



Fvigo

12-20-2018 11:26 A

This article has been updated to reflect changes to the Azure AD Application registration process and to point users to a new MineMeld output node. The old node will be deprecated.

If you are not familiar with MineMeld, we recommend you start with a [Quick Tour](#).

MineMeld can be used to aggregate multiple threat intelligence feeds and extend to your Windows Defender ATP tenant. Windows Defender ATP can ingest:

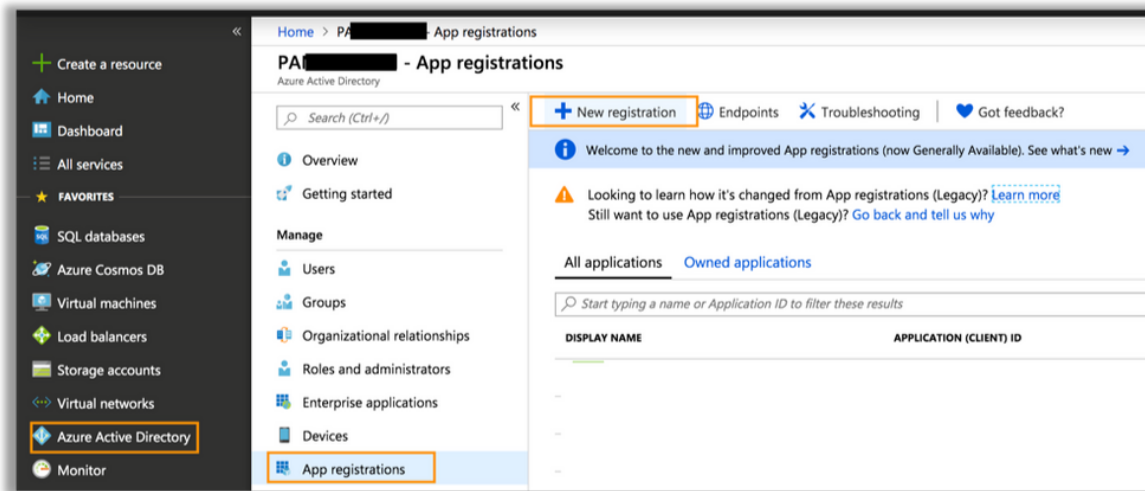
- IPv4 addresses
- File hashes
- URLs
- Domains and FQDNs

There are three steps to connecting MineMeld to Windows Defender ATP:

1. Create an application in Azure Active Directory. You will assign scopes from your Windows Defender ATP to this application, and all of the alerts tied to the threat intelligence provided will be tied to this application name. The MineMeld Miner will be associated with this application.
2. Install the Windows Defender extension in MineMeld.
3. Configure the extension to connect to the Windows Defender ATP tenant.

Azure Active Directory Configuration

1. Log in to the Azure Portal (portal.azure.com).
2. Go to Azure Active Directory.
3. Navigate to **Enterprise Applications > App Registrations > click New Application Registration**.



4. Create a name for this application. All of the alerts tied to the threat intelligence coming from MineMeld will be attributed to this application name. We recommend calling this "Palo Alto Networks MineMeld" to avoid any confusion.

NOTE: *You do not need to set a redirect URI.*

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (Palo Alto Networks)

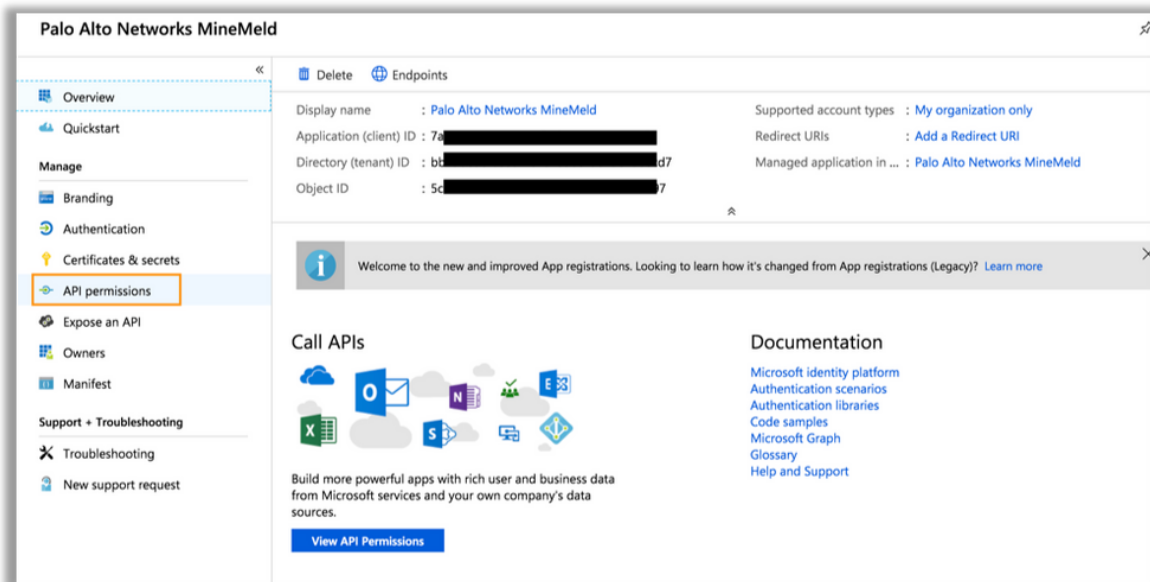
Accounts in any organizational directory

Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

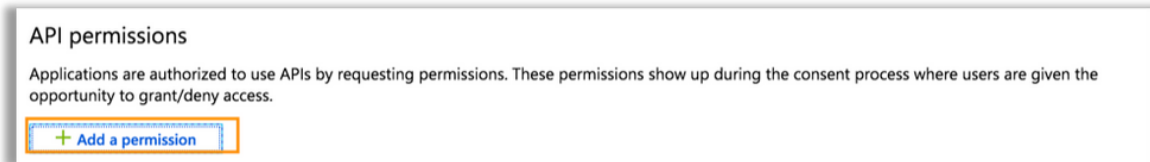
[Help me choose...](#)

5. Click **Register**.

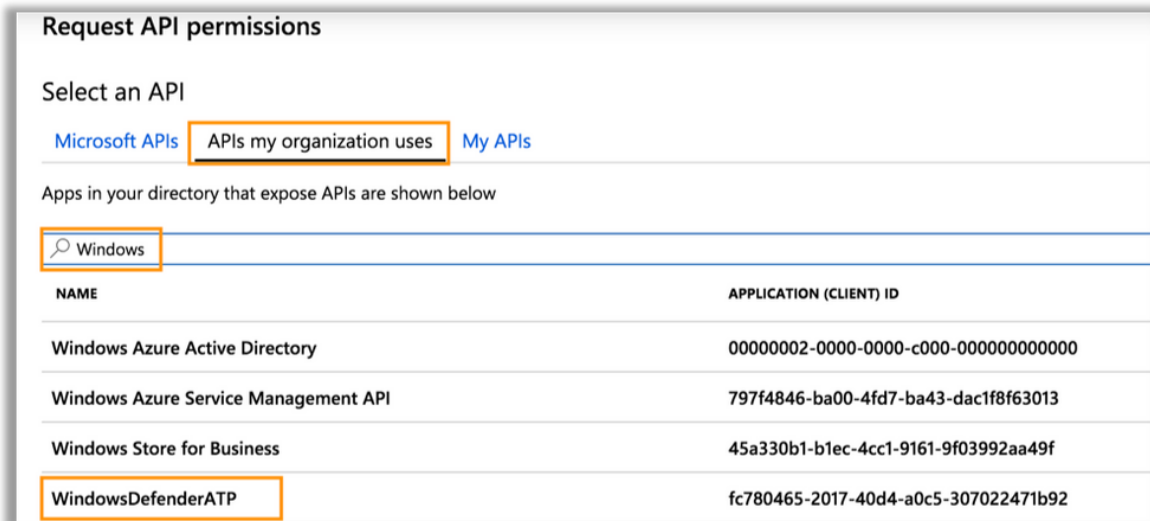
6. From the Application page, click **API Permissions**.



7. Click Add a Permission.



8. Click APIs my organization uses, type “Windows” in the search bar, and select WindowsDefendertATP.



9. Click Application Permissions, select “Ti.ReadWrite” and then click Add Permissions.

Request API permissions

[← All APIs](#)

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

PERMISSION	ADMIN CONSENT REQUIRED
▶ AdvancedQuery	
▶ Alert	
▶ Event	
▶ File	
▶ Ip	
▶ Machine	
▼ Ti (1)	
<input type="checkbox"/> Ti.ReadWrite Read and write IOCs belonging to the app ⓘ	Yes
<input checked="" type="checkbox"/> Ti.ReadWrite.All Read and write all IOCs ⓘ	Yes

Add permissions
Discard

10. Grant admin consent.

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

[Grant admin consent for PA \[REDACTED\]](#)

