

IBM Resilient



Incident Response Platform

MASTER ADMINISTRATOR GUIDE v27

Licensed Materials – Property of IBM

© Copyright IBM Corp. 2010, 2017. All Rights Reserved.

US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Resilient Incident Response Platform Master Administrator Guide

Platform Version	Publication	Notes
27.1	February 2017	Addresses 27.1 features and changes; added the Designing a Playbook section.
27.0	December 2016	Minor change to Section 4.2 to clarify impact to new LDAP users.
27.0	December 2016	Initial publication

Table of Contents

1.	Introduction	5
1.1.	Dynamic Playbooks	5
1.2.	Modules	5
2.	Designing a Playbook	6
2.1.	Categorize Types of Incidents.....	6
2.2.	Determine Phases	7
2.3.	Determine Tasks and Instructions.....	7
2.4.	Determine Fields and Data Tables.....	8
2.5.	Determine Scripts	8
2.6.	Determine Rules	8
2.7.	Determine Layout.....	8
3.	Administrator Settings.....	9
3.1.	Users	9
3.1.1.	New User and Permissions	9
3.1.2.	Reassign Incidents and Tasks	10
3.1.3.	Deactivate or Delete Users	10
3.2.	Groups	11
3.3.	Timeframes	11
3.4.	Network.....	11
3.5.	Organization.....	12
3.5.1.	Details	12
3.5.2.	Settings	12
3.5.3.	Migrate Settings	13
3.6.	Threat Sources	14
3.7.	Notifications	14
3.8.	Artifacts.....	15
4.	Customization Settings.....	15
4.1.	Layouts	15
4.1.1.	New Incident Wizard	16
4.1.2.	Incident Tabs.....	17
4.1.3.	Close Incident	19
4.1.4.	Fields	20
4.1.5.	Views	20
4.1.6.	Data Tables.....	20
4.1.7.	Blocks	21
4.2.	Rules.....	22
4.2.1.	Conditions	23
4.2.2.	Activities	24

4.2.3.	Destinations	25
4.2.4.	Considerations for Creating a Rule	26
4.3.	Scripts	27
4.3.1.	Scope	27
4.3.2.	Writing Scripts	28
4.3.3.	Testing Scripts	30
4.4.	Message Destinations	31
4.5.	Phases & Tasks	32
4.5.1.	Phases	32
4.5.2.	Tasks	32
4.6.	Incident Types	33
4.7.	Breach	33
5.	Managing LDAP Authentication	34
5.1.	Before Enabling LDAP Authentication	34
5.2.	Enabling LDAP Authentication	35
5.3.	Managing LDAP Users in Groups	36
5.4.	Deleting LDAP Users	36

1. Introduction

Based on a knowledgebase of incident response best practices, industry standard frameworks, and regulatory requirements, the Resilient Incident Response Platform helps make incident response efficient and compliant.

This guide provides Resilient Incident Response Platform master administrators with an introduction to the system's administrative user interface and requirements. The document walks through a setup of a new organization and maintenance of organization-wide settings.

1.1. Dynamic Playbooks

With this release, IBM Resilient introduces the concept of dynamic playbooks. A *dynamic playbook* is the set of rules, conditions, business logic and tasks used to respond to an incident. The Resilient platform updates the response automatically as the incident progresses and is modified. Although the term, *playbook*, is not shown in the user interface, you create playbooks by configuring rules, conditions and activities, phases and tasks, message destinations, scripts and remote action processing programs (also called action processors).

The primary focal point for dynamic playbooks is the Rules tab under Customization Settings. From the Rules tab, you define the conditions that trigger the rule and the activities that are executed when the conditions are met. Activities include setting incident field values, inserting tasks into the task list, running internal scripts to implement business logic and placing items on message destinations to be acted upon by remote action processors. The remote action processors allow you to integrate the Resilient platform with existing security systems to create a single hub for incident response. The coordinated application of all of these features make dynamic playbooks a powerful tool for accelerating the execution of methodical incident responses processes and, ultimately, remediation of incidents.

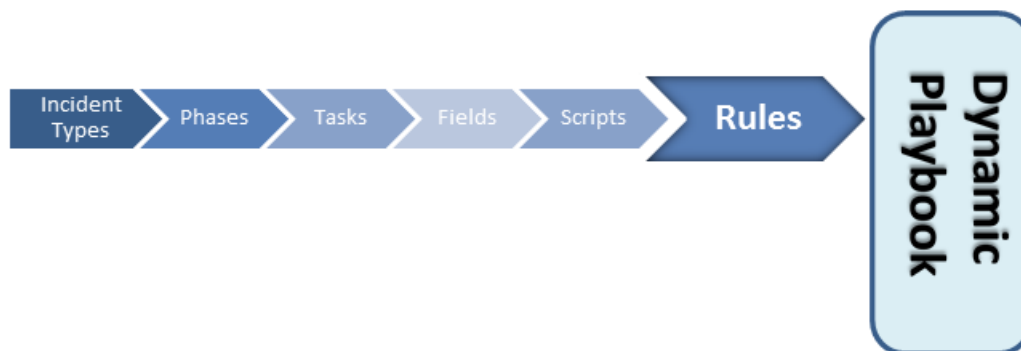
1.2. Modules

The following describes the modules that may be included with your Resilient platform, depending on the packaging purchased by your organization:

- **Action Module**, which provides the script and message destinations functions. If this module is not available for your organization, the Message Destinations and Script tabs are disabled, as well as the ability to configure a rule to post to a message destination or a run a script.
- **Security Module**, which enables the Resilient platform to search cyber threat sources which have been integrated into the product. If an artifact is added to an incident and is found in one or more of threat sources, it is highlighted in red and additional information is displayed.
- **Privacy Module**, which contains the privacy database and the breach notification rules. If this module is not available for your organization, then data breach compliance tasks are not generated in incident task lists regardless of indication of a data breach or breach data being recorded in the Breach tab.

2. Designing a Playbook

Creating a dynamic playbook involves a set of Incident Types, Phases, Tasks, Fields, Scripts and Rules to respond to an incident through intelligence, automation, and orchestration. IBM Resilient recommends the following object creation approach when designing a dynamic playbook.



You access these settings from the Customization Settings menu. The following sections provide a high-level overview of how to use each setting when designing a dynamic playbook.

2.1. Categorize Types of Incidents

To start, you need to classify the types of incidents you need for your environment then create the incident types in the Resilient platform. There are many methods for classifying incidents. The one you use will be dependent on:

- The current threats your organization faces
- What is required by policy
- What is relative in the current threat landscape

The incident types that you define should be relevant and meaningful to the full life cycle of the Incident Handling and Response actions, specifically, Pre, Intra and Post Incident.

Organizations typically follow pre-defined methods and standards when dealing with incidents, whether it be an emphasis on tools and automation, reporting and metrics, or information sharing. The following set of industry standards can help define your Incident Program:

- **NIST Special Publication 800-61R2** (August 2012) - [Computer Security Incident Handling Guide](#)
- **Verizon's VERIS Framework** – [Vocabulary for Event Recording and Incident Sharing](#)
- **Department of Defense CJCSM 6510.01B** (18DEC14) – [Cyber Incident Handling Program](#)

Once you define your incident types, you can create those types in the **Incident Types** tab under Customization Settings, or modify the existing types to fit your needs. You can also create incident type hierarchies. For example, there may be general activities your organization executes for any lost laptop but also some specific activities performed for a lost HR laptop differently than a lost Sales laptop, due to the nature of the data that is on the device. For details, see [Incident Types](#).

2.2. Determine Phases

Phases logically and visually separate tasks within a dynamic playbook. Like incident types, the phases you need for your environment is largely dependent on the organizations response approach and tracking methods.

Phases are used for two primary purposes:

- Capture the general intent of the response action, gathering supporting information during assessment.
- For leadership and management to be able to identify the current work state of the incident.

You define phases in the **Phases & Tasks** tab under Customization Settings. For details, see [Phases & Tasks](#).

2.3. Determine Tasks and Instructions

You can dynamically add tasks through the configurations of rules and their conditions and activities. You can add tasks to the incident task list based on the field values of the following objects: Incident, Tasks, Notes, Milestones, Artifacts, Attachments and Data Tables.

Tasks and their accompanying instructions are used as doctrine, policy, and/or as an advisory response procedure for an analyst. These tasks should be specific and repeatable to the incident or situation at hand.

Tasks also play a vital role as a system of record and as a method of training. Analysts new to your organization can quickly learn specific processes by following the dynamic playbooks presented within the Resilient platform.

You manage tasks in the **Phases & Tasks** tab under Customization Settings, where you also assign the task to a phase.

Check the following when creating or editing a task:

- Tasks are ordered when assigned to a phase. When you assign a task to a phase, check to make sure that it is in the proper order.
- Make sure that the task is enabled.
- If there is a SLA (Service Level Agreement) associated to that specific task, you can set the due date from the time the task is created on the incident.
- You can provide instructions to users from within a task. Be as detailed as possible, using rich text, references to internal and external resources, hyperlinks and embedded images when applicable.
- You have the option of creating custom **fields** and **data tables** within the task creation. You can place these **fields** and **data tables** onto a task for ease of entry and information reference.
- You can add a task to one or more rules. You can also add and create tasks when creating or editing a rule.

Once you assign a task to a rule, it shows the rule name(s) under the **Associated Rules** column.

For details, see [Phases & Tasks](#).

2.4. Determine Fields and Data Tables

You can use fields as data capture points for analysis review and to produce metrics. They specifically support incident response actions, reports, list incident views, and analytics dashboards. Fields should be distinct, specific and purposeful.

You create and manage fields and data tables in two locations - within the **Layouts** tab under Customization Settings where you can add them to the various incident tabs, and when creating or editing tasks.

Custom fields are available throughout the entire Resilient platform for assignment and for reporting purposes.

With data tables, you can capture and organize field values in a spreadsheet table format, using rows and columns each defined for their own respective field type.

Note: Data table values are not reflected in the List Incident views, and analytics dashboards.

For details, see [Fields](#) and [Data Tables](#).

2.5. Determine Scripts

You can use the Resilient scripts feature to implement business logic. They allow for additional functionality and flexibility outside of rules and are intended to handle complex conditions otherwise unsuitable or too intricate for simple rule conditions and activities.

You can write scripts to create and modify incident object types such as tasks, notes, milestones, and artifacts. Scripts inherit the attributes of the parent object.

You must be familiar with writing scripts using Python 2.7, and the scripts feature requires the Action Module.

You create and manage scripts within the **Scripts** tab under Customization Settings. For details, see [Scripts](#).

2.6. Determine Rules

Rules in the Resilient platform define an ordered and referenceable set of activities that are triggered when conditions are met. These activities include setting incident field values, adding tasks into the task list, running internal scripts to implement business logic, and placing items on message destinations to be acted upon by integrations.

There are two types of rules, Automatic and Menu Item. An automatic rule executes without user involvement when its conditions are satisfied. A menu item rule displays in the Resilient platform as an action in the designated object's Actions drop-down list and only executes when a user invokes it.

You manage rules within the **Rules** tab under Customization Settings. You can add conditions, order those conditions, add activities, provide the rule's results to an external program, and more as described in [Rules](#).

2.7. Determine Layout

With the ability to add fields to tasks, users can spend more time performing actions and capturing information directly in the tasks and less time switching between the incident tabs. Values of a specific field within the Resilient platform is viewable anywhere that same field is placed. IBM Resilient recommends that when possible, to add relevant fields to each task for easier data capture AND the incident tab(s) layout to allow and ease of review and reporting.

See [Layouts](#) for the procedure to modify layouts for incident tabs.

3. Administrator Settings

The most critical step in readying your organization to make use of the system is setting your organization's properties.

These settings allow you to tune the system to your specific preferences. To establish these settings, click on the drop-down arrow near your user name in the upper right corner of the screen, and click **Administrator Settings**. Once on the Administrator Settings page, several tabs are available to configure different aspects of the system.

NOTE: Many of the text fields allow you to add formatting options using industry-standard toolbars.

3.1. Users

The Users tab allows you to manage users, which includes creating new accounts, assigning groups, assigning permissions, reassigning incidents and tasks, deactivating, and deleting.

If LDAP is enabled for your organization, the users of authorized LDAP groups are listed and given the Default permission. For LDAP users, you can only reassign incident and tasks in the Users tab. You must use LDAP for the other tasks. See [Managing LDAP Authentication](#) for more information.

3.1.1. New User and Permissions

To set up a new user, click **Administrator Settings** then go to the Users tab and perform the following:

1. In the **Users** tab, click **Invite User**.
2. Enter the user's email address.
3. Add the user to one or more groups by selecting them from the drop-down. This feature allows you to build up incident response teams that can be assigned to incidents.
4. Select the appropriate permission:
 - **Default:** Users with default access are able to view, modify, reassign, and delete tasks (unless marked private) and attachments, and generate reports only for incidents of which they are a member. Default users may be given the ability to create new incidents, if appropriate. Default users can add and remove team members but only for the incidents that they own.
 - **Observer:** Observers are able to view all tasks, incidents, and attachments throughout the organization beyond those that they are assigned. Observers can add comments on tasks and incidents, and generate reports, and can be given the ability to create new incidents, if appropriate. Observers cannot update the details of an incident or modify, reassign, or delete tasks unless they are a member of the incident.
 - **Regular Administrator:** Regular Administrators have all the same permissions as default users, but are also able to view, modify, and reassign tasks and incidents across the entire organization. They are also able to generate reports for all incidents in the organization, run simulations, and add/remove incident team members. Regular Administrators do not need to be added to a particular incident in order to perform these functions. By default, Regular Administrators are able to create new incidents.
 - **Master Administrator:** Master Administrators have all the same permissions as Regular Administrators, but are also able to edit the organization's configuration settings, customize certain aspects of the system, and administer user accounts for the organization. Master Administrator is the highest level of access within the Resilient Incident Response Platform.

5. Choose whether the user can create incidents.
6. Click **Send Invitation**.

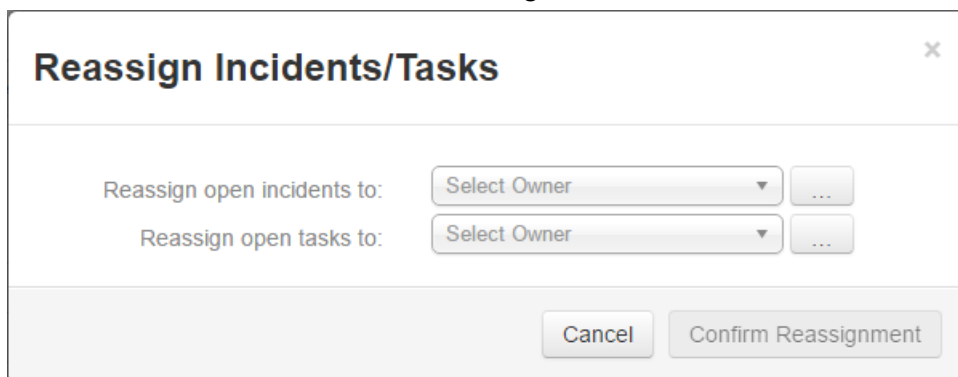
The user receives an email containing a link to log in and create a password. New users should go to **My Settings** from the drop-down menu near their name in the upper right hand corner and complete their contact information.

You can change the settings and permissions later by selecting the user in the list of usernames then clicking **Edit** in the User Details section.

3.1.2. Reassign Incidents and Tasks

You can reassign open incidents and incomplete tasks from active and deactivated users to another active user as follows. If using LDAP, you can also reassign a deleted LDAP user's open incidents and incomplete tasks.

1. Click on the drop-down arrow near your user name then click **Administrator Settings**.
2. In the **Users** tab, click the user's username.
3. In the User Details section, click the **Reassign Incidents/Tasks** button.



The dialog box titled "Reassign Incidents/Tasks" has a close button (X) in the top right corner. It contains two rows of controls. The first row is labeled "Reassign open incidents to:" and features a "Select Owner" dropdown menu followed by a three-dot menu button. The second row is labeled "Reassign open tasks to:" and also features a "Select Owner" dropdown menu followed by a three-dot menu button. At the bottom of the dialog, there are two buttons: "Cancel" and "Confirm Reassignment".

4. Choose to reassign all the user's incidents, tasks, or both by selecting a specific user or group to become the new owner. If the drop-down list is long, click the ... button to filter the user list.
5. Click **Confirm Reassignment** to implement your change.

3.1.3. Deactivate or Delete Users

Deactivating a user allows you to suspend the user's account temporarily, where you can reactivate the user at any time. Deleting a user removes the account permanently.

The following occurs when you deactivate a user:

- The user remains the owner of any incidents and tasks unless you reassign them.
- The user cannot be assigned new tasks or incidents.
- The user appears as deactivated in the Groups tab. An administrator can change group membership for deactivated users.
- Any saved incident filters containing the deactivated user are not affected.

The system does not send notifications to deactivated or deleted users.

To deactivate or delete a user, perform the following:

1. Click on the drop-down arrow near your user name then click **Administrator Settings**.
2. In the **Users** tab, select the user's username.

3. In the User Details section, click the **Deactivate User** drop-down then choose to deactivate or delete the user.
4. With either selection, choose to reassign any open tasks and incidents to another user. If the user is to be deactivated for a considerable amount of time, you should reassign the incidents and tasks.
5. Implement your change.

You can reactivate the user in the Users tab by selecting the username and choosing to reactivate.

3.2. Groups

It is often useful to have groups of users predefined so that they can easily be added to incidents together. For example, you may have different teams who are added to an incident based on the incident type, location or whether there is a privacy breach component to the incident. Groups can be created from the Groups tab.

To create a new group, click on the **Create Group** button. In the Create Group dialog, enter the group name and optionally add users to it by selecting them from the pull-down or typing their name and then clicking the **Add** button. When done, create the group by clicking on the **Create** button.

Optionally, you can configure the group to own incidents by checking the **Allow Incident Ownership** box. This allows you to assign an incident to a group, where every member of the group has the incident owner permissions. Should an administrator remove a member from the group, that user is no longer an incident owner. Adding a user to the group automatically makes the user an incident owner.

You can modify an existing group by selecting it in the list, making your modifications and saving. You can also add users to existing groups from the Users tab.

If you have LDAP enabled in the Organization tab, you can link a Resilient group to an LDAP group. See [Managing LDAP Authentication](#) for more information.

3.3. Timeframes

Although some regulations dictate specific timeframes for responses (e.g., 14 days), many are written in more general terms (e.g., as soon as possible). Timeframes are your organization's specific maximum turnaround times (in number of days) associated with these terms for the purpose of assigning due dates to tasks in your playbooks. Go to the **Timeframes** tab and click the **Edit** button to enable changes and then click **Save** when you have made the desired modifications. Although settings are suggested, it is strongly advised that you consult with internal or external counsel to establish appropriate timeframes for your organization. IBM Resilient does not provide legal advice. Dates can also be adjusted on a per-task basis within any playbook.

3.4. Network

The Network tab allows you to define an approved list of IP addresses that are allowed to connect to the Resilient platform for your organization. To specify specific IP addresses or ranges, click the **Add New IP** button and fill in the appropriate information. If you specify one or more IP address ranges, connections are only be possible from those locations. If you do not specify an IP address range then users can connect from any IP address.

3.5. Organization

The Organization tab provides the details for your organization and allows you to define various settings, such as attachment and, if enabled, LDAP and two factor authentication. If enabled, you can also export and import various fields and customized settings.

3.5.1. Details

The organization details for your organization are defined when IBM Resilient initializes your organization. To change this information contact IBM Resilient at support@resilientsystems.com.

3.5.2. Settings

In this tab, you can access the following settings:

- **Attachments:** The Resilient platform allows the master administrator to control whether users can upload attachments to the system. To allow files to be attached to incidents and tasks for your organization, switch the indicator to **On**. There is a limit to the amount of data that may be stored; please consult your specific agreement for details. If you find that you require additional storage, please contact IBM Resilient at sales@resilientsystems.com.
- **Default Tasