NetWitness® Platform

Microsoft Office 365 Event Source Log Configuration Guide

NETWITNESS
Platform

Microsoft Office 365

Last Modified: Tuesday, June 18, 2024

Event Source Product Information:

Vendor: Microsoft

Event Source: Office 365

Versions: API v1.0

RSA Product Information:

Supported On: NetWitness Platform 12.2 and later

Event Source Log Parser: cef, msoffice365 (v12.2 & beyond)

Note: The CEF and msoffice365 parsers parse this event source as **device.type=msoffice365**.

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

Note: For 12.2.x and beyond, NetWitness can now parse JSON event data directly on the Log Decoder and there is no need to transform logs into CEF. Previously, plugins had to be tailored to each JSON schema individually. Now, all of the raw JSON event data can be sent straight to the Log Decoder. In v12.2, the plugin can collect logs in JSON event data and will pass them through to Log decoder directly in RFC 5424 format by adding a header, and it will be parsed by the JSON parser instead of the CEF parser (based on Raw JSON Event Parameter setting).

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

February, 2024

Contents

Collecting Office 365 Events in NetWitness Platform

Office 365 is a Web-based version of Microsoft's Office suite of enterprise-grade productivity applications. Office 365 is delivered to users through the cloud and includes Exchange Online for email, SharePoint Online for collaboration, Lync Online for unified communications, and a suite of Office Web Apps (web-based versions of the traditional Microsoft Office suite of applications).

The Office 365 integration consumes activity logs using the Office 365 Management Activity API. The Office 365 Management Activity API aggregates actions and events into tenant-specific content blobs, which are classified by the type and source of the content they contain. Currently, these content types are supported:

- Audit.AzureActiveDirectory
- Audit.Exchange
- Audit.SharePoint
- Audit.General (includes all other workloads not included in the previous content types)
- DLP.All (DLP events only for all workloads)

Note: Advanced Threat Protection and Threat Intelligence events are available under the Audit.General resource group.

For more details, see the following Microsoft Office 365 web pages:

- Getting Started: https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-reference
- Schema: https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema

The following sections describe how to configure Office 365 as an event source:

- Configure the Office 365 Event Source
- Set Up the Office 365 Event Source in NetWitness Platform
- Office 365 Collection Configuration Parameters

Configure the Office 365 Event Source

Perform the following tasks to configure your event source:

I. Begin Recording User and Admin Activity

II. Enable Mailbox Auditing

III. Use the Azure Management Portal to Register an Application

IV. Deploy the Office 365 Files from NetWitness Platform Live

V. Enable Subscription

For more information on Office 365, see the following Microsoft URLs:

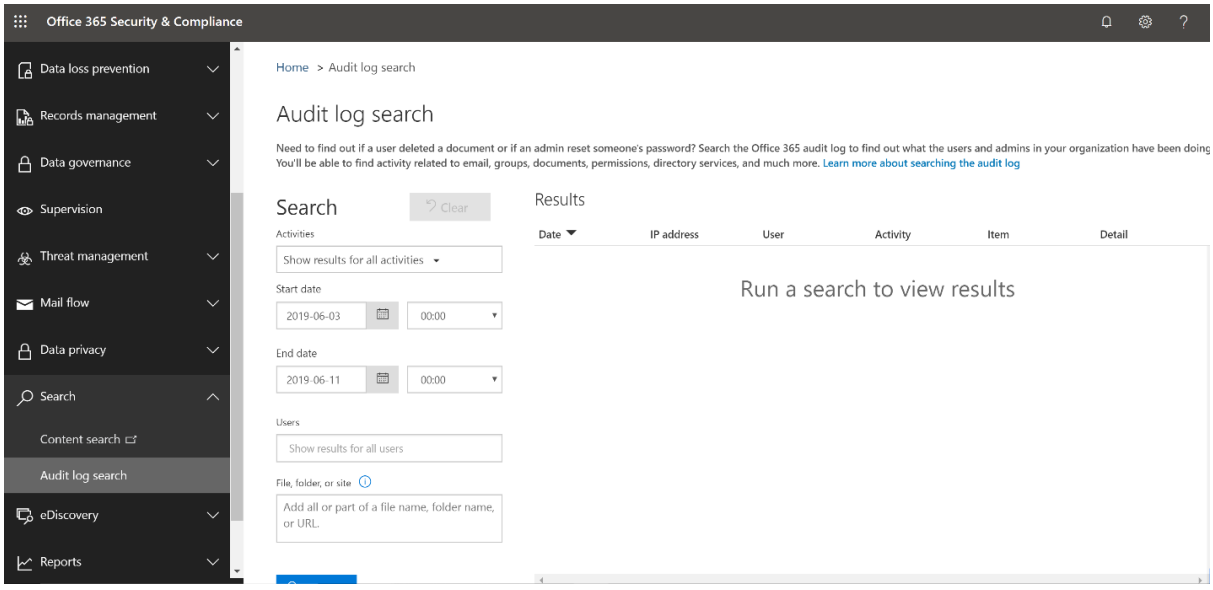
- Office 365 Management API getting started: https://msdn.microsoft.com/en-us/office-365/get-started-with-office-365-management-apis
- Enable mailbox auditing in Office 365: https://technet.microsoft.com/en-us/library/dn879651.aspx

Begin Recording User and Admin Activity

This section describes how to begin recording user and admin activity.

