After you know which server sent the authentication validation, you should investigate the server by checking its events such as 4624 to better understand the authentication process.

Remediation

Complex and long passwords provide the necessary first level of security against brute-force attacks.

Suspicious service creation

Description

Attackers attempt to run suspicious services on your network. ATA raises an alert when a new service that seems suspicious has been created on a domain controller. This alert relies on event 7045, and it is detected from each domain controller that is covered by an ATA Gateway or Lightweight Gateway.

Investigation

1. If the computer in question is an administrative workstation, or a computer on which IT team members and service accounts perform administrative tasks, this may be a false positive and you may need to **Suppress** the alert and add it to the Exclusions list if necessary.
2. Is the service something you recognize on this computer?
   - Is the **account** in question allowed to install this service?
   - If the answer to both questions is *yes*, then **Close** the alert or add it to the Exclusions list.
3. If the answer to either questions is *no*, then this should be considered a true positive.

Remediation

- Implement less privileged access on domain machines to allow only specific users the right to create new services.

Suspicion of identity theft based on abnormal behavior

Description

ATA learns the entity behavior for users, computers, and resources over a sliding three-week period. The behavior model is based on the following activities: the machines the entities logged in to, the resources the entity requested access to, and the time these operations took place. ATA sends an alert when there is a deviation from the entity's behavior based on machine learning algorithms.

Investigation

1. Is the user in question supposed to be performing these operations?
2. Consider the following cases as potential false positives: a user who returned from vacation, IT personnel who perform excess access as part of their duty (for example a spike in help-desk support in a given day or week), remote desktop applications.+ If you **Close and exclude** the alert, the user will no longer be part of the detection

Remediation

Different actions should be taken depending on what caused this abnormal behavior to occur. For example, if the network was scanned, the source machine should be blocked from the network (unless it is approved).

Unusual protocol implementation

Description

Attackers use tools that implement various protocols (SMB, Kerberos, NTLM) in non-standard ways. While this type of network traffic is accepted by Windows without warnings, ATA is able to recognize potential malicious intent. The behavior is indicative of techniques such as Over-Pass-the-Hash, as well as exploits used by advanced ransomware, such as WannaCry.

Investigation

Identify the protocol that is unusual – from the suspicious activity time line, click on the suspicious activity to access the details page; the protocol appears above the arrow: Kerberos or NTLM.

- **Kerberos**: Often triggered if a hacking tool such as Mimikatz was potentially used an Overpass-the-Hash attack. Check if the source computer is running an application that implements its own Kerberos stack, that is not in accordance with the Kerberos RFC. In that case, it is a benign true positive and the alert can be **Closed**. If the alert keeps being triggered, and it is still the case, you can **Suppress** the alert.
- **NTLM**: Could be either WannaCry or tools such as Metasploit, Medusa, and Hydra.

To determine whether the activity is a WannaCry attack, perform the following steps:

1. Check if the source computer is running an attack tool such as Metasploit, Medusa, or Hydra.
2. If no attack tools are found, check if the source computer is running an application that implements its own NTLM or SMB stack.
3. If not, check if caused by WannaCry by running a WannaCry scanner script, for example this scanner against the source computer involved in the suspicious activity. If the scanner finds that the machine as infected or vulnerable, work on patching the machine and removing the malware and blocking it from the network.
4. If the script didn't find that the machine is infected or vulnerable, then it could still be infected but SMBv1 might have been disabled or the machine has been patched, which would affect the scanning tool.

Remediation

Apply the latest patches to all of your machines, and check all security updates are applied.

1. Disable SMBv1
2. Remove WannaCry
3. Data in the control of some ransom software can sometimes be decrypted. Decryption is only possible if the user hasn't restarted or turned off the computer. For more information, see Wanna Cry Ransomware

> **NOTE**
> To disable a suspicious activity alert, contact support.

Related Videos

- Joining the security community

See Also

- ATA suspicious activity playbook
- Check out the ATA forum!
- Working with suspicious activities

Working with ATA audit logs

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

The ATA audit logs are kept in the Windows Event Logs under **Applications and Services** and then **Microsoft ATA** both on the ATA Center and ATA Gateway machines.

The ATA Center audit log contains:

- Suspicious activity information
- Health alerts (health page)
- ATA Console logins
- All configuration changes*

The ATA Gateway audit log contains:

- Gateway configuration changes*

(All ATA Gateway configuration changes are configured on the ATA Center but are still audited on the Gateway machine itself.)

*The configuration change audit log contains both the previous configuration and the new configuration.

See Also

- Working with suspicious activities
- Check out the ATA forum!

Troubleshooting ATA known issues

7/20/2020 • 7 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

This section details possible errors in the deployments of ATA and the steps required for troubleshooting them.

ATA Gateway and Lightweight Gateway errors

ERROR	DESCRIPTION	RESOLUTION
System.DirectoryServices.Protocols.LdapException: A local error occurred	The ATA Gateway failed to authenticate against the domain controller.	1. Confirm that the domain controller's DNS record is configured properly in the DNS server. 2. Verify that the time of the ATA Gateway is synchronized with the time of the domain controller.
System.IdentityModel.Tokens.SecurityTokenValidationException: Failed to validate certificate chain	The ATA Gateway failed to validate the certificate of the ATA Center.	1. Verify that the Root CA certificate is installed in the trusted certificate authority certificate store on the ATA Gateway. 2. Validate that the certificate revocation list (CRL) is available and that certificate revocation validation can be performed.
Microsoft.Common.ExtendedException: Failed to parse time generated	The ATA Gateway failed to parse syslog messages that were forwarded from the SIEM.	Verify that the SIEM is configured to forward the messages in one of the formats that are supported by ATA.
System.ServiceModel.FaultException: An error occurred when verifying security for the message.	The ATA Gateway failed to authenticate against ATA Center.	Verify that the time of the ATA Gateway is synchronized with the time of the ATA Center.
System.ServiceModel.EndpointNotFoundException: Could not connect to net.tcp://center.ip.addr:443/IEntityReceiver	The ATA Gateway failed to establish a connection to the ATA Center.	Ensure that the network settings are correct and that the network connection between the ATA Gateway and the ATA Center is active.
System.DirectoryServices.Protocols.LdapException: The LDAP server is unavailable.	The ATA Gateway failed to query the domain controller using the LDAP protocol.	1. Verify that the user account used by ATA to connect to the Active Directory domain has read access to all the objects in the Active Directory tree. 2. Make sure that the domain controller is not hardened to prevent LDAP queries from the user account used by ATA.
Microsoft.Tri.Infrastructure.ContractException: Contract exception	The ATA Gateway failed to synchronize the configuration from the ATA Center.	Complete configuration of the ATA Gateway in the ATA Console.
System.Reflection.ReflectionTypeLoadException: Unable to load one or more of the requested types. Retrieve the LoaderExceptions property for more information.	Message Analyzer is installed on the ATA Gateway.	Uninstall Message Analyzer.
Error [Layout] System.OutOfMemoryException: Exception of type 'System.OutOfMemoryException' was thrown.	The ATA Gateway does not have enough memory.	Increase the amount of memory on the domain controller.
Fail to start live consumer ---> Microsoft.Opn.Runtime.Monitoring.MessageSessionException: The PEFNDIS event provider is not ready	PEF (Message Analyzer) was not installed correctly.	If using Hyper-V, try to upgrade Hyper-V Integration services otherwise, contact support for a workaround.
Installation failed with error: 0x80070652	There are other pending installations on your computer.	Wait for the other installations to complete and, if necessary, restart the computer.
System.InvalidOperationException: Instance 'Microsoft.Tri.Gateway' does not exist in the specified Category.	PIDs was enabled for process names in the ATA Gateway	Use KB281884 to disable PIDs in process names
'System.InvalidOperationException: Category does not exist.	Counters might be disabled in the registry	Use KB2554336 to rebuild Performance Counters
System.ApplicationException: Unable to start ETW session MMA-ETW-Livecapture-a4f595bd-f567-49a7-b963-20fa4e370329	There is a host entry in the HOSTS file pointing to the machine's shortname	Remove the host entry from C:\Windows\System32\drivers\etc\HOSTS file or change it to an FQDN.

ERROR	DESCRIPTION	RESOLUTION

System.IO.IOException: Authentication failed because the remote party has closed the transport stream or could not create an SSL/TLS secure channel	TLS 1.0 is disabled on the ATA Gateway, but .Net is set to use TLS 1.2	Enable TLS 1.2 for .Net by setting the registry keys to use the operating system defaults for SSL and TLS, as follows:
		`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v "SystemDefaultTlsVersions"=dword:00000001`
		`[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NE "SystemDefaultTlsVersions"=dword:00000001`
		`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v "SchUseStrongCrypto"=dword:00000001`
		`[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NE " SchUseStrongCrypto"=dword:00000001`

System.TypeLoadException: Could not load type 'Microsoft.Opn.Runtime.Values.BinaryValueBufferManager' from assembly 'Microsoft.Opn.Runtime, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35'	ATA Gateway failed to load required parsing files.	Check to see if Microsoft Message Analyzer is currently installed. Message Analyzer is not supported to be installed with the ATA Gateway / Lightweight Gateway. Uninstall Message Analyzer and restart the Gateway service.
System.Net.WebException: The remote server returned an error: (407) Proxy Authentication Required	The ATA Gateway communication with the ATA Center is being disrupted by a proxy server.	Disable the proxy on the ATA Gateway machine. Note that proxy settings may be per-account.
System.IO.DirectoryNotFoundException: The system cannot find the path specified. (Exception from HRESULT: 0x80070003)	One or more of the services needed to operate ATA did not start.	Start the following services: Performance Logs and Alerts (PLA), Task Scheduler (Schedule).
System.Net.WebException: The remote server returned an error: (403) Forbidden	The ATA Gateway or Lightweight Gateway was forbidden from establishing an HTTP connection because the ATA Center is not trusted.	Add the NetBIOS name and FQDN of the ATA Center to the trusted websites list and clear the cache on Internet Explorer (or the name of the ATA Center as specified in the configuration if the configured is different than the NetBIOS/FQDN).
System.Net.Http.HttpRequestException: PostAsync failed [requestTypeName=StopNetEventSessionRequest]	The ATA Gateway or ATA Lightweight Gateway can't stop and start the ETW session that collects network traffic due to a WMI issue	Follow the instructions in WMI: Rebuilding the WMI Repository to fix the WMI issue
System.Net.Sockets.SocketException: An attempt was made to access a socket in a way forbidden by its access permissions	Another application is using port 514 on the ATA Gateway	Use `netstat -o` to establish which process is using that port.

