



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/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



September1, 2022

FortiAnalyzer ServiceNow Integration 2.0 User Guide

05-640-838967-20220901

TABLE OF CONTENTS

| | |
|---|-----------|
| Overview | 4 |
| Setting Up FortiAnalyzer | 5 |
| Setting up the FortiAnalyzer Integration App | 7 |
| ServiceNow requirements | 7 |
| Download the FortiAnalyzer Integration App | 7 |
| Create a ServiceNow API account | 7 |
| Set up the system properties | 7 |
| Automation with business rules | 9 |
| FortiAnalyzer incidents | 11 |
| FortiAnalyzer events | 13 |
| ServiceNow roles | 14 |
| Troubleshooting | 15 |
| Connection problems | 15 |
| Others | 16 |
| Change Log | 17 |

Overview

This document explains the setup and usage of the FortiAnalyzer Integration App for ServiceNow with FortiAnalyzer 6.4 devices.

You can use the FortiAnalyzer Integration App to:

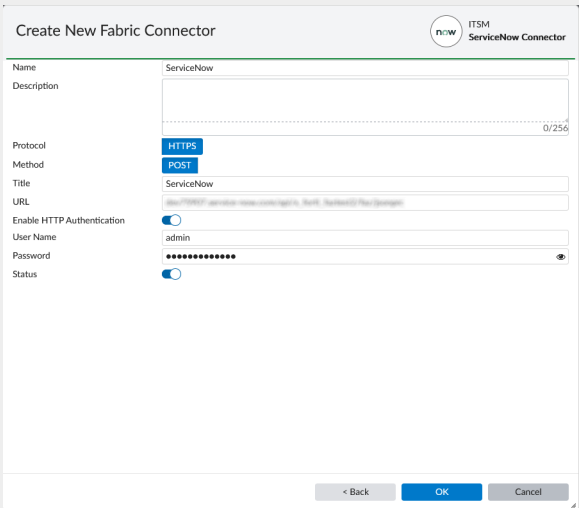
- Import and review incidents and events generated in FortiAnalyzer to the ServiceNow platform.
You can use the imported data with other apps and services to respond to incidents.
- Automatically or manually create security incidents from the FortiAnalyzer Integration App GUI on the ServiceNow SecOps 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 7](#).

For information on using FortiAnalyzer, see the FortiAnalyzer guides in the [Fortinet Document Library](#), including the Administration Guide, Release Notes, and Best Practices.

Setting Up FortiAnalyzer

| Task | Description |
|--|--|
| Create or select an account to use for integration with the FortiAnalyzer Integration App. | <p>Set up JSON-RPC read-write permission for the account.</p> <p>The profile for this account requires read-write access to <i>Incidents & Events/FortiSoC</i>.</p> <p>API calls from the app require the account to have JSON-RPC read-write permission.</p> <p>Use CLI commands to set JSON-RPC permission:</p> <pre>config system admin user edit servicenow_account set rpc-permit read-write end</pre> <p>For more information, see the FortiAnalyzer Administration Guide in the Fortinet Document Library.</p> |
| Install a trusted, signed SSL certificate and CA certificate | <p>ServiceNow requires a trusted, signed SSL certificate and CA certificate for secure API communication.</p> <p>For more information, see the <i>Certificates</i> section in the FortiAnalyzer Administration Guide in the Fortinet Document Library.</p> |
| Create a ServiceNow Fabric Connector in <i>Fabric View</i> . | <p>You will use the Fabric Connector to send notifications to the FortiAnalyzer Integration App upon creation or update of incidents:</p> <ul style="list-style-type: none"> Get the <i>ServiceNow API URL</i> from the <i>FortiAnalyzer Integration App > FortiAnalyzer System Properties</i>. Use the same credentials for the ServiceNow API account from the <i>FortiAnalyzer System Properties > Connection to ServiceNow API</i> section. See Set up the system properties on page 7.  <p>For more information, see <i>Creating or editing ITSM connectors</i> section in the FortiAnalyzer Administration Guide in the Fortinet Document Library.</p> |

| Task | Description |
|--|--|
| Enable incident notifications on FortiAnalyzer | <p>This will notify the FortiAnalyzer Integration App when an incident is raised or updated on FortiAnalyzer.</p> <p>Go to <i>FortiSoC > Incidents > Settings</i> to enable notifications.</p> <p>For more information, see the following sections in the FortiAnalyzer Administration Guide in the Fortinet Document Library:</p> <ul style="list-style-type: none">• <i>Creating or editing ITSM connectors</i>• <i>Configuring incident settings</i> |