11. From the Application page, click **Certificates and Secrets**.

Home > Palo Alto Networks MineMeld

Palo Alto Networks MineMeld

Overview | Quickstart | Manage | Branding | Authentication | **Certificates & secrets** | API permissions | Expose an API | Owners | Manifest | Support + Troubleshooting | Troubleshooting | New support request

Display name : Palo Alto Networks MineMeld | Supported account types : My organization only
 Application (client) ID : 7ad[redacted] | Redirect URIs : Add a Redirect URI
 Directory (tenant) ID : bb1[redacted]d7 | Managed application in ... : Palo Alto Networks MineMeld
 Object ID : 5c0[redacted]37

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Call APIs
 Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.
[View API Permissions](#)

Documentation
[Microsoft identity platform](#)
[Authentication scenarios](#)
[Authentication libraries](#)
[Code samples](#)
[Microsoft Graph](#)
[Glossary](#)
[Help and Support](#)

12. Click New Client Secret.

Palo Alto Networks MineMeld - Certificates & secrets

Overview | Quickstart | Manage | Branding | Authentication | **Certificates & secrets** | API permissions | Expose an API | Owners | Manifest | Support + Troubleshooting | Troubleshooting | New support request

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates
 Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.
[Upload certificate](#)

THUMBPRINT	START DATE	EXPIRES
No certificates have been added for this application.		

Client secrets
 A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
[New client secret](#)

DESCRIPTION	EXPIRES	VALUE
No client secrets have been created for this application.		

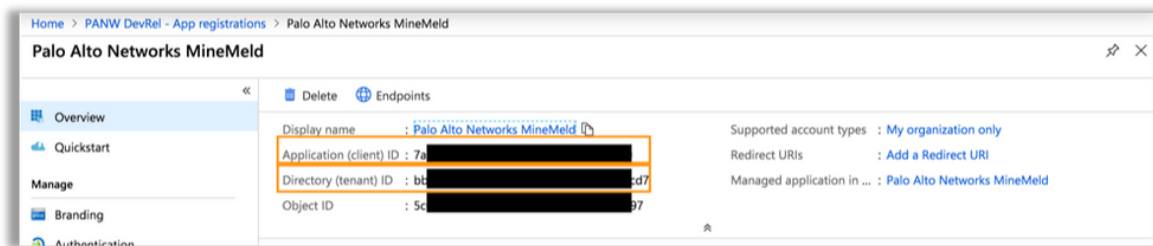
13. Copy the client secret you created.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
[New client secret](#)

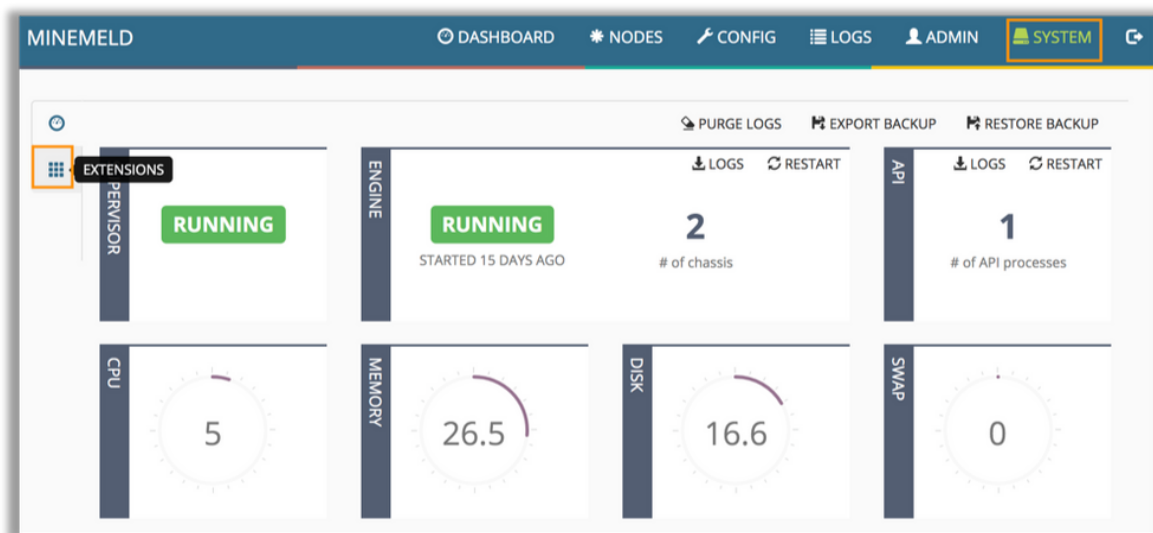
DESCRIPTION	EXPIRES	VALUE
Access Key	5/7/2020	yl[redacted]1=8

