FortiAnalyzer ServiceNow Integration - User Guide

Version 2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 20, 2020
FortiAnalyzer ServiceNow Integration 2.0 User Guide
05-602-508182-20200520

TABLE OF CONTENTS

Overview

Use the FortiAnalyzer Integration App to:

- Import and review incidents and events generated in FortiAnalyzer to the ServiceNow platform.
  You can use the imported data with other apps and services to respond to incidents.
- Automatically or manually create security incidents from the FortiAnalyzer Integration App GUI on the ServiceNow SecOps Incident Response App.

You can also use the data with other ServiceNow apps and services using ServiceNow scripts and business rules. In order to set up the FortiAnalyzer Integration App, some configuration are required on both FortiAnalyzer and ServiceNow platform.

The FortiAnalyzer Integration App is supported for desktop use in English and is available in the ServiceNow Store. See Setting up the FortiAnalyzer Integration App on page 6.

For information on using FortiAnalyzer, see the FortiAnalyzer guides in the Fortinet Document Library, especially the Administration Guide, the Release Notes, and Best Practices.

Setting Up FortiAnalyzer

Task	Description

Create or select an account to use for integration with the FortiAnalyzer Integration App.	Set up JSON-RPC read-write permission for the account.
	The profile for this account only requires read-write access to *Incidents & Events*.
	API calls from the app require the account to have JSON-RPC read-write permission.
	Use CLI commands to set JSON-RPC permission:
	`config system admin user`
	`   edit servicenow_account`
	`      set rpc-permit read-write`
	`   end`
	For more information, see the FortiAnalyzer Administration Guide in the Fortinet Document Library.

Install a trusted, signed SSL certificate and CA certificate	ServiceNow requires a trusted, signed SSL certificate and CA certificate for secure API communication. See the *Certificates* section in the *FortiAnalyzer Administration Guide*.
Create Fabric Connectors in *Fabric View*.	You will use the Fabric Connector to send notifications to the FortiAnalyzer Integration App upon creation or update of incidents: • Get the *ServiceNow API URL* from the *FortiAnalyzer Integration App* > *FortiAnalyzer System Properties*. • Use the same credentials for the ServiceNow API account from the *FortiAnalyzer System Properties* > *Connection to ServiceNow API* section. See Set up the system properties on page 6. For more information, see *Creating or editing ITSM connectors* section in the *FortiAnalyzer Administration Guide*.
Enable incident notifications on FortiAnalyzer.	This will notify the FortiAnalyzer Integration App when an incident is raised or updated on FortiAnalyzer. Go to *Incidents & Events* > *Incidents* > *Settings* to enable notifications. For more information, see the following sections in the *FortiAnalyzer Administration Guide*: • *Creating or editing ITSM connectors* • *Configuring incident settings*

Setting up the FortiAnalyzer Integration App

ServiceNow requirements

- A ServiceNow subscription.
- FortiAnalyzer 6.0.2 or higher.
- ServiceNow SecOps Incident Response App

For information on ServiceNow licenses, contact ServiceNow.

For information on ServiceNow user roles and permissions, see ServiceNow roles on page 13

Download the FortiAnalyzer Integration App

To download the app, go to the ServiceNow store and search for **FortiAnaylzyer Integration App V2**. Click *Get*, then follow the onscreen instructions to download the app.

After downloading the app, add it to the *Favorites* menu for easy access.

Create a ServiceNow API account

1. In ServiceNow, create an account for API communication with FortiAnalyzer.
   For more information, see the ServiceNow documentation.
2. Assign these roles to this account:

Role	Description
`import_transformer`	This is a system role to manage import set transform maps and run transforms.
`x_forti_fazintgv2.snAPI`	This role is required to access ServiceNow API so FortiAnalyzer can send incident notifications to the FortiAnalyzer Integration App.
`sn_si.basic`	This role comes with ServiceNow SecOps Incident Response App to view and create security incidents.

Refer to ServiceNow documents for more information.

Set up the system properties

1. Open the *FortiAnalyzer Integration App* and go to *FortiAnalyzer System Properties*.
2. Configure *Connection to FortiAnalyzer API*:

Property	Description
Domain	Enter the FortiAnalyzer domain name without the protocol, for example,

Property	Description
	`fortianalyzer.myorganization.com`
Port number	If you change the port number, you must also change it in FortiAnalyzer.
Username *Password*	Enter the username and password of the FortiAnalyzer account to use with the FortiAnalyzer Integration App. This account must have JSON-RPC read-write permission in FortiAnalyzer.