Deployment errors

ERROR	DESCRIPTION	RESOLUTION
.Net Framework 4.6.1 installation fails with error 0x800713ec	The pre-requisites for .Net Framework 4.6.1 are not installed on the server.	Before installing ATA, verify that the windows updates KB2919442 and KB2919355 are installed on the server.
System.Threading.Tasks.TaskCanceledException: A task was canceled	The deployment process timed out as it could not reach the ATA Center.	1. Check network connectivity to the ATA Center by browsing to it using its IP address. 2. Check for proxy or firewall configuration.
System.Net.Http.HttpRequestException: An error occurred while sending the request. ---> System.Net.WebException: The remote server returned an error: (407) Proxy Authentication Required.	The deployment process timed out as it could not reach the ATA Center due to a proxy misconfiguration.	Disable the proxy configuration before deployment, then enable the proxy configuration again. Alternatively, you can configure an exception in the proxy.

System.Net.Sockets.SocketException: An existing connection was forcibly closed by the remote host		Enable TLS 1.2 for .Net by setting the registry keys to use the operating system defaults for SSL and TLS, as follows:
		`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v "SystemDefaultTlsVersions"=dword:00000001`
		`[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NE "SystemDefaultTlsVersions"=dword:00000001`
		`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v "SchUseStrongCrypto"=dword:00000001`
		`[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NE " SchUseStrongCrypto"=dword:00000001`

ERROR	DESCRIPTION	RESOLUTION
Error [\[]DeploymentModel[\]] Failed management authentication [\ []CurrentlyLoggedOnUser=\Status=FailedAuthentication Exception=[\]]	The deployment process of the ATA Gateway or ATA Lightweight Gateway could not successfully authenticate against the ATA Center	Open a browser from the machine on which the deployment process failed and see if you can reach the ATA Console. If not, start troubleshooting to see why the browser can't authenticate against the ATA Center. Things to check: Proxy configuration Networking issues Group policy settings for authentication on that machine that differs from the ATA Center.
Error [\[]DeploymentModel[\]] Failed management authentication	Center certificate validation failed	The Center certificate may require an internet connection for validation. Make sure your Gateway service has the proper proxy configuration to enable the connection and validation.

ATA Center errors

ERROR	DESCRIPTION	RESOLUTION
System.Security.Cryptography.CryptographicException: Access denied.	The ATA Center failed to use the issued certificate for decryption. This most likely happened due to use of a certificate with KeySpec (KeyNumber) set to Signature (AT_SIGNATURE) which is not supported for decryption, instead of using KeyExchange (AT_KEYEXCHANGE).	1. Stop the ATA Center service. 2. Delete the ATA Center certificate from the center's certificate store. (Before deleting, make sure you have the certificate backed up with the private key in a PFX file.) 3. Open an elevated command prompt and run certutil -importpfx "CenterCertificate.pfx" AT_KEYEXCHANGE 4. Start the ATA Center service. 5. Verify everything now works as expected.

ATA Gateway and Lightweight Gateway issues

ISSUE	DESCRIPTION	RESOLUTION
No traffic received from the domain controller, but health alerts are observed	No traffic was received from a domain controller using port mirroring through an ATA Gateway	On the ATA Gateway capture NIC, disable these features in **Advanced Settings**: Receive Segment Coalescing (IPv4) Receive Segment Coalescing (IPv6)
This health alert is displayed: Some network traffic is not being analyzed	If you have an ATA Gateway or Lightweight Gateway on VMware virtual machines, you might receive this health alert. This happens because of a configuration mismatch in VMware.	Set the following settings to 0 or Disabled in the virtual machine NIC configuration: TsoEnable, LargeSendOffload, TSO Offload, Giant TSO Offload

Multi Processor Group mode

For Windows operating systems 2008R2 and 2012, ATA Gateway is not supported in **Multi Processor Group** mode.

Suggested possible workarounds:

- If hyperthreading is on, turn it off. This may reduce the number of logical cores enough to avoid needing to run in **Multi Processor Group** mode.
- If your machine has less than 64 logical cores and is running on a HP host, you may be able to change the **NUMA Group Size Optimization** BIOS setting from the default of **Clustered** to **Flat**.

See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

Troubleshooting ATA using the ATA logs

7/20/2020 • 4 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

The ATA logs provide insight into what each component of ATA is doing at any given point in time.