1. Go to admin portal for Office365: https://portal.office.com/adminportal/home#/homepage.
2. Go to **Admin centers > Security and Compliance > Audit Log Search** and enable logging. If logging has already been enabled, you may not see the option to enable logs.

Note: It make take up to 24 hours for some logs to appear once logging has been enabled.



Enable Mailbox Auditing

Audit logging is turned on by default for Microsoft 365 organizations. For more information : https://learn.microsoft.com/en-us/purview/audit-log-enable-disable?tabs=microsoft-purview-portal#turn-on-auditing

Note: This step is only required if you wish to consume Audit.Exchange logs.

To enable mailbox auditing:

1. Run the following command in Exchange Online PowerShell

   ```
   Set-OrganizationConfig -AuditDisabled $false
   ```

   For more information on enabling mailbox auditing, go to Microsoft Knowledge Base:

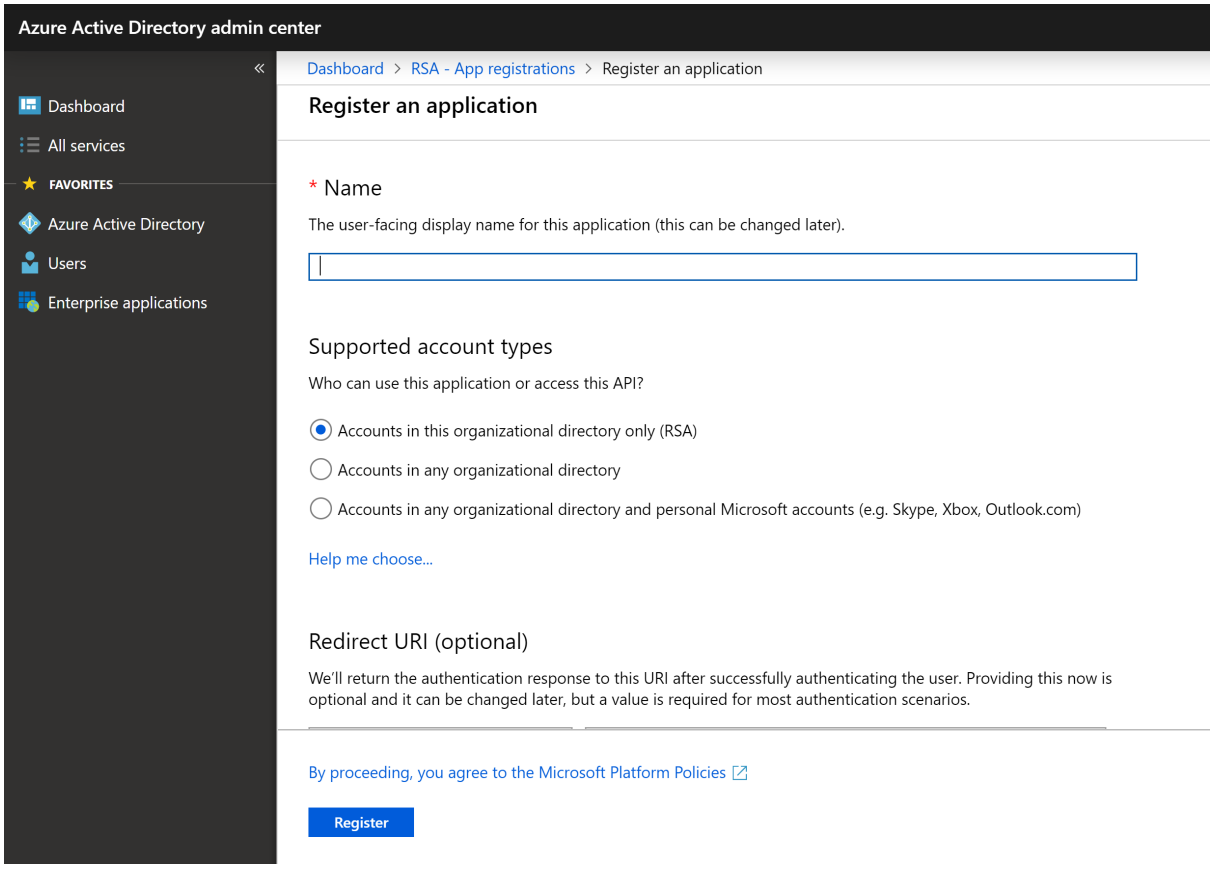
   https://learn.microsoft.com/en-us/purview/audit-mailboxes

Use the Azure Management Portal to Register an Application

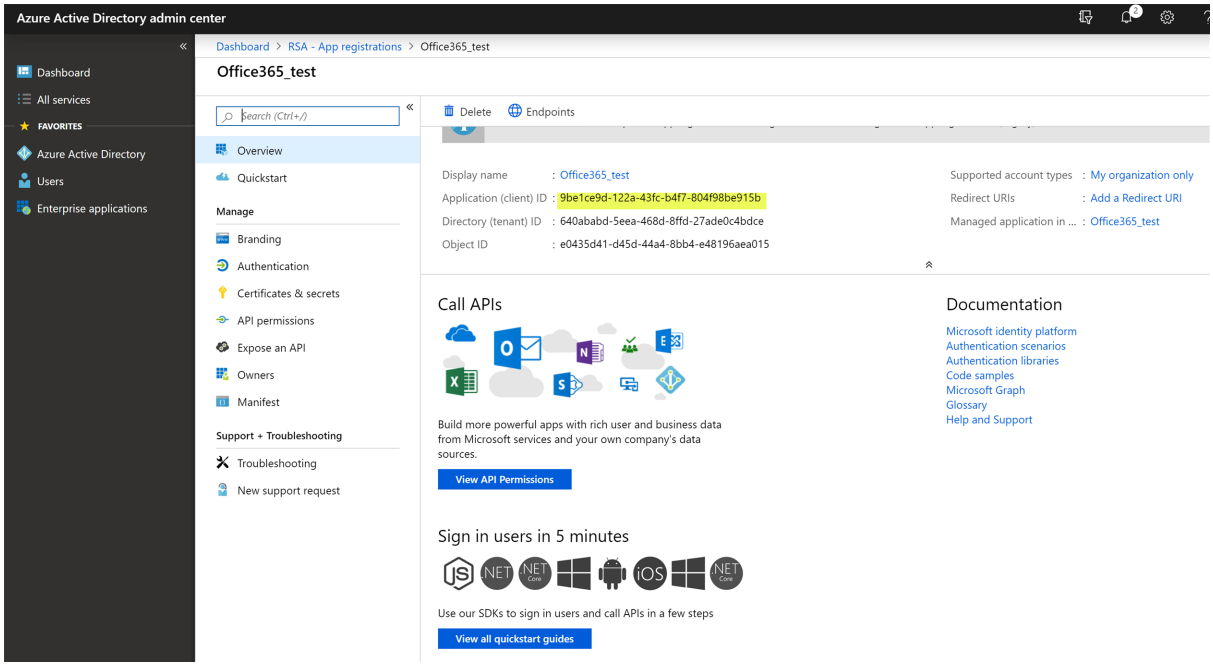
This section describes how to use the Azure Management Portal to register your application in Azure AD and authenticate.

To register your application:

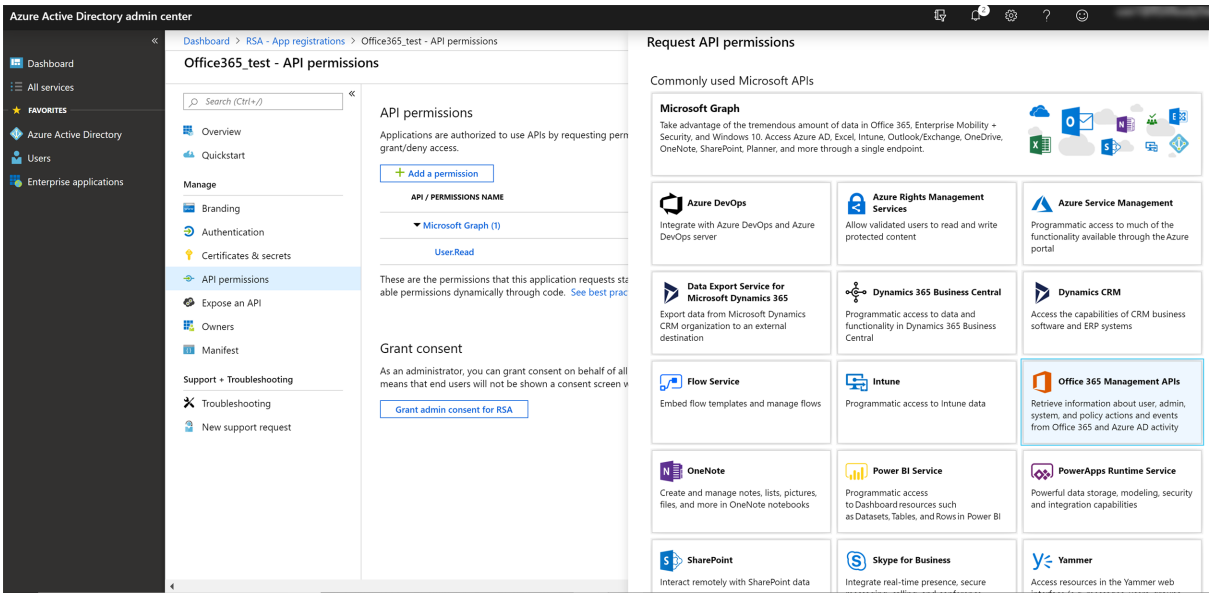
1. Go to **Office365 portal > Admin centers > Azure AD Admin center**.
2. In the left-hand navigation pane, select the **Azure Active Directory** service, and then select **App registrations > New registration**.
3. Provide a name for your application and click **Register** at the bottom of the blade.