3. Configure *Connection to ServiceNow API*.
   Enter the *Username* and *Password* for the ServiceNow API account you created in the previous section.
4. Configure *App Settings*:

Property	Description
Create a security incident in Security Incident Response App, upon receiving new incident notifications from FortiAnalyzer	Automatically creates an incident in the FortiAnalyzer Integration App from an imported FortiAnalyzer incident. You can create a business rule to further customize incidents after creation in ServiceNow. See Automation with business rules on page 8.
Keep updating FortiAnalyzer incidents, upon receiving update notifications from FortiAnalyzer	Updates FortiAnalyzer incidents after the initial import. This setting is enabled by default.
Fetch events from FortiAnalyzer ADOMs automatically	1. From the *FortiAnalyzer ADOMs* list, select the ADOMs you want to import events from. 2. Use the *Start Date* filter to select the date to start importing events. 3. (Optional) Select *Keep updating FortiAnalyzer events* to automatically update FortiAnalyzer events after the initial import.

5. Click *Save*.

Automation with business rules

You can use a business rule to automate tasks on SeviceNow. A business rule is a server-side script that runs when a record is displayed, inserted, updated, or deleted, or when a table is queried.

You can create a business rule to monitor FortiAnalyzer incidents and events imported or updated on the FortiAnalyzer Integration App.

To create a business rule:

1. In ServiceNow go to *System Definition* > *Business Rules* or type `Business Rules` in the application explorer.
2. In the *Business Rules* page, click *New*.

Example business rule:

The following example uses a business rule to create a **customized** security incident when a *Denial of Service* incident is raised in FortiAnalyzer.

1. Configure the business rule settings.

Property	Description
Name	Enter a name for the business rule.
Table	Select *faz_incident_secops* from the list.
Application	This is the application that contains the business rule. The application is set to *Global* by default and cannot be changed.
Active	This enables the business rule.
Advanced	Select this option to see the advanced version of the form.

2. In the *When to Run* area, configure the business rule condition.

When	Select *After* to run the business rule when the conditions are met.
Update	Select this option to run the business rule when the incident is updated.
Filter Conditions	• Select *Category* from the *choose field* list. • Set the operator to *Is*. • Enter `CAT2` in the *Value* field to run the business rule when FortiAnalyzer creates a *Denial of Service(DoS)* incident.
Role Conditions	Select the roles users who are modifying records in the table must have for this business rule to run. ServiceNow roles on page 13

3. In the *Advanced* area, create a script that runs when the defined condition is true.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td><b>Conditions</b></td><td>Enter a conditional statement to specify when the business rule should run.</td></tr>
<tr><td><b>Script</b></td><td>The following script demonstrates how to change the form fields when the condition is met:
<pre>
(function executeRule(current, previous /*null when async*/)
     {
  var incid = current.getValue('incid');
  // Check whether it exists or not
  var egr = new GlideRecord('sn_si_incident');
     egr.addQuery('short_description=' + incid);
     egr.query();
     if (egr.next()) {
                   return;
     }

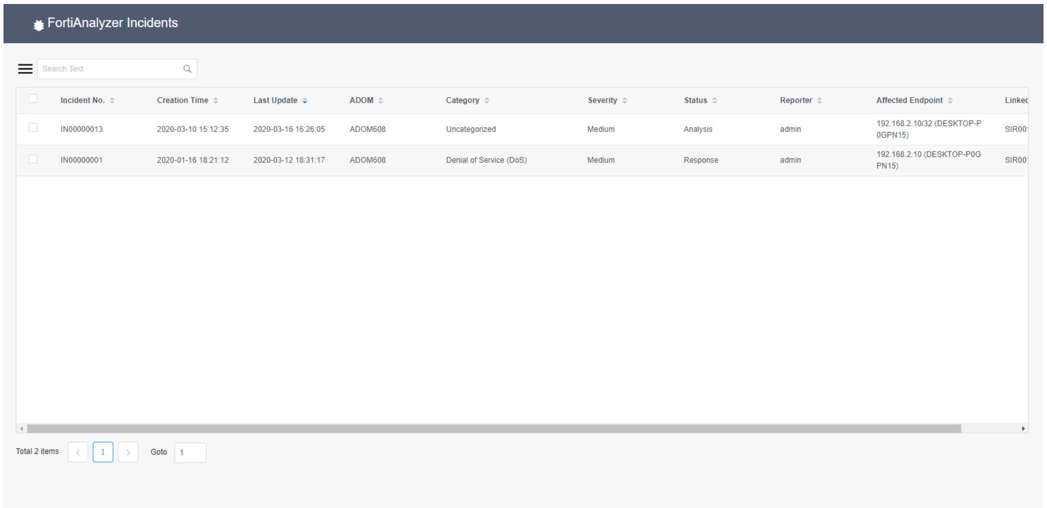
     // Current data
     var severity = current.getValue('severity');
     var description = current.getValue('description');
     var sn_impact = 3; // low
     var sn_priority = 4; // low
     var sn_Severity = 3; // low
     if (severity == "high") {
        sn_impact = 1;
        sn_priority = 2;
        sn_Severity = 1;
     } else if (severity == "medium") {
        sn_impact = 2;
        sn_priority = 3;
        sn_Severity =2;
     }