ATA Gateway logs

In this section, every reference to the ATA Gateway is relevant also for the ATA Lightweight Gateway.

The ATA Gateway logs are located in a subfolder called **Logs** where ATA is installed; the default location is: **C:\Program Files\Microsoft Advanced Threat Analytics**. In the default installation location, it can be found at: **C:\Program Files\Microsoft Advanced Threat Analytics\Gateway\Logs**.

The ATA Gateway has the following logs:

- **Microsoft.Tri.Gateway.log** – This log contains everything that happens in the ATA Gateway (including resolution and errors). Its main use is getting the overall status of all operations in the chronological order in which they occurred.
- **Microsoft.Tri.Gateway-Resolution.log** – This log contains the resolution details of the entities seen in traffic by the ATA Gateway. Its main use is investigating resolution issues of entities.
- **Microsoft.Tri.Gateway-Errors.log** – This log contains just the errors that are caught by the ATA Gateway. Its main use is performing health checks and investigating issues that need to be correlated to specific times.
- **Microsoft.Tri.Gateway-ExceptionStatistics.log** – This log groups all similar errors and exceptions, and measures their count. This file starts out empty each time the ATA Gateway service starts and is updated every minute. Its main use is understanding if there are any new errors or issues with the ATA Gateway (because the errors are grouped it is easier to read and quickly understand if there are any new issues).
- **Microsoft.Tri.Gateway.Updater.log** - This log is used for the gateway updater process, which is responsible for updating the ATA Gateway if configured to do so automatically. For the ATA Lightweight Gateway, the gateway updater process is also responsible for the resource limitations of the ATA Lightweight Gateway.
- **Microsoft.Tri.Gateway.Updater-ExceptionStatistics.log** - This log groups all similar errors and exceptions together, and measures their count. This file starts out empty each time the ATA Updater service starts and is updated every minute. It enables you to understand if there are any new errors or issues with the ATA Updater. The errors are grouped to make it easier to quickly understand if any new errors or issues are detected.

> **NOTE**
> The first three log files have a maximum size of up to 50 MB. When that size is reached, a new log file is opened and the previous one is renamed to "<original file name>-Archived-00000" where the number increments each time it is renamed. By default, if more than 10 files from the same type already exist, the oldest are deleted.

ATA Center logs

The ATA Center logs are located in a subfolder called **Logs**. In the default installation location, it can be found at: **C:\Program Files\Microsoft Advanced Threat Analytics\Center\Logs**".

> **NOTE**
> The ATA console logs that were formerly under IIS logs are now located under ATA Center logs.

The ATA Center has the following logs:

- **Microsoft.Tri.Center.log** – This log contains everything that happens in the ATA Center, including detections and errors. Its main use is getting the overall status of all operations in the chronological order in which they occurred.
- **Microsoft.Tri.Center-Detection.log** – This log contains just the detection details of the ATA Center. Its main use is investigating detection issues.
- **Microsoft.Tri.Center-Errors.log** – This log contains just the errors that are caught by the ATA Center. Its main use is performing health checks and investigating issues that need to be correlated to specific times.
- **Microsoft.Tri.Center-ExceptionStatistics.log** – This log groups all similar errors and exceptions, and measures their count. This file starts out empty each time the ATA Center service starts and is updated every minute. Its main use is understanding if there are any new errors or issues with the ATA Center - because the errors are grouped it is easier to quickly understand if there is a new error or issue.

> **NOTE**
> The first three log files have a maximum size of up to 50 MB. When that size is reached, a new log file is opened and the previous one is renamed to "<original file name>-Archived-00000" where the number increments each time it is renamed. By default, if more than 10 files from the same type already exist, the oldest are deleted.

ATA Deployment logs

The ATA deployment logs are located in the temp directory for the user who installed the product. In the default installation location, it can be found at: **C:\Users<logged-in-user>\AppData\Local\Temp** (or one directory above %temp%).

ATA Center deployment logs:

- **Microsoft Advanced Threat Analytics Center_YYYYMMDDHHMMSS.log** - This log lists the steps in the process of the deployment of the ATA Center. Its main use is tracking the ATA Center deployment process.
- **Microsoft Advanced Threat Analytics Center_YYYYMMDDHHMMSS_0_MongoDBPackage.log** - This log lists the steps in the process of MongoDB deployment on the ATA Center. Its main use is tracking the MongoDB deployment process.
- **Microsoft Advanced Threat Analytics Center_YYYYMMDDHHMMSS_1_MsiPackage.log** - This log file lists the steps in the process of the deployment of the ATA Center binaries. Its main use is tracking the deployment of the ATA Center binaries.

ATA Gateway and ATA Lightweight Gateway deployment logs:

- **Microsoft Advanced Threat Analytics Gateway_YYYYMMDDHHMMSS.log** - This log lists the steps in the process of the deployment of the ATA Gateway. Its main use is tracking the ATA Gateway deployment process.