Setting up the FortiAnalyzer Integration App

ServiceNow requirements

- A ServiceNow subscription.
- FortiAnalyzer 6.4.0 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 14](#)

Download the FortiAnalyzer Integration App

To download the app, go to the [ServiceNow store](#) and search for *Security Operations FortiAnalyzer 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 |
|--------------------------------------|---|
| <code>import_transformer</code> | This is a system role to manage import set transform maps and run transforms. |
| <code>x_forti_fazintgv2.snAPI</code> | This role is required to access ServiceNow API so FortiAnalyzer can send incident notifications to the FortiAnalyzer Integration App. |
| <code>sn_si.basic</code> | 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 |
|---------------|--|
| <i>Domain</i> | Enter the FortiAnalyzer domain name without the protocol, for example, |

| Property | Description |
|--------------------|---|
| | <code>fortianalyzer.myorganization.com</code> |
| <i>Port number</i> | If you change the port number, you must also change it in FortiAnalyzer. |
| <i>Username</i> | 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. |
| <i>Password</i> | |

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 |
|---|--|
| <i>Create a security incident in Security Incident Response App, upon receiving new incident notifications from FortiAnalyzer</i> | <p>Automatically creates an incident in the FortiAnalyzer Integration App from an imported FortiAnalyzer incident.</p> <hr/> <div>  <p>You can create a business rule to further customize incidents after creation in ServiceNow. See Automation with business rules on page 9.</p> </div> |
| <i>Keep updating FortiAnalyzer incidents, upon receiving update notifications from FortiAnalyzer</i> | <p>Updates FortiAnalyzer incidents after the initial import.</p> <p>This setting is enabled by default.</p> |
| <i>Fetch events from FortiAnalyzer ADOMs automatically</i> | <ol style="list-style-type: none"> 1. From the <i>FortiAnalyzer ADOMs</i> list, select the ADOMs you want to import events from. 2. Use the <i>Start Date</i> filter to select the date to start importing events. 3. (Optional) Select <i>Keep updating FortiAnalyzer events</i> 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 ServiceNow. 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 <i>faz_incident_secops</i> from the list. |
| Application | This is the application that contains the business rule. The application is set to <i>Global</i> 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 <i>After</i> 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 | <ul style="list-style-type: none"> • Select <i>Category</i> from the <i>choose field</i> list. • Set the operator to <i>Is</i>. • Enter <code>CAT2</code> in the <i>Value</i> field to run the business rule when FortiAnalyzer creates a <i>Denial of Service(DoS)</i> 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 14 |

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

| Property | Description |
|-------------------|---|
| Conditions | Enter a conditional statement to specify when the business rule should run. |
| Script | <p>The following script demonstrates how to change the form fields when the condition is met:</p> <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(); }])(current,previous); </pre> |

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 |
|--------------|---------------------|---------------------|---------|-------------------------|----------|----------|----------|----------------------------------|--------|
| IN0000013 | 2020-03-10 15:12:35 | 2020-03-16 16:26:05 | ADOM608 | Uncategorized | Medium | Analysis | admin | 192.168.2.10/32 (DESKTOP-0GPN15) | SIR80 |
| IN0000001 | 2020-01-16 16:21:12 | 2020-03-12 16:31:17 | ADOM608 | Denial of Service (DoS) | Medium | Response | admin | 192.168.2.10 (DESKTOP-P0GPN15) | SIR90 |

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:

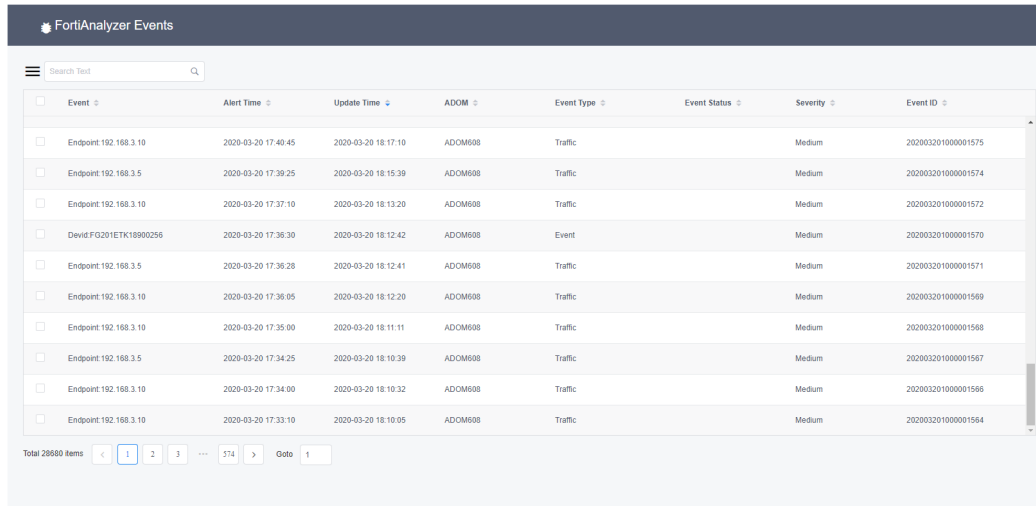
Select the incident and click *Delete*. Removing an incident from the view does not delete it from the database.



You must have `x_forti_fazintgv2.admin` user role to remove an incident. See [ServiceNow roles on page 14](#).

FortiAnalyzer events

Events will be imported in predefined 10-second intervals from FortiAnalyzer and displayed in *FortiAnalyzer Integration App > 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 |
| David 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 7](#).



You must have `x_forti_fazintgv2.admin` user role to remove an event. See [ServiceNow roles on page 14](#).

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 |
|--|---|
| <code>x_forti_fazintgv2.admin</code> | This role has full control over the app. Admins who do debugging and maintenance need this role to edit tables and records. |
| <code>x_forti_fazintgv2.analyst</code> | This role is required to view FortiAnalyzer incidents, events, tables, and records in the app. Security analysts need this role to work with incidents. |
| <code>x_forti_fazintgv2.snAPI</code> | 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 7](#).

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:SSLPeerUnverifiedException
```

| | | | | | | |
|--------------------------|--|---------------------|-------|--|---|------------------------|
| <input type="checkbox"/> | | 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: URL5cy |
| <input type="checkbox"/> | | 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: URL5cy |
| <input type="checkbox"/> | | 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: URL5cy |

- 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.

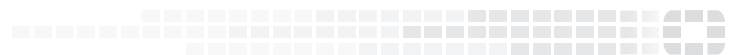
| Error | Possible solutions |
|--|--|
| User cannot log in | <ul style="list-style-type: none"> • Check that the user account has the correct roles. • Check the spelling of the username and password. |
| Error message: FortiAnalyzer: fileName: ; line: 0; message: Unknown host | Check the name and spelling of the Domain. |
| Error message: ServiceNow API user snapi needs to have x_forti_fazintgv2.snAPI role assigned | Assign the <i>x_forti_fazintgv2.snAPI</i> role to the ServiceNow account. See Setting up the FortiAnalyzer Integration App on page 7 . |
| Error message: ServiceNow API user snapi needs to have import_transformerrole assigned | Assign the <i>import_transformer</i> to the ServiceNow account. See Setting up the FortiAnalyzer Integration App on page 7 . |
| FortiAnalyzer Incidents are not up-to-date | Synchronizing incidents takes time. Wait a few minutes and try again. |

Change Log

| Date | Change Description |
|------------|--------------------|
| 2022-09-01 | Initial release. |



FORTINET®



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.