14. You will also need to copy the Application ID and Directory ID.

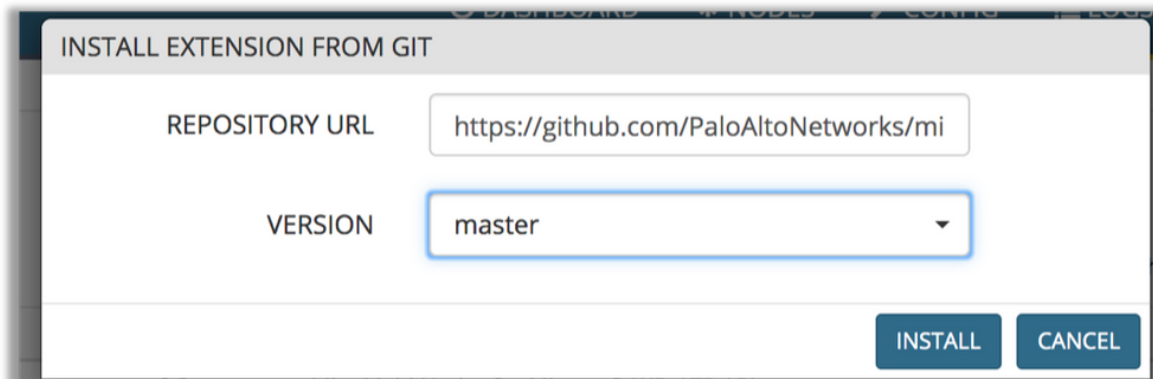


MineMeld Configuration

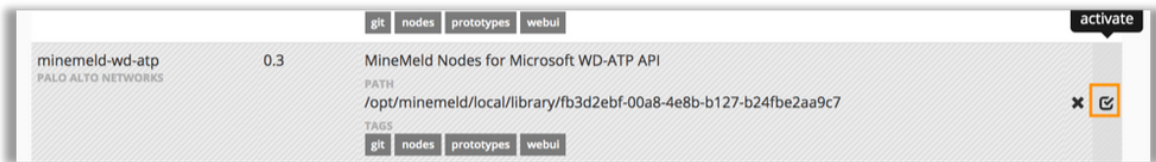
1. In MineMeld, go under **SYSTEM** and click the **Extensions** icon.



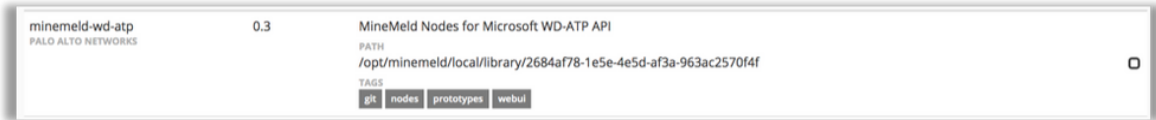
2. Click the GitHub icon in the lower, right-hand corner, then copy this link "<https://github.com/PaloAltoNetworks/minemeld-wd-atp.git>" and paste into the **Repository URL** field. Click the dropdown menu for **Version** and select "master" then click **Install**.



3. Click the checkmark to activate the extension.

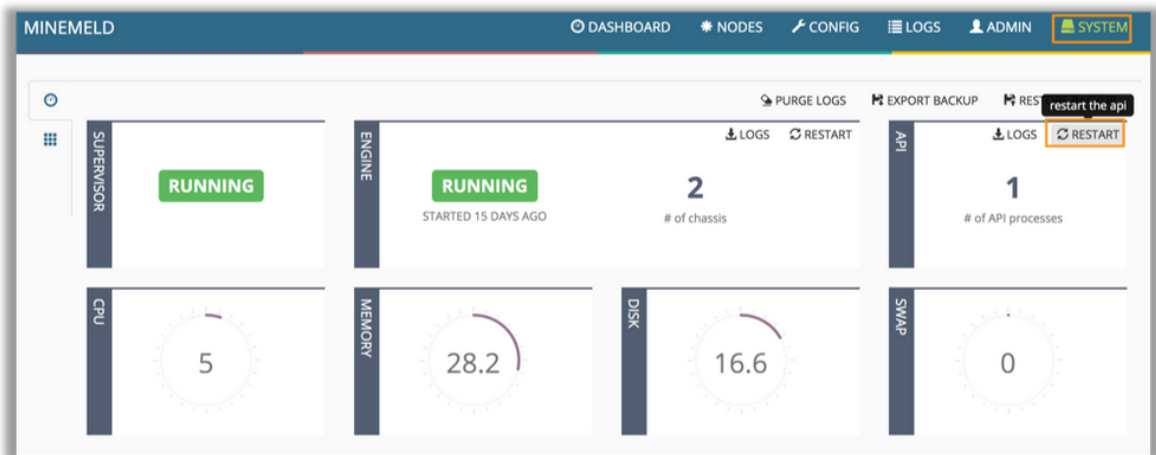


The extension will activate shortly, and the empty square will signify the extension is active.