- **Microsoft Advanced Threat Analytics Gateway_YYYYMMDDHHMMSS_001_MsiPackage.log** - This log file lists the steps in the process of the deployment of the ATA Gateway binaries. Its main use is tracking the deployment of the ATA Gateway binaries.

> **NOTE**
> In addition to the deployment logs mentioned here, there are other logs that begin with "Microsoft Advanced Threat Analytics" that can also provide additional information on the deployment process.

See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

Troubleshooting ATA using the performance counters

7/20/2020 • 11 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

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 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.

Retrieving performance monitor files for troubleshooting

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

1. Open perfmon.
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**.

ATA Gateway performance counters

In this section, every reference to ATA Gateway refers also to the ATA Lightweight Gateway.

You can observe the real-time performance status of the ATA Gateway by adding the ATA Gateway's performance counters. This is done by opening **Performance Monitor** and adding all counters for the ATA Gateway. The name of the performance counter object is: **Microsoft ATA Gateway**.

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

COUNTER	DESCRIPTION	THRESHOLD	TROUBLESHOOTING
Microsoft ATA Gateway\NetworkListener PEF Parsed Messages\Sec	The amount of traffic being processed by the ATA Gateway every second.	No threshold	Helps you understand the amount of traffic that is being parsed by the ATA Gateway.

COUNTER	DESCRIPTION	THRESHOLD	TROUBLESHOOTING
NetworkListener PEF Dropped Events\Sec	The amount of traffic being dropped by the ATA Gateway every second.	This number should be zero all of the time (rare short burst of drops are acceptable).	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 Gateway\NetworkListener ETW Dropped Events\Sec	The amount of traffic being dropped by the ATA Gateway every second.	This number should be zero all of the time (rare short burst of drops are acceptable).	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 Gateway\NetworkActivityTranslator Message Data # Block Size	The amount of traffic queued for translation to Network Activities (NAs).	Should be less than the maximum-1 (default maximum: 100,000)	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 Gateway\EntityResolver Activity Block Size	The number of Network Activities (NAs) queued for resolution.	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 Gateway\EntitySender Entity Batch Block Size	The amount of Network Activities (NAs) queued to be sent to the ATA Center.	Should be less than the maximum-1 (default maximum: 1,000,000)	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.

COUNTER	DESCRIPTION	THRESHOLD	TROUBLESHOOTING
Microsoft ATA Gateway\EntitySender Batch Send Time	The amount of time it took to send the last batch.	Should be less than 1000 milliseconds most of the time	Check if there are any networking issues between the ATA Gateway and the ATA Center.

NOTE

- Timed counters are in milliseconds.
- It is sometimes more convenient to monitor the full list of the counters by using the **Report** graph type (example: real-time monitoring of all the counters)

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 names 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.

COUNTER	DESCRIPTION	THRESHOLD	TROUBLESHOOTING
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.

COUNTER	DESCRIPTION	THRESHOLD	TROUBLESHOOTING
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.

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 preceding **ATA Component Process**. 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 preceding **ATA Component Process**. Check that there is no issue with the CPU or memory.

COUNTER	DESCRIPTION	THRESHOLD	TROUBLESHOOTING
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: 100,000)	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 preceding **ATA Component Process**. Check that there is no issue with the CPU or memory.
Microsoft ATA Center\Database * Block Size	The number of Network Activities, 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 preceding **ATA Component Process**. Check that there is no issue with the CPU or memory.

NOTE

- Timed counters are in milliseconds
- It is sometimes more convenient to monitor the full list of the counters using the graph type for Report (example: real-time monitoring of all the counters).

Operating system counters

The following table lists the main operating system counters to pay attention to:

COUNTER	DESCRIPTION	THRESHOLD	TROUBLESHOOTING
Processor(_Total)% Processor Time	The percentage of elapsed time that the processor spends to execute a non-Idle thread.	Less than 80% on average	Check if there is a specific process that is taking a lot more processor time than it should. Add more processors. Reduce the amount of traffic per server. The "Processor(_Total)% Processor Time" counter may be less accurate on virtual servers, in which case the more accurate way to measure the lack of processor power is through the "System\Processor Queue Length" counter.

COUNTER	DESCRIPTION	THRESHOLD	TROUBLESHOOTING
System\Context Switches\sec	The combined rate at which all processors are switched from one thread to another.	Less than 5000*cores (physical cores)	Check if there is a specific process that is taking a lot more processor time than it should. Add more processors. Reduce the amount of traffic per server. The "Processor(_Total)% Processor Time" counter may be less accurate on virtual servers, in which case the more accurate way to measure the lack of processor power is through the "System\Processor Queue Length" counter.
System\Processor Queue Length	The number of threads that are ready to execute and are waiting to be scheduled.	Less than five*cores (physical cores)	Check if there is a specific process that is taking a lot more processor time than it should. Add more processors. Reduce the amount of traffic per server. The "Processor(_Total)% Processor Time" counter may be less accurate on virtual servers, in which case the more accurate way to measure the lack of processor power is through the "System\Processor Queue Length" counter.
Memory\Available MBytes	The amount of physical memory (RAM) available for allocation.	Should be more than 512	Check if there is a specific process that is taking a lot more physical memory than it should. Increase the amount of physical memory. Reduce the amount of traffic per server.