     // Security Incident
     var gr = new GlideRecord('sn_si_incident');
     gr.initialize();
     gr.state = 1; // Analysis
     gr.substate = 3; // Pending incident
     gr.category = "Denial of Service";
     gr.subcategory = 12; // Inbound or outbound
     gr.severity = sn_Severity;
     gr.impact = sn_impact;
     gr.priority = sn_priority;
     gr.short_description = incid ;
     gr.description = 'copy description from faz: ' +
           description;
     gr.insert();
  ])(curent,previous);
</pre></td></tr>
</table>

4. Click *Submit*.

FortiAnalyzer incidents

Incidents will be imported from FortiAnalyzer and displayed in the *FortiAnalyzer Integration App* > *FortiAnalyzer Incidents* after ServiceNow receives notification from FortiAnalyzer upon the creation or update of an incident.



□	Incident No.	Creation Time	Last Update	ADOM	Category	Severity	Status	Reporter	Affected Endpoint	Linked
□	IN00000013	2020-03-10 15:12:35	2020-03-16 16:26:05	ADOM608	Uncategorized	Medium	Analysis	admin	192.168.2.10/32 (DESKTOP-P0GPN15)	SIR00
□	IN00000001	2020-01-16 18:21:12	2020-03-12 18:31:17	ADOM608	Denial of Service (DoS)	Medium	Response	admin	192.168.2.10 (DESKTOP-P0GPN15)	SIR00

To create a security incident manually in the FortiAnalyzer Integration App:

1. Go to *FortiAnalyzer Integration App* > *FortiAnalyzer Incidents*.
2. Click an incident to display the incident details.
3. In the incident details view, click *Create Security Incident*.
   A message shows the security incident number.

To view a security incident:

1. Go to *FortiAnalyzer Integration App* > *FortiAnalyzer Incidents*.
2. Click an incident to display the incident details
3. In the incident details view, click *Open Security Incident*.
   The *FortiAnalyzer Incident* tab displays FortiAnalyzer incident details and attached events

To search for a security incident:

The *Search Text* field is not case-sensitive. You can search for multiple keywords using a pair of ampersands separated by a space.

For example, `11 && 22 && 33`.

To customize the view:

Click *Menu* next to the search field to *Refresh List* or *Manage Columns*.

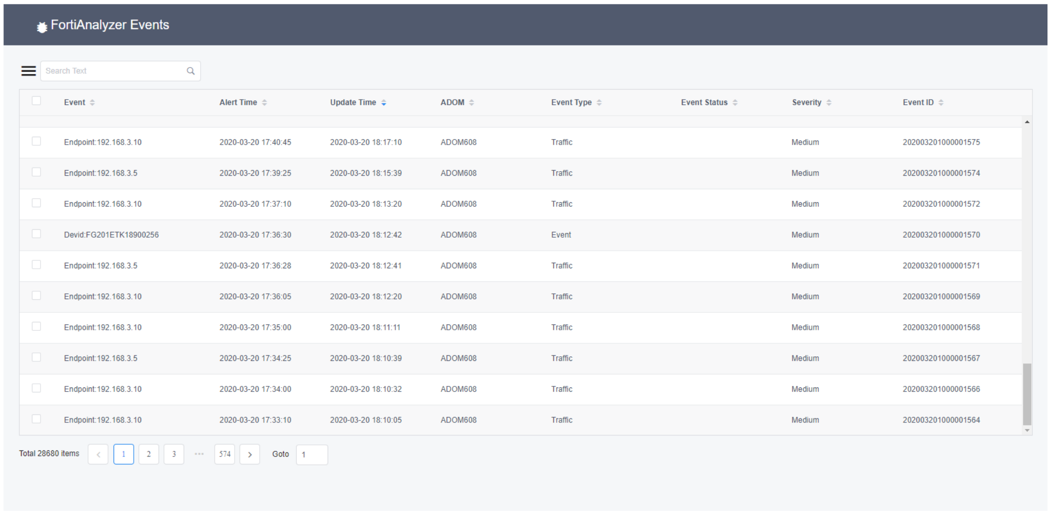
To remove an incident:

Select the incident and click *Delete*. Removing an incident from the view does not delete it from the database.

