Accelerate Event Management value realization with ITOM Guided Setup

Improve mean time to repair (MTTR) and incident reduction with these implementation steps.

What’s in this Success Insight

This Success Insight will help you accelerate Event Management implementation and value realization by showing you how to use ITOM Guided Setup to quickly add an event source, get events flowing into your instance, and setup rules to create and manage alerts.

This Success Insight answers these key questions:

1. What is Event Management and what value does it provide?
2. Why should I use ITOM Guided Setup to get started with Event Management?
3. What do I need to do before I start with Guided Setup?
4. How do I use ITOM Guided Setup to get started with Event Management?
5. What are my next steps after completing Guided Setup?

1. What is Event Management and what value does it provide?

Part of the IT Operations Management (ITOM) product suite, Event Management provides the real-time state of IT infrastructure you need to look at your business service health and work to improve it. Event Management brings the events that your existing infrastructure monitoring tools capture into ServiceNow for consolidation, analysis, and action. The application processes infrastructure events through a combination of event mappings and rules, converted, and consolidated into significant alerts for investigation and remediation. Review the product documentation to learn more about Event Management’s capabilities and features.

Event Management helps you improve your mean time to repair (MTTR) and reduce the number of incidents you have through intelligent event and alert analysis. With these analyses, you can respond appropriately to any arising issues and monitor the health of your business services and
infrastructure using a single management console. Specifically, Event Management helps you deliver the following business outcomes:

- Reduction in incidents
- Possible reduction in workforce
- Shortened mean time to identify or repair (MTTR)
- Streamlined ITSM processes

2. Why should I use ITOM Guided Setup to get started with Event Management?

ITOM Guided Setup let you realize value faster by walking you through the steps needed to implement the base setup for applications that are part of the ITOM suite, including Event Management.

Using ITOM Guided Setup for Event Management accelerates your Event Management implementation and gets you to value faster. You can quickly set up your first event source and get events into the platform so you can begin managing the health of your business services and infrastructure. After you complete the ITOM Guided Setup process, you’ll be able to:

- Consolidate events from different sources
- Filter events to reduce noise and generate qualified events
- Bind events to CMDB CIs
- Identify alerts and alerts created due to planned maintenance
- Perform service impact analysis
- Provide Operator Workspace and Overview Dashboard for understanding service health/visualizing service status
- Spawn ServiceNow tasks from alerts
- Assist with alert remediation (both automated and manual)

3. What do I need to get done before I start with Guided Setup?

a) Confirm the technical prerequisites.

To do this:

- **Configure a MID Server** – If you don’t have one, work with your core ServiceNow team to request a new MID Server for Event Management. The MID Server uses the out-of-the-box (OOTB) connector to poll the monitoring source database to bring back events. You can also configure the MID Server as an SNMP trap listener or REST endpoint.

- **Enable the Event Management plugin** – If you don’t already have the plugin enabled, submit a service request on the HI Service Portal to activate it.

- **Gather login credentials for your monitoring sources** – Get the login credentials you’ll need for the Event Management OOTB connectors you want to include using ITOM Guided Setup. Examples of OOTB connectors include SolarWinds and Netcool. You can find a full list in the **product documentation**.
b) **Enlist the right team resources.**
There are multiple roles and specific skills required to implement Event Management with ITOM Guided Setup. Make sure you have the right people in place before you start your implementation. The table below includes an overview of the resources you’ll need. For more detailed information on the roles, responsibilities, and skills, review the Event Management – Process Guide and ITOM – Product Skills Profiles.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event management administrator</td>
<td>This admin should have technical expertise and should have completed the ServiceNow System Administrator and Event Management training. They’re responsible for the general management of Event Management until the implementation is complete.</td>
</tr>
<tr>
<td>Monitoring source owner(s)</td>
<td>You need these subject matter experts to provide the access and potential configuration to support forwarding the appropriate events and alerts to ServiceNow. They’re responsible for the target event sources.</td>
</tr>
<tr>
<td>Security team member</td>
<td>Security team members are responsible for making decisions regarding the necessary credentials and permissions to allow Event Management to operate.</td>
</tr>
<tr>
<td>Incident process manager</td>
<td>This manager or team member is responsible for making decisions regarding the flow of information and actions from events to alerts and ultimately to incidents.</td>
</tr>
<tr>
<td>Other ITIL process manager(s)</td>
<td>These managers or team members are responsible for making decision regarding the flow of information and actions from events to alerts and ultimately to other tasks when events kick off activities outside of the incidents (a change, for example).</td>
</tr>
</tbody>
</table>

c) **Complete the necessary ServiceNow training.**
There are multiple systems and steps involved in implementing Event Management. Use the training ServiceNow offers to train your implementation and app management team members in the necessary terminology, functionality, and technical solutions. We recommend:
- Event Management Fundamentals (self-paced or instructor led)
- Flow Designer Fundamentals (Orlando)
Also, review the ITOM product training guidance for additional relevant training.
4. How do I use Guided Setup to configure and go live with Event Management?

a) Open Event Management in ITOM Guided Setup.
To open Event Management Guided Setup, navigate to Guided Setup > ITOM Guided Setup in your instance. Click Get Started, and then scroll down and click Get Started under Event Management. Read the ServiceNow product documentation for in-depth information on using Guided Setup.
b) Add an Event Management Connector.
Event Management includes many connectors and listeners with your subscription to pull or push events from external devices. Connectors and listeners are also available from the ServiceNow Store as well as from third parties. Follow these steps to add and configure at least one connector using ITOM Guided Setup. For more detailed instructions, please see the Event Management product documentation.

- **Navigate to Connector instances** – From the Event Management Guided Setup, select the **Connectors** tab under **Event Sources and Properties** and click **Configure**.