COUNTER	DESCRIPTION	THRESHOLD	TROUBLESHOOTING
LogicalDisk(*)\Avg. Disk sec\Read	The average latency for reading data from the disk (you should choose the database drive as the instance).	Should be less than 10 milliseconds	Check if there is a specific process that is utilizing the database drive more than it should. Consult with your storage team/vendor if this drive can deliver the current workload while having less than 10 ms of latency. The current workload can be determined by using the disk utilization counters.
LogicalDisk(*)\Avg. Disk sec\Write	The average latency for writing data to the disk (you should choose the database drive as the instance).	Should be less than 10 milliseconds	Check if there is a specific process that is utilizing the database drive more than it should. Consult with your storage team\vendor if this drive can deliver the current workload while having less than 10 ms of latency. The current workload can be determined by using the disk utilization counters.
\LogicalDisk(*)\Disk Reads\sec	The rate of performing read operations to the disk.	No threshold	Disk utilization counters can add insight when troubleshooting storage latency.
\LogicalDisk(*)\Disk Read Bytes\sec	The number of bytes per second that are being read from the disk.	No threshold	Disk utilization counters can add insight when troubleshooting storage latency.
\LogicalDisk*\Disk Writes\sec	The rate of performing write operations to the disk.	No threshold	Disk utilization counters (can add insights when troubleshooting the storage latency)
\LogicalDisk(*)\Disk Write Bytes\sec	The number of bytes per second that are being written to the disk.	No threshold	Disk utilization counters can add insight when troubleshooting storage latency.

See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

Troubleshooting ATA using the ATA database

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

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.

Interacting with the database

The default and most basic way to query the database is using the Mongo shell:

1. Open a command-line window 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: `mongo.exe ATA`. Make sure to type ATA with all capital letters.

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({CompleteSearchNames: "<name of entity in lower case>"})`	
Find Kerberos authentication traffic originating from a specific computer on a specific day.	`db.KerberosAs_<datetime>.find({SourceComputer: "<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.
Make advanced configuration changes. In this example, change the send queue size for all ATA Gateways to 10,000.	`db.SystemProfile.update( {_t: "GatewaySystemProfile"} , {$set: {"Configuration.EntitySenderConfiguration.EntityBatchBlockMaxSize" : "10000"}})`	`

The following example provides sample code using the syntax provided earlier. If you are investigating a suspicious activity that occurred on 20/10/2015 and want to learn more about the NTLM activities that "John Doe" performed on that day:

First, find the ID of "John Doe"

```
db.UniqueEntity.find({Name: "John Doe"})
```

Take a note of the ID as indicated by the value of `_id` For example, assume the ID is `123bdd24-b269-h6e1-9c72-7737as875351`

Then, search for the collection with the closest date that is before the date you are looking for, in the example 20/10/2015.

Then, search for John Doe's account NTLM activities:

```
db.Ntlms_<closest date>.find({SourceAccountId: "123bdd24-b269-h6e1-9c72-7737as875351"})
```

See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

Troubleshooting service startup

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

Troubleshooting ATA Center service startup

If your ATA Center does not start, perform the following troubleshooting procedure:

1. Run the following Windows PowerShell command: `Get-Service Pla | Select Status` to make sure the Performance counter service is running. If it's not, then it's a platform issue, and you need to make sure you get this service running again.
2. If it was running, Try to restart it, and see if it resolves the issue: `Restart-Service Pla`
3. Try to create a new data collector manually (any will suffice, even just collect machine CPU for example). If it can start, the platform is probably fine. If not, it is still a platform issue.
4. Try to manually recreate the ATA data collector, using an elevated prompt, running these commands:

```
sc stop ATACenter
logman stop "Microsoft ATA Center"
logman export "Microsoft ATA Center" -xml c:\center.xml
logman delete "Microsoft ATA Center"
logman import "Microsoft ATA Center" -xml c:\center.xml
logman start "Microsoft ATA Center"
sc start ATACenter
```

Troubleshooting ATA Lightweight Gateway startup

Symptom

Your ATA Gateway does not start and you get this error:
System.Net.Http.HttpRequestException: Response status code does not indicate success: 500 (Internal Server Error)

Description

This happens because as part of the Lightweight Gateway installation process, ATA allocates a CPU threshold that enables the Lightweight Gateway to utilize CPU with a buffer of 15%. If you have independently set a threshold using the registry key: this conflict will prevent the Lightweight Gateway from starting.

Resolution

1. Under the registry keys, if there is a DWORD value called **Disable Performance Counters** make sure it is set to **0**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PerfOS\Performance\` `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PerfProc\Performance`
2. Then restart the Pla service. The ATA Lightweight Gateway will automatically detect the change and restart the service.

See Also

- ATA prerequisites
- ATA capacity planning

- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

ATA disaster recovery

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

This article describes how to quickly recover your ATA Center and restore ATA functionality when the ATA Center functionality is lost 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.