You must have `x_forti_fazintgv2.admin` user role to remove an incident. See ServiceNow roles on page 13.

FortiAnalyzer events

Events will be imported in predefined 10-second intervals from FortiAnalyzer and displayed in *FortiAnalyzer Integration App* > *FortiAnalyzer Events*.



FortiAnalyzer Events

□	Event	Alert Time	Update Time	ADOM	Event Type	Event Status	Severity	Event ID
□	Endpoint:192.168.3.10	2020-03-20 17:40:45	2020-03-20 18:17:10	ADOM608	Traffic		Medium	202003201000001575
□	Endpoint:192.168.3.5	2020-03-20 17:39:25	2020-03-20 18:15:39	ADOM608	Traffic		Medium	202003201000001574
□	Endpoint:192.168.3.10	2020-03-20 17:37:10	2020-03-20 18:13:20	ADOM608	Traffic		Medium	202003201000001572
□	Devid:FG201ETK18900256	2020-03-20 17:36:30	2020-03-20 18:12:42	ADOM608	Event		Medium	202003201000001570
□	Endpoint:192.168.3.5	2020-03-20 17:36:28	2020-03-20 18:12:41	ADOM608	Traffic		Medium	202003201000001571
□	Endpoint:192.168.3.10	2020-03-20 17:36:05	2020-03-20 18:12:20	ADOM608	Traffic		Medium	202003201000001569
□	Endpoint:192.168.3.10	2020-03-20 17:35:00	2020-03-20 18:11:11	ADOM608	Traffic		Medium	202003201000001568
□	Endpoint:192.168.3.5	2020-03-20 17:34:25	2020-03-20 18:10:39	ADOM608	Traffic		Medium	202003201000001567
□	Endpoint:192.168.3.10	2020-03-20 17:34:00	2020-03-20 18:10:32	ADOM608	Traffic		Medium	202003201000001566
□	Endpoint:192.168.3.10	2020-03-20 17:33:10	2020-03-20 18:10:05	ADOM608	Traffic		Medium	202003201000001564

To search for an event:

The *Search Text* field is not case-sensitive. You can search for multiple keywords using a pair of ampersands separated by a space.

For example, `11 && 22 && 33`.

To customize the view:

Click *Menu* next to the search field to *Refresh List* or *Manage Columns*.

To remove an event:

Select the event and click *Delete*. Removing an event from the view does not delete it from the database.

The event may reappear when "*Keep updating FortiAnalyzer incidents, upon receiving update notifications from FortiAnalyzer*" is selected in *System Properties*. See Setting up the FortiAnalyzer Integration App on page 6.

You must have `x_forti_fazintgv2.admin` user role to remove an event. See ServiceNow roles on page 13.

ServiceNow roles

Admins need a ServiceNow account with the right roles to work with ServiceNow apps. For information on ServiceNow-specific roles, see the ServiceNow Base system roles.

Admins also need to have the right roles added by the FortiAnalyzer Integration App depending on their responsibilities. The following are the FortiAnalyzer Integration App roles and descriptions:

Role	Description
x_forti_fazintgv2.admin	This role has full control over the app. Admins who do debugging and maintenance need this role to edit tables and records.
x_forti_fazintgv2.analyst	This role is required to view FortiAnalyzer incidents, events, tables, and records in the app. Security analysts need this role to work with incidents.
x_forti_fazintgv2.snAPI	This role is required to access ServiceNow API so FortiAnalyzer can send incident notifications to the FortiAnalyzer Integration App.

Troubleshooting

Error messages in the FortiAnalyzer Integration App GUI and in the ServiceNow *Application Logs* describe the problem and usually contain recommendations to correct it.