4. You will need to go back to the **SYSTEM** page and restart the API.

NOTE: *After the restart completes, make sure you refresh the browser page.*



Setting Up the Output Node to Complete the Integration

1. In MineMeld, click **CONFIG**, then click the Browse Prototype icon.

NAME	TYPE	PROTOTYPE	INPUTS
dshield_blocklist	MINER	dshield.block	None
fromASI	MINER	stdlib.localDB	None
localDB-Sentinel	MINER	stdlib.localDB	None
ransomware_c2	MINER	ransomwaretracker.RW_IPBL	None
ransomware_c2_domains	MINER	ransomwaretracker.RW_DOMBL	None
spamhaus_DROP	MINER	spamhaus.DROP	None
spamhaus_EDROP	MINER	spamhaus.EDROP	None
wiWhiteListIPv4	MINER	stdlib.listIPv4Generic	None
dag_IP_ASI	OUTPUT	stdlib.dagPusher	fromASI
edl_IP_ASI	OUTPUT	stdlib.feedHCGreen	fromASI
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundagggregator
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundagggregator
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundagggregator
MicrosoftGraphSecurityAPI	OUTPUT	microsoft_graph_secapi.output	inboundagggregator
test_graphui	OUTPUT	microsoft_graph_secapi.output	ransomware_c2 ransomware_c2_domains
inboundagggregator	PROCESSOR	stdlib.agggregatorIPv4Inbound	spamhaus_DROP spamhaus_EDROP dshield_blocklist wiWhiteListIPv4

2. Type “windows” into the search bar to shorten the list, and select the “microsoft_wd_atp.outputBatch” node.

NOTE: The “microsoft_wd_atp.output” node will be deprecated as it relies on an older API interface. Please do not use that node.