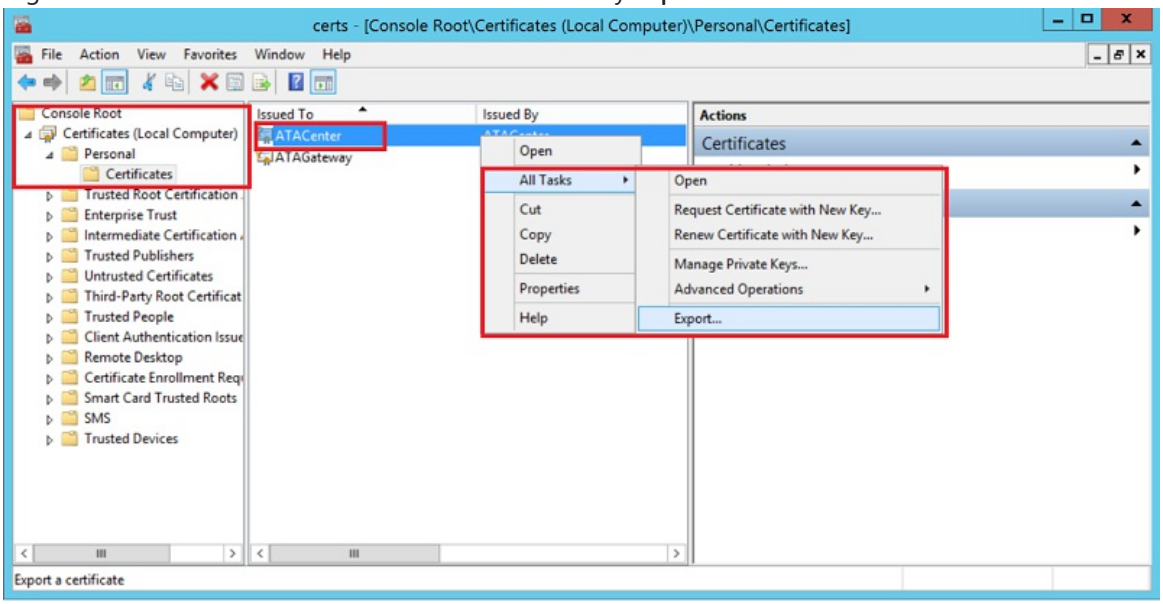
Back up your ATA Center configuration

1. The ATA Center configuration is backed up to a file every 4 hours. 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.

2. Export the ATA Center certificate.

   a. In the certificate manager, navigate to **Certificates (Local Computer)** -> **Personal** ->**Certificates**, and select **ATA Center**.

   b. Right-click **ATA Center** and select **All Tasks** followed by **Export**.



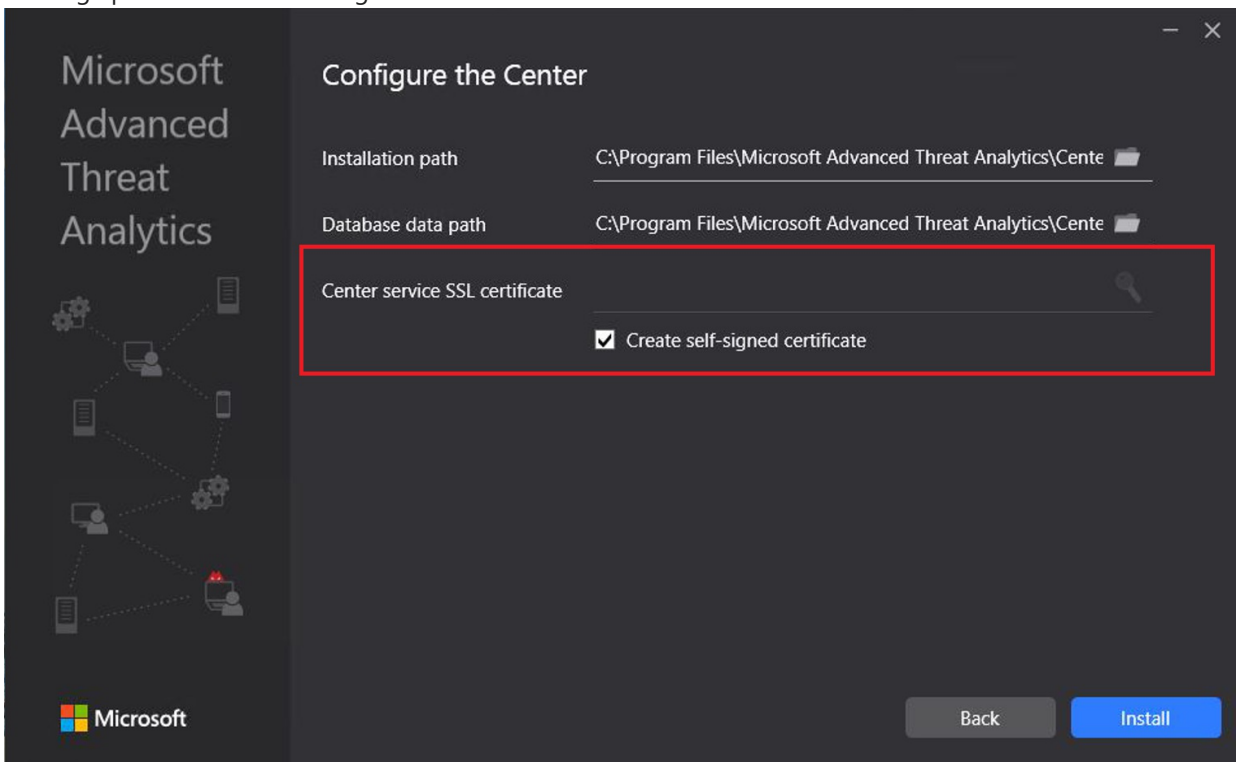
   c. Follow the instructions to export the certificate, making sure to export the private key as well.