- **Configure a new Connector** – From the **Connector Instances** view, click **New** and populate the form with the **required information**, then click **Submit/Update**.

- **Test the connection** – From the connector instance, click **Test Connector**. This authenticates the connector through the MID Server to the monitoring source and grabs the most recent 10 events. These events will *not* be written to the event table—this happens only to test the connection.

- **Activate the connector** – After you’ve successfully tested the connection, click the **Active** checkbox.

**Practitioner insight**
The first time you run a connector, it can take some time as it will grab the most recent 3,000 events. Each subsequent pull will take much less time, using the date/time stamp and grabbing the deltas.
- Review this example to see a completed setup for Solarwinds

![Solarwinds Connector Instance](image)

- Host IP: 10.0.103.59
- Credential: solarwinds cred
- Event collection last runtime: -- None --
- Event collection schedule (seconds): 120

**Practitioner insight**

For some OOTB connectors, such as SolarWinds, you'll need to work with your monitoring source admin to get a read-only credential and IP address that lets the instance access SolarWinds.

**c) Configure the event rules**

**Event rules** generate alerts for tracking and remediation. They're stored in the Event Rule [em_match_rule] table, and you can configure and customize them to manage events and alert generation. Keep in mind that event rules don’t change the event records in the Event table. Changes to event data are stored in the ServiceNow instance memory.

- **Navigate to Event Rules** – From the Event Management Guided Setup, select the Event Rules tab under the Event Rules header and click **Configure**.
- **Create events rules for each event sources** – Follow the steps in the event rule product documentation to create or edit event rules for deduplication, format events, and set appropriate fields in alerts.
- **Implement an event binding strategy** – Set up your event rules to automatically bind alerts to configuration items. This makes tracking and remediation easier because it shows information about the CI that caused the event.
d) **Set up your alert management rules.**

Many organizations create tasks for alerts, such as incidents, manually or automatically through complex integrations that are difficult to manage. Alert management rules let you use alerts to trigger various actions within the platform. For example, one of the most common use cases is to create an Incident based on an alert.

Alert management rules check open alerts every time there is an update to the alert. Updates to closed alerts don’t cause alert management rules to run. You can create a filter so that the rule doesn’t act on every update of the alert, only when the condition that you set occurs.

- **Create a service matrix to map how you handle events today** – The service matrix captures the way actions from alerts can be raised and their priorities. Here is an example:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Create an Alert?</th>
<th>Create an Incident?</th>
<th>Associated CI?</th>
<th>Assign to CI Support Group + SME &amp; Product owners</th>
<th>Email Notification</th>
<th>Response SLA</th>
<th>Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Yes</td>
<td>Yes – Priority Critical</td>
<td>Required</td>
<td>CI Support Group &amp; Manager</td>
<td>1 Hour</td>
<td>Daily</td>
<td></td>
</tr>
<tr>
<td>Major</td>
<td>Yes</td>
<td>Yes – Priority High</td>
<td>Required</td>
<td>CI Support Group + SME</td>
<td>1 Day</td>
<td>Daily</td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td>Yes</td>
<td>Yes – Priority Moderate</td>
<td>Required</td>
<td>CI Support Group (NOC)</td>
<td>No</td>
<td>5 Days</td>
<td>Weekly</td>
</tr>
<tr>
<td>Warning</td>
<td>Yes</td>
<td>No</td>
<td>Required</td>
<td>No</td>
<td>No</td>
<td>None</td>
<td>Weekly Quantity of Alerts/CI</td>
</tr>
<tr>
<td>Info</td>
<td>No</td>
<td>No</td>
<td>Required</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Clear</td>
<td>No</td>
<td>No</td>
<td>Required</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

- **Identify the tasks to automate with alert management rules** – Work with your monitoring and ITSM admin to determine what tasks from your service matrix (incidents, changes, or service requests, for example) ServiceNow should automatically create for an alert that meets a specific condition.

- **Create your alert management rules** – From Event Management Guided Setup, select the Alert Management tab under the Knowledge, Tasks and Automation header and click Configure. Then, from the Alert Management Rules table, click New and populate the required fields. Refer to the product documentation for more detailed guidance.

By default, alert management rule actions include a number of remediation subflows with the base system. You can modify and create additional subflows, which requires the flow.designer role.
Concluding takeaway

ServiceNow’s Event Management provides intelligent event and alert analysis, business service health monitoring, and automated mitigation tasks to help you improve MTTR and reduce your number of incidents. With ITOM Guided Setup, you can quickly get started with Event Management, adding your first event source and setting up event and alert management rules to help you manage and act on events.

Once you have completed the steps to get started with Event Management, we recommend implementing Service Mapping. The Service Mapping application will help you get a better understanding of the business impact of an alert on an application service by providing a visual representation that shows the severity of each configuration item as it relates to the application service.

Additional resources

- Event Management product documentation
- Now Community

Additional resources are also available on our Customer Success Center.

If you have any questions on this topic or you would like to be a contributor to future ServiceNow best practice content, please contact us at best.practices@servicenow.com.
Customer Success Best Practices

ServiceNow's Best Practice Center of Excellence provides prescriptive, actionable advice to help you maximize the value of your ServiceNow investment.

Definitive guidance on a breadth of topics

- **Strategic**
  - Critical processes
  - Expert insights
  - Common pitfalls and challenges
- **Technical**
- **Tactical**

Created and vetted by experts

- Best practice insights from customers, partners, and ServiceNow teams
- Based on **thousands of successful implementations** across the globe
- Distilled through a **rigorous process** to enhance your success

Proven to help you transform with confidence

- Practical
- Actionable
- Value-added
- Expert-validated

Get started today.

Visit [Customer Success Center](#).

Contact your ServiceNow team for personalized assistance.