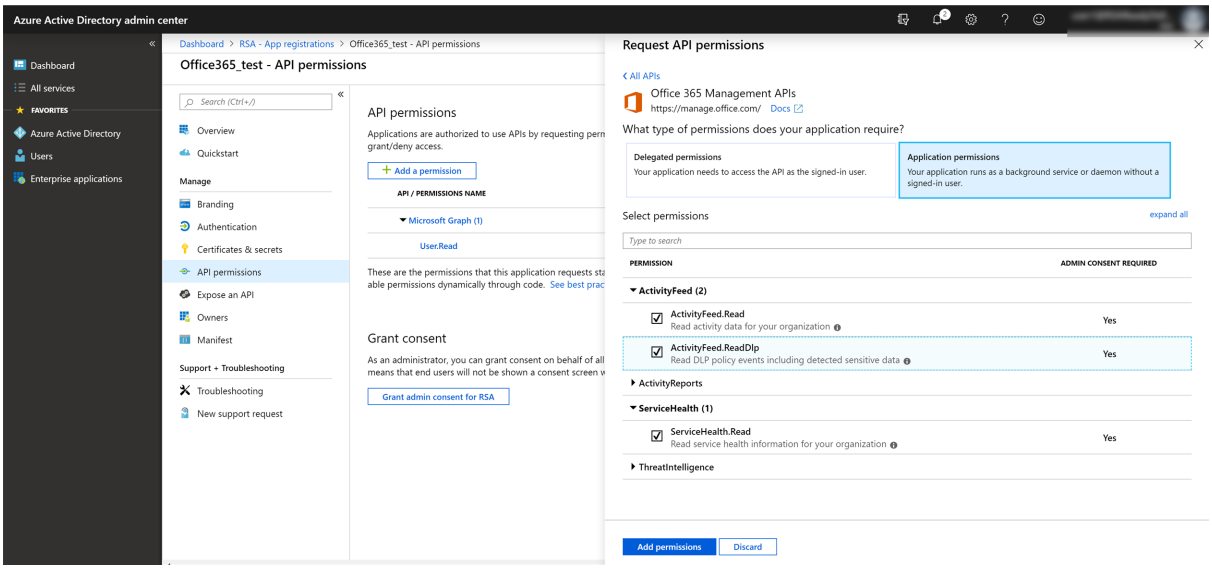
4. After clicking **Register**, the Overview page for the application is displayed. Azure AD assigns a unique application (client) ID to your app.



5. In the left menu bar, click **API permissions**, then **Add a permission > Select an API** and choose **Office 365 Management APIs**.

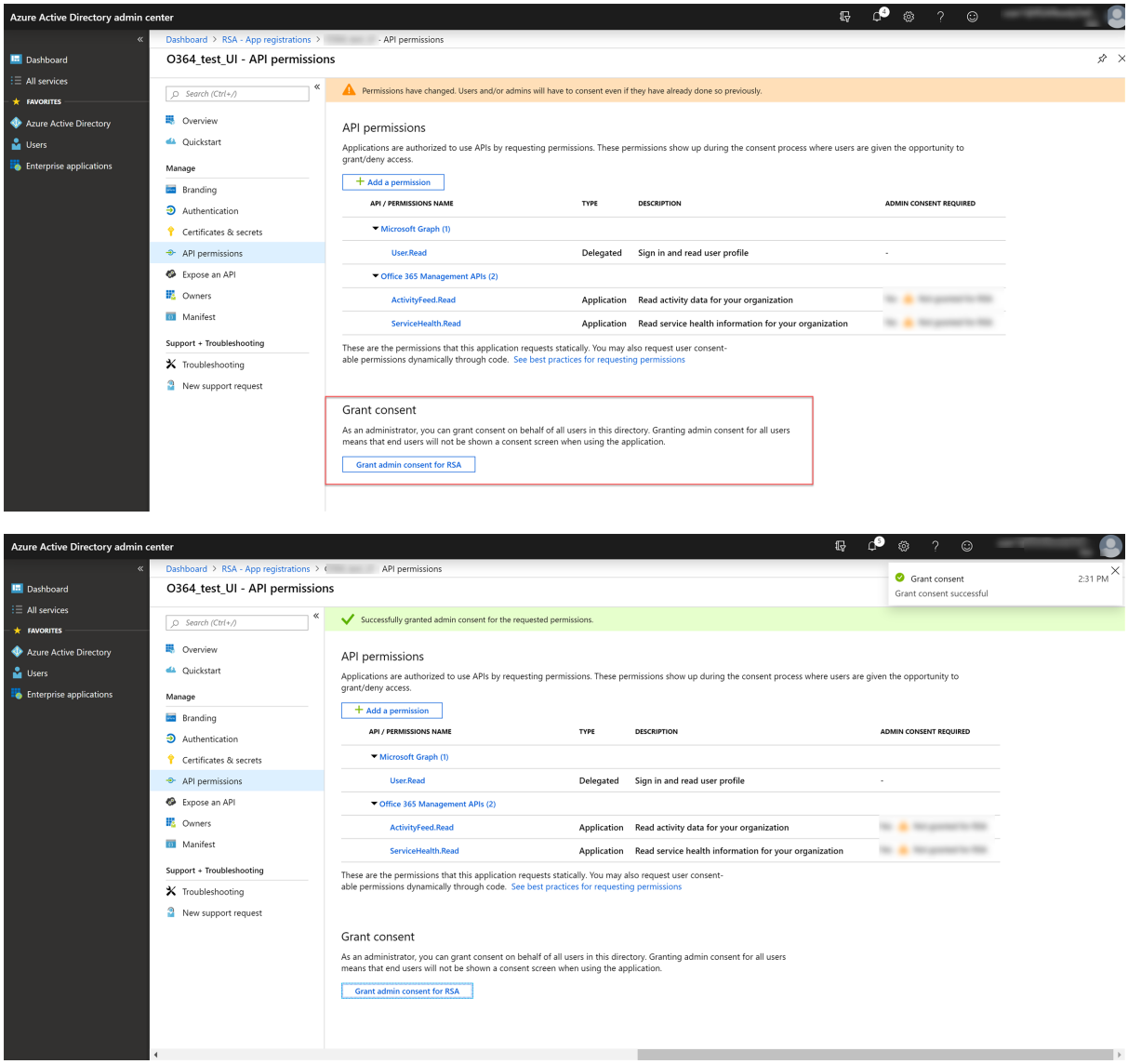


6. Under **What type of permissions does your application require** option, choose **Application permissions** and enable the permissions as shown here:



Note: Assign the **Read DLP policy events including detected sensitive data** permission only if logs are being read from the **DLP.All** resource group.