   d. 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, and then export it.

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 earlier, to the new server.
3. Follow the instructions to Deploy the ATA Center 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.



4. Stop the ATA Center service.
5. Import the backed-up ATA Center configuration:
   a. Remove the default ATA Center System Profile document from the MongoDB:
      a. Go to **C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin**.
      b. Run `mongo.exe ATA`
      c. Run this command to remove the default system profile: `db.SystemProfile.remove({})`
      d. Leave the Mongo shell and return to the command prompt by entering: `exit`
   b. Run the command:
      ```
      mongoimport.exe --db ATA --collection SystemProfile --file "<SystemProfile.json backup file>" --upsert
      ```
      using the backup file from step 1.
      For a full explanation of how to locate and import backup files, see Export and import the ATA configuration.
   c. Start the ATA Center service.
   d. Open the ATA Console. You should see all the ATA Gateways linked under the Configuration/Gateways tab.
   e. Make sure to define a **Directory services user** and to choose a **Domain controller synchronizer**.

See Also

- ATA prerequisites
- ATA capacity planning
- Configure event collection
- Configuring Windows event forwarding
- Check out the ATA forum!

ATA readiness roadmap

7/20/2020 • 2 minutes to read • Edit Online

Applies to: Advanced Threat Analytics version 1.9

This article provides you a readiness roadmap that will assist you to get started with Advanced Threat Analytics.

Understanding ATA

Advanced Threat Analytics (ATA) is an on-premises platform that helps protect your enterprise from multiple types of advanced targeted cyberattacks and insider threats. Use the following resources to learn more about ATA:

- ATA overview
- ATA introduction video - short
- ATA introductory video - full

Deployment decisions

ATA is composed of the ATA Center, which you can install on a server, and ATA Gateways, which you can install on separate computers or by using the Lightweight Gateway directly on your domain controllers. Before you get up and running, it's important to make the following deployment decisions:

CONFIGURATION	DECISION
Hardware type	Physical, virtual, Azure VM
Workgroup or Domain	Workgroup, domain
Gateway sizing	Full Gateway, Lightweight Gateway
Certificates	PKI, self-signed

If you are using physical servers, you should plan capacity. You can get help from the sizing tool to allocate space for ATA:

ATA sizing tool - The sizing tool automates the collection of the amount of traffic ATA needs. It automatically provides supportability and resource recommendations for both the ATA Center and ATA Lightweight Gateways.

ATA capacity planning

Deploy ATA

These resources will help you download and install the ATA Center, connect to Active Directory, download the ATA Gateway package, set up event collection, and optionally integrate with your VPN and set up honeytoken accounts and exclusions.

Download ATA - Before deploying ATA, if you haven't made the decision to purchase ATA, you can download the evaluation version.

ATA POC playbook - Guide to all the steps necessary to do a successful POC deployment of ATA.

ATA deployment video - This video provides an overview of ATA deployment steps in less than 10 minutes.

ATA settings

The basic necessary settings in ATA are configured as part of the installation wizard. However, there are a number of other settings that you can configure to fine-tune ATA that makes detections more accurate for your environment, such as SIEM integration and audit settings.

Audit settings – Audit your domain controller health before and after an ATA deployment.

ATA general documentation

Work with ATA

After ATA is up and running, you can view suspicious activities that are detected in the Attack timeline. This is the default landing page you are taken to when you log in to the ATA Console. By default, all open suspicious activities are shown on the attack time line. You can also see the severity assigned to each activity. Investigate each suspicious activity by drilling down into the entities (computers, devices, users) to open their profile pages that provide more information. These resources will help you work with ATA's suspicious activities:

ATA suspicious activity playbook - This article walks you through credential theft attack techniques using readily available research tools on the internet. At each point of the attack, you can see how ATA helps you gain visibility into these threats.

ATA suspicious activity guide

Security best practices

ATA best practices - Best practices for securing ATA.

ATA frequently asked questions - This article provides a list of frequently asked questions about ATA and provides insight and answers.

Additional resources

Microsoft Security Channel 9 page

Community resources

ATA blog ATA community