Connection problems

To troubleshoot connection problems between FortiAnalyzer and the FortiAnalyzer Integration App:

1. In FortiAnalyzer, go to *System Settings* > *Admin* > *Administrators*.
    a. Click the account used for integration with the FortiAnalyzer Integration App and check that the settings are correct.
    See Setting Up FortiAnalyzer on page 5.
2. Check that you have set up JSON-RPC permission correctly.

    Ensure the Username can be found in FortiAnalyzer and has JSON-RPC permission.

    See Setting Up FortiAnalyzer on page 5.
3. Go to the FortiAnalyzer Integration App *System Properties*.
    a. Check that the connection settings are correct, especially the domain name, port number, ADOMs, and API credentials.

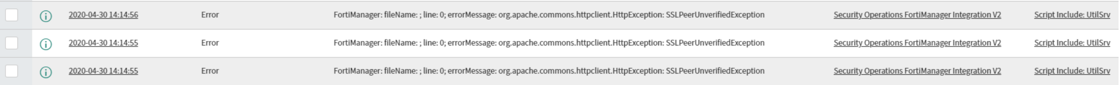
    - Ensure the Domain HTTPS link is correct.
    - Ensure a trusted, signed SSL certificate is installed.
    - Ensure the port number is correct.
    - Ensure the password is correct.

    See Setting up the FortiAnalyzer Integration App on page 6.

    If connection settings are incorrect, the app displays an error message when you click *Save*.

    b. Check that you are using a supported firmware version.
4. Check that the FortiAnalyzer is missing a certificate, or the certificate is incomplete. ServiceNow requires a trusted certificate on FortiAnalyzer to establish a secured connection.
    a. In ServiceNow, go to *Application Log* > *Errors*. The following error may indicate the certificate is incomplete:

```
fileName:
      ;line:0;errorMessage:org.apache.commons.httpclient.HttpException:SSLPeerUnverifie
      dException
```



☐	2020-04-30 14:14:56	Error	FortiManager: fileName: ; line: 0; errorMessage: org.apache.commons.httpclient.HttpException: SSLPeerUnverifiedException	Security Operations FortiManager Integration V2	Script Include: UtilSrv
☐	2020-04-30 14:14:55	Error	FortiManager: fileName: ; line: 0; errorMessage: org.apache.commons.httpclient.HttpException: SSLPeerUnverifiedException	Security Operations FortiManager Integration V2	Script Include: UtilSrv
☐	2020-04-30 14:14:55	Error	FortiManager: fileName: ; line: 0; errorMessage: org.apache.commons.httpclient.HttpException: SSLPeerUnverifiedException	Security Operations FortiManager Integration V2	Script Include: UtilSrv

    b. Use a third-party service such as *digicert* or *sslshopper* to identify the errors on the FortiAnalyzer side.
    c. In FortiAnalyzer, go to *System Settings* > *Certificates*, to fix the certificate issues, such as adding an intermediate CA certificate.

To troubleshoot event logs that are not updating:

Event logs are not automatically updated after a FortiAnalyzer service outage when "*Fetch events from FortiAnalyzer ADOMs automatically*" is enabled. To resume updates after service is restored, run the *Run_FetchFAZEvents* script.

You must have an admin role to perform this task.

1. Go to *System Definition* > *Scheduled Jobs*, or type `scheduled jobs` in the system explorer.
2. Type `*faz` in the *Search* field.
3. Click *Run_FetchFAZEvents*.
4. Deselect *Active* and select it again to resume the updates.

Others

To view log message errors, go to ServiceNow, click *All applications* and search for *System Log*. Then select *Application Logs*.

In the *App Log* pane, check for errors. You can filter by keywords to search for messages.

Error	Possible solutions
User cannot log in	• Check that the user account has the correct roles. • Check the spelling of the username and password.
Error message: `FortiAnalyzer: fileName: ; line: 0; message: Unknown host`	Check the name and spelling of the Domain.
Error message: `ServiceNow API user snapi needs to have x_forti_fazintgv2.snAPI role assigned`	Assign the *x_forti_fazintgv2.snAPI* role to the ServiceNow account. See Setting up the FortiAnalyzer Integration App on page 6.
Error message: `ServiceNow API user snapi needs to have import_transformerrole assigned`	Assign the *import_transformer* to the ServiceNow account. See Setting up the FortiAnalyzer Integration App on page 6.
FortiAnalyzer Incidents are not up-to-date	Synchronizing incidents takes time. Wait a few minutes and try again.

Change Log

Date	Change Description
2020-03-31	Initial release.
2020-05-20	Updated Troubleshooting on page 14 and Setting Up FortiAnalyzer on page 5.