7. Click **Add permissions**.
8. Click **Grant admin consent**, then click **Yes** when prompted.



Continue to the next procedure to create a key and add a certificate.

Office365 Authentication

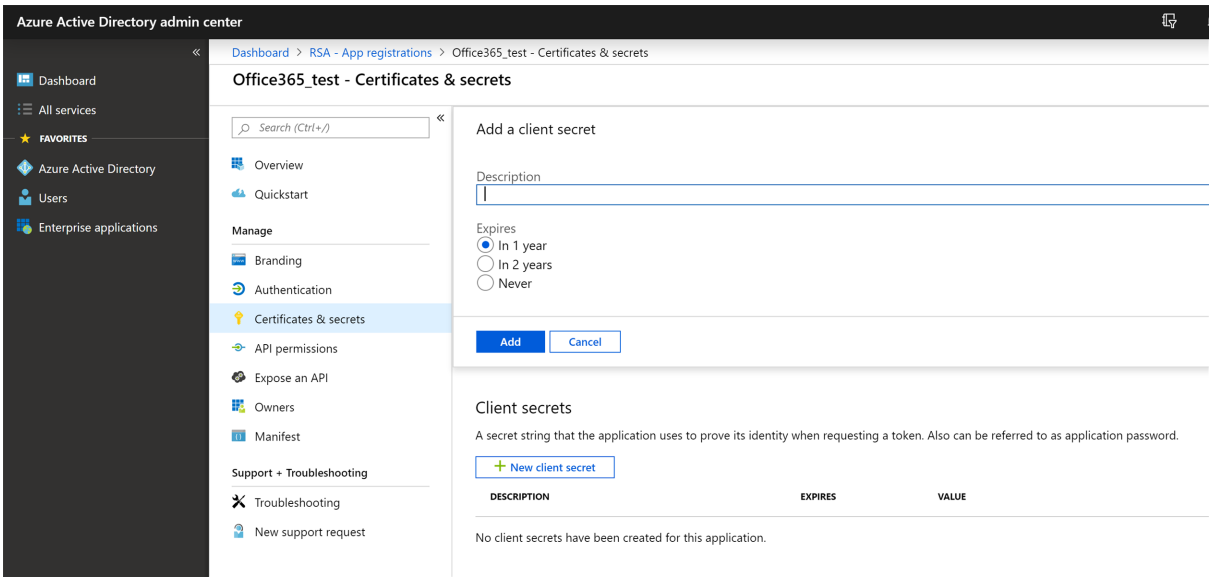
Authenticate Office365 in Active Directory by following any one of the methods below.

- Secret Key Creation
- Certificate Authentication

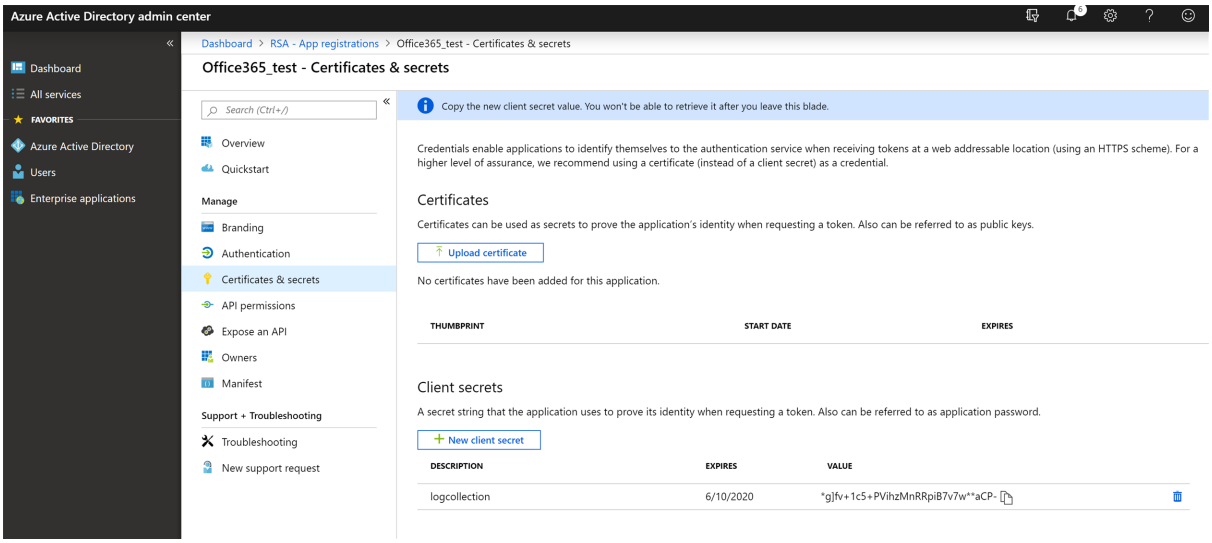
Secret Key Creation

This topic explains the process of creating a key to enable subscription and configure NetWitness plugin.