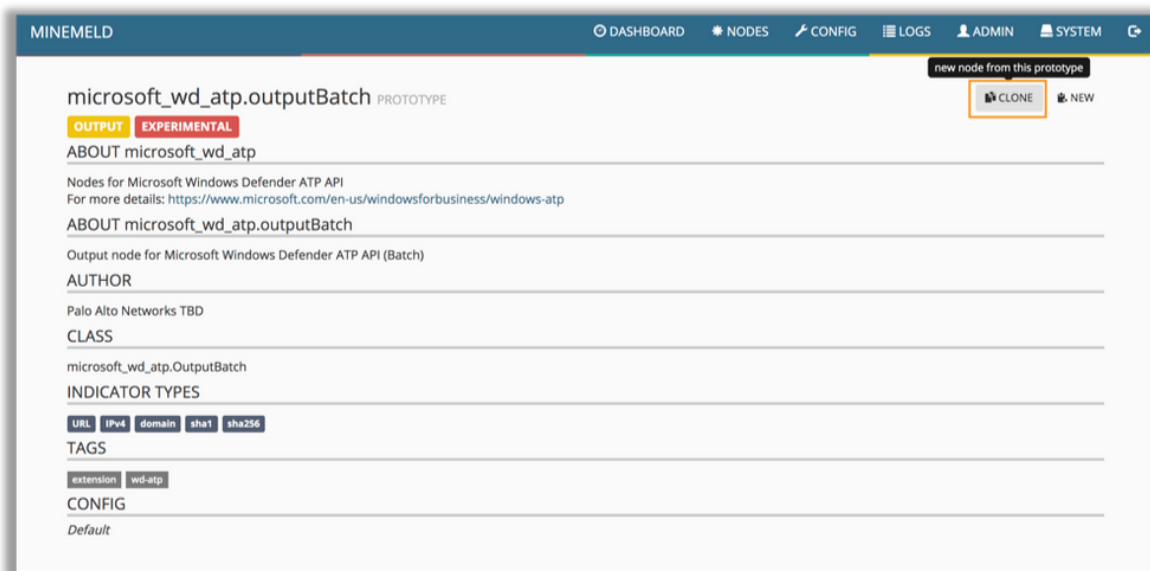
PROTOTYPES

Show 50 entries

Search: wind

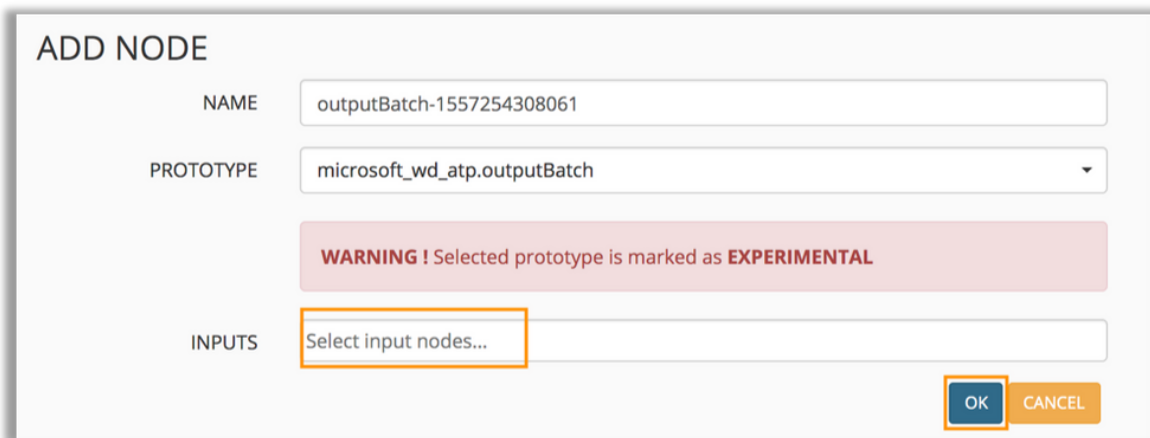
NAME	TYPE	INDICATORS	DESCRIPTION
microsoft_wd_atp.output <small>PALO ALTO NETWORKS TRD</small>	OUTPUT	URL IPv4 domain	EXPERIMENTAL microsoft_wd_atp Nodes for Microsoft Windows Defender ATP API microsoft_wd_atp.output Output node for Microsoft Windows Defender ATP API TAGS: extension wd-atp
microsoft_wd_atp.outputBatch <small>PALO ALTO NETWORKS TRD</small>	OUTPUT	URL IPv4 domain sha1 sha256	EXPERIMENTAL microsoft_wd_atp Nodes for Microsoft Windows Defender ATP API microsoft_wd_atp.outputBatch Output node for Microsoft Windows Defender ATP API (Batch) TAGS: extension wd-atp
stdlib.agggregatorWindowsRegistryValue <small>MINE MELD CORE TEAM</small>	PROCESSOR	windows-registry-value	stdlib Library of prototypes for commonly used nodes stdlib.agggregatorWindowsRegistryValue Aggregator for windows-registry-value indicators. Inputs with names starting with "wl" will be interpreted as whitelists.

3. Click **Clone** on the top, right of the page.



4. Name the cloned node and add the appropriate threat feeds that you want to send to your Windows Defender ATP tenant in the **INPUTS** nodes section and then click OK.

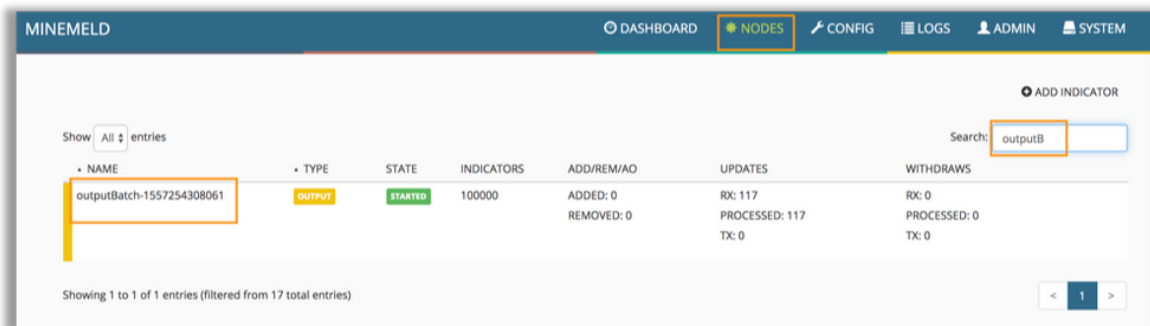
NOTE: To understand the concepts of input nodes and what to connect to this, refer to the MineMeld [documentation](#) on LIVEcommunity.



5. Click the **COMMIT** button in the top left of the **CONFIG** page.

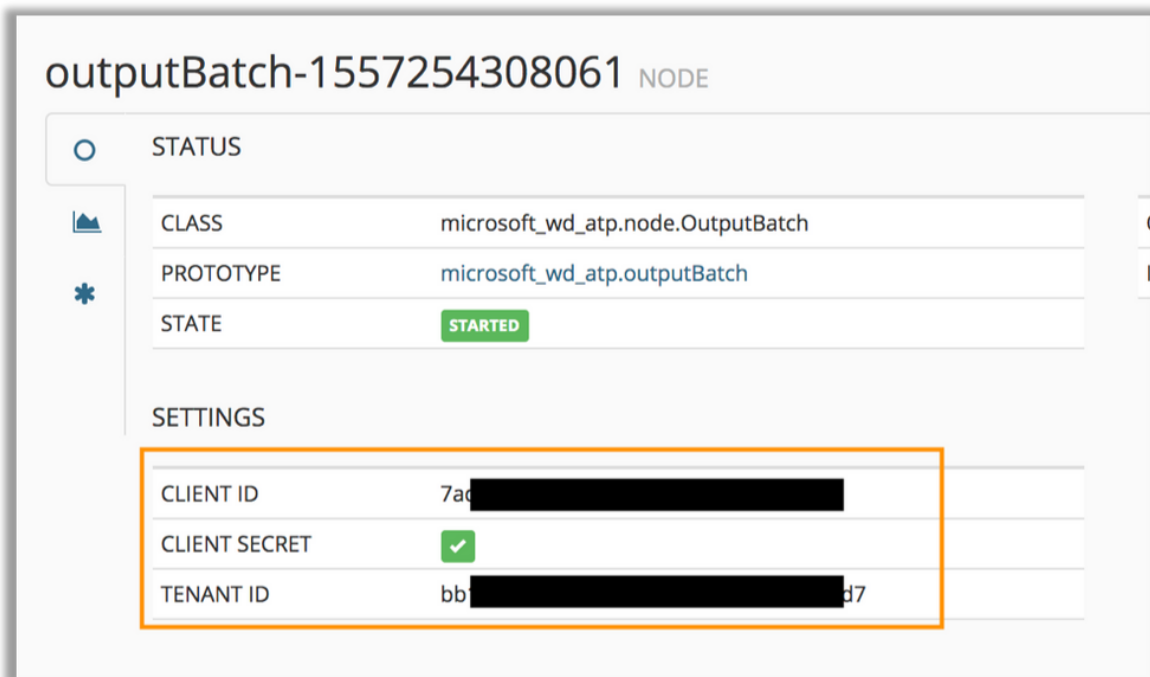


6. Click **NODES** on the top menu and search for the node you just created. Click the node to pull up the configuration.



7. In Azure AD, enter the Client ID (Application), Client Secret, and Tenant (Directory) ID you copied earlier when you created the MineMeld application.

NOTE: After this is done, your configuration will then be complete.



outputBatch-1557254308061 NODE

STATUS

CLASS microsoft_wd_atp.node.OutputBatch

PROTOTYPE microsoft_wd_atp.outputBatch

STATE **STARTED**

SETTINGS

CLIENT ID	7ad [REDACTED]
CLIENT SECRET	<input checked="" type="checkbox"/>
TENANT ID	bb [REDACTED] d7

Testing

To validate this is hooked up correctly, you will need to verify that an event fires if you try to access a blocked website. We recommend you create an indicator that is tied to a known good website for this, so you are not actively going to a malicious website.

1. Click **NODES** at the top and then click **ADD INDICATOR**



MINEMELD

DASHBOARD **NODES** CONFIG LOGS ADMIN SYSTEM

Show All entries

ADD INDICATOR

Search:

NAME	TYPE	STATE	INDICATORS	ADD/REM/AD	UPDATES	WITHDRAWS
------	------	-------	------------	------------	---------	-----------

2. Enter in a known IP address as an **INDICATOR** and add it to the Input node (**TYPE**) you used to configure your microsoft_wd_atp.outputBatch node. Then click OK.

ADD INDICATOR

INDICATOR	<input type="text" value="Indicator (required)"/>
TYPE	<input type="text" value="IPv4"/>
SHARE LEVEL	<input type="button" value="GREEN"/>
COMMENT	<input type="text" value="Comment (optional)"/>
MINERS	<input type="text" value="Miners to add the indicator to..."/>

3. Wait for the indicator to be pushed to your Windows Defender ATP tenant. Then try to load that URL on a client that is running Windows Defender ATP. You should see an event fire in the Windows Defender ATP console.