1. In the left menu bar, click **Certificates & secrets**, then click **New client secret**.



2. Add new client secret information and click **Add**.



IMPORTANT: Azure only displays the client secret at the time you initially generate it. You cannot navigate back to this page and retrieve the client secret later. Make sure to copy and save this key, as it is needed for further configuration.

Certificate Authentication

This topic explains the process of creating a certificate to enable subscription and configure NetWitness plugin.

1. Create a certificate and a private key for authentication. Follow the steps in the link below.

   https://github.com/AzureAD/azure-activedirectory-library-for-python/wiki/Client-credentials#client-credentials-with-certificate.

   IMPORTANT: When you execute Create a certificate request command, make sure that you pass a blank value for `A challenge password []:`

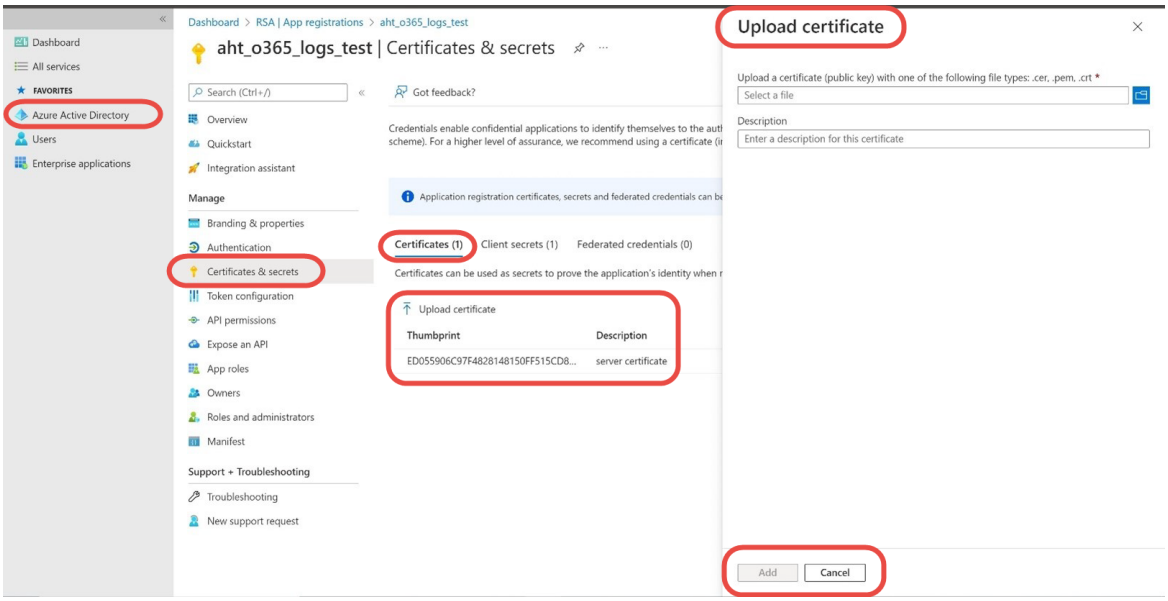
   IMPORTANT: Keep the `server.pem` file securely as it is required to enable subscription and NetWitness plugin configuration.

2. In **Azure Active Directory** app, go to **Certificates & secrets** > **Certificates** > **Upload certificate**.

3. On the **Upload certificate** dialog,

   a. Select the `server.crt` certificate that you have created in step 1.

   b. Provide a short description in the **Description box** and click **Add**. A Thumbprint is created after the certificate is uploaded successfully. This thumbprint is required to enable subscription and configure NetWitness plugin.



Deploy the Office 365 Files from NetWitness Platform Live

Office 365 requires resources available in Live NetWitness Platform in order to collect logs. Office 365 uses the cef/json parser.

Note: For 12.2.x and beyond, while configuring the Office 365 Event Source in the RSA NetWitness Platform, by default Enable Raw JSON Event parameter will be set to False. Based on the value for the parameter “Enable Raw JSON Event” choose the appropriate parser. If Enable Raw JSON Event set to false, then use cef parser.(Default setting). If Enable Raw JSON Event set to true, then use msoffice365 parser.

To deploy the Office 365 content from Live:

1. In the RSA NetWitness Platform menu, select **Live**.
2. Follow the below steps:

a. Browse Live for the cef/msoffice365 parser, using **RSA Log Device** as the Resource Type.

b. Select the cef/msoffice365 parser from the list.

c. Click **Deploy** to deploy the cef/msoffice365 parser to the appropriate Log Decoders, using the Deployment Wizard.

3. You also need to deploy the Office 365 package. Browse Live for MS Office 365 content, typing **Office 365** into the Keywords text box and click **Search**.
4. Select the item returned from the search and click **Deploy** to deploy to the appropriate Log Collectors.

Note: On a hybrid installation, you need to deploy the package on both the VLC and the LC. If you deploy the package on the LC, you need to restart the logdecoder and log collector services: otherwise, logs are not collected.

5. Restart the **nwlogcollector** service.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the *Live Resource Guide* on RSA Link.

Note: The msoffice365 parser can be used only for versions 12.2.x and beyond.

Enable Subscription

Go to the **office365audit** folder on the VLC/log collector and execute **SubscribeLogCategory.py** to subscribe to a resource group:

```
# cd
/etc/netwitness/ng/logcollection/content/collection/cmdscript/office365audit
# source /opt/rh/rh-python36/enable
# python -V
```

Note: Make sure the command `python -V` returns the value **version 3.6**.

1. If you opt for secret key authentication, execute the command below.

```
# python3 SubscribeLogCategory.py <TenantID> <Application id> <ResourceGroup>
--application_key=<> --certificate_authentication=false [--proxy_server PROXY_
SERVER] [--proxy_port PROXY_PORT] [--proxy_user PROXY_ USER] [--proxy_password
PROXY_PASSWORD]
```

Note: `application_key` value should be the secret key created by following the steps mentioned in Secret Key Creation.

Note: `Application id` should be your client id of Azure AD application.

Example:

```
1.cd/etc/netwitness/ng/logcollection/content/collection/cmdscript/office365au
dit
2.python3 SubscribeLogCategory.py xxxtenantidxx xxxresource_
groupxxxAudit.AzureActiveDirectory --application_key=xxxxxxx --certificate_
authentication=false
```

2. If you opt for certificate authentication,

   - Copy the `server.pem` file you created in step 1 of the section Certificate Authentication, and paste it into the `/etc/netwitness/ng/logcollection/content/collection/cmdscript/office365audit` directory in Log Collector.
   - Execute the below command.

     ```
     # python3 SubscribeLogCategory.py <TenantID> <Application id>
     <ResourceGroup> --private_key=server.pem --certificate_
     authentication=true --thumbprint=<Thumbprint> [--proxy_server PROXY_
     SERVER] [--proxy_port PROXY_PORT] [--proxy_user PROXY_ USER] [--proxy_
     password PROXY_PASSWORD]
     ```

     Note: `thumbprint` value can be found in **office365** > **Azure active directory** > **Certificates&Secrets**. For more information, see Certificate Authentication.

     Example:

     ```
     [root@LH3 office365audit]# pwd
     /etc/netwitness/ng/logcollection/content/collection/cmdscript/office365au
     dit
     [root@LH3 office365audit]# python3 SubscribeLogCategory.py RSA_
     Netwitness.onmicrosoft.com 925e1a0d-cc79-4d7c-a1c6-xyzwmmmw
     Audit.AzureActiveDirectory --private_key=server.pem --certificate_
     authentication=true --
     thumbprint=ED055906C97F4828148150FF515CD1234590C8975
     ```

Set Up the Office 365 Event Source in NetWitness Platform

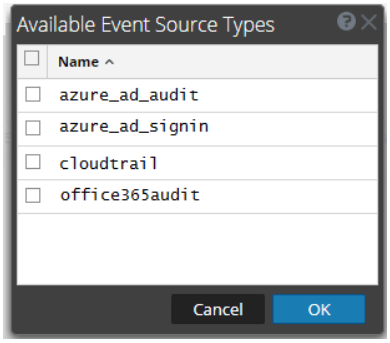
This section contains details on setting up the event source in NetWitness Platform . In addition to the procedure, the Office 365 Collection Configuration Parameters are described, as well as how to Collecting Office 365 Events in NetWitness Platform.

To configure the Office 365 Event Source:

1. In the RSA NetWitness Platform menu, select **Administration > Services**.
2. In the **Services grid**, select a Log Collector service, and from the **Actions** menu, choose **View** > **Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The **Event Categories** panel displays the File event sources that are configured, if any.
4. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog is displayed.

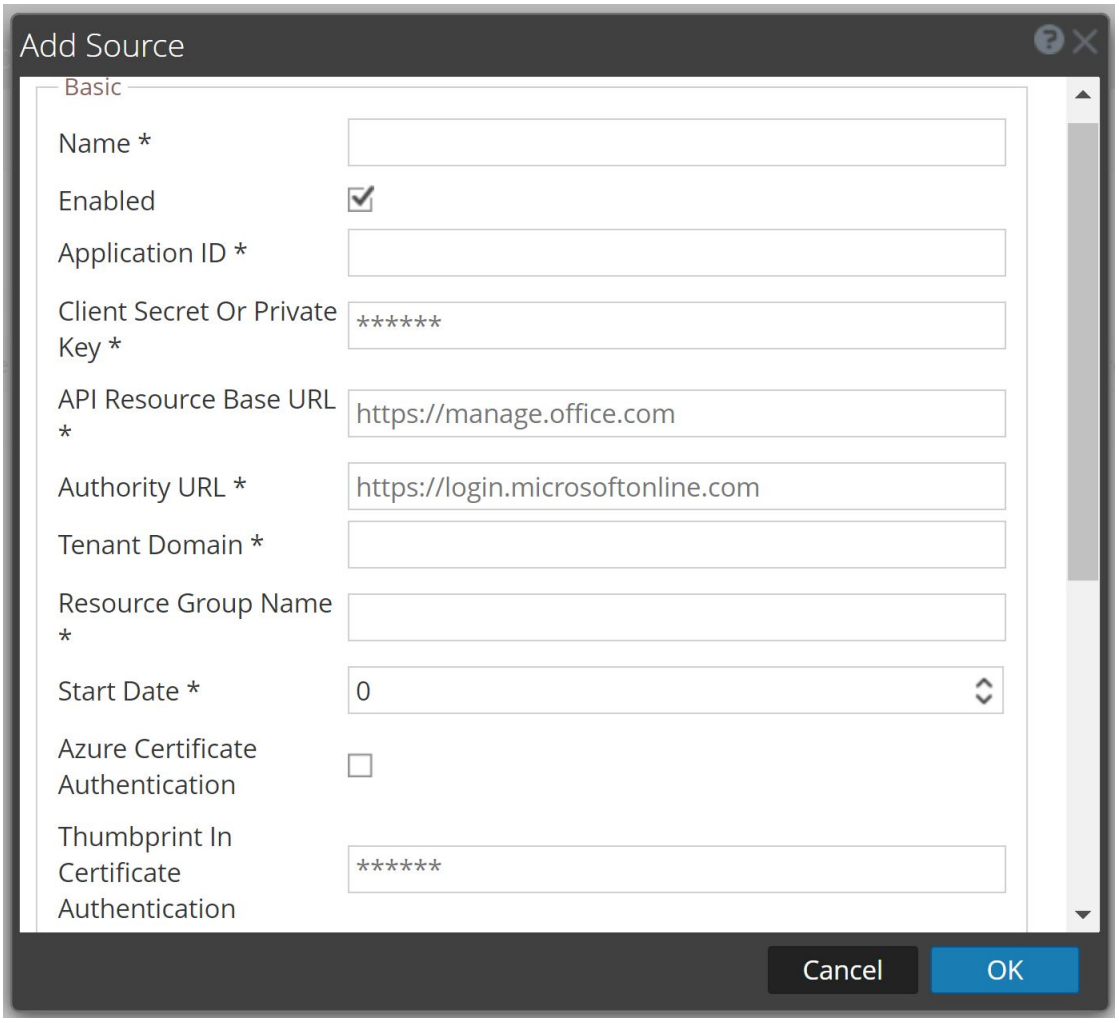


5. Select **office365audit** from the list, and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.

6. Select the **new type** in the **Event Categories** panel and click + in the **Sources** panel toolbar.

   The **Add Source** dialog is displayed.



7. Define parameter values, as described in Office 365 Collection Configuration Parameters.
8. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

   Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and RSA NetWitness Platform displays an error message.

9. If the test is successful, click **OK**.

   The new event source is displayed in the Sources panel.

Office 365 Collection Configuration Parameters

The following table describes the configuration parameter for the Microsoft Office 365 integration with NetWitness Platform . Fields marked with an asterisk (*) are required.

Note: When run from behind an SSL proxy, if certificate verification needs to be disabled, uncheck the **SSL Enable** checkbox in the **Advanced** section.

Note: For more details, see the following Microsoft website: https://msdn.microsoft.com/en-us/office-365/office-365-management-activity-api-reference#retrieving-content.

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the box to enable the event source configuration to start collection. The box is selected by default.
Application ID *	The Client ID is found the Azure Application Configure tab. Scroll down until you see it.
Client Secret or Private Key *	When you are configuring the event source, • If you opt for secret key authentication, enter the client secret. For more information, see Secret Key Creation. • If you opt for certificate authentication, enter full content from the file `server.pem` that was created in step 1 of Certificate Authentication.
API Resource Base URL *	Enter https://manage.office.com
Authority URL	Enter https://login.microsoftonline.com
Tenant Domain * / Tenant ID	Go to the active directory and click on the directory. In the Active Directory list, click the directory that you are using with your Office 365 tenant . The tenant ID for your Office 365 tenant is displayed as part of the URL. RSA recommends you use a Tenant Domain, rather than an ID. Example Tenant Domain: `netwitnesstest.onmicrosoft.com`

Name	Description
Resource Group Names *	Resource group names specify the Log categories to which you are subscribed. For details, see Collecting Office 365 Events in NetWitness Platform. Enter one of the following values: `[Audit.AzureActiveDirectory , Audit.Exchange , Audit.SharePoint , Audit.General, DLP.All]` To subscribe to more than one log category, you need to repeat the Collecting Office 365 Events in NetWitness Platform procedure and select another value.
Start Date *	Choose the date from which to start collecting. This parameter defaults to the current date.
Azure Certificate Authentication	Select this checkbox if you want to use office365 certificate authentication method. This is unchecked by default.
Thumbprint in Certificate Authentication	Enter the thumbprint value available in your **office365** > **Azure active directory** > **Certificates&Secrets**. For more information, see Certificate Authentication.
Use Proxy	Check to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	Enter the proxy port.
Proxy User	Username for the proxy (leave empty if using anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).
Source Address	A custom value chosen to represent the hostname for the Office365 Event Source in the customer environment, such as **jupiter.example.net**. The value of this parameter is captured by the **device.host** meta key.

Name	Description
Enable Raw JSON event	Enable Raw JSON event in configuration UI is applicable only on LC version 11.5 or above. Default behavior is that the raw events are transformed to cef format. Enabling this skips the transformation as the raw JSON events are sent to decoder in syslog 5424 format. To parse these logs collected in raw JSON format, need to deploy msoffice365 parser from live.

Advanced Parameters

Click **Advanced** to view and edit the advanced parameters.

Name	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is 180.For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug Caution	Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Caution: Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: Off = (default) disabled On = enabled Verbose = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit

	the number of event sources to minimize performance impact.
SSL Enable	Uncheck to disable certificate verification.
No of Threads*	No of concurrent threads to use to collect events. Be cautious in increasing this value as more threads might lead to throttling resulting in delay in log collection.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.