Alerts > A suspicious domain was detected based on Palo Alto...

 A suspicious domain was detected based on Palo Alto Networks MineMeld

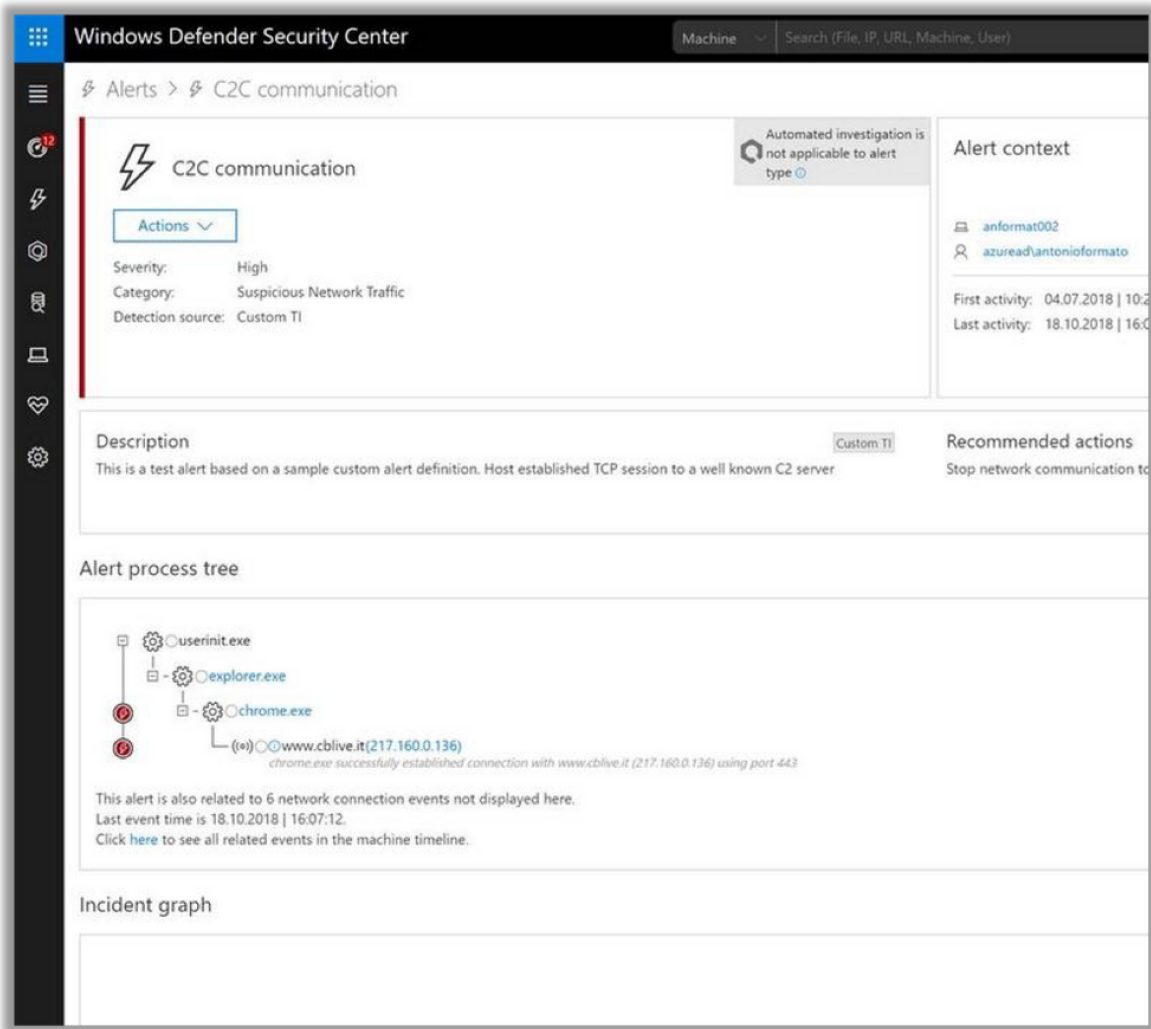
Automated investigation is not applicable to alert type

Actions

Severity: Low
Category: General
Detection source: Custom TI

Description
A malicious domain associated with cyberespionage activity was detected based on Palo Alto Networks MineMeld threat intelligence.

Custom TI



Additional Information

You can find out more information about this capability by reading [Pushing custom Indicator of Compromise \(IoCs\) to Microsoft Defender ATP](#) on the Microsoft website.



5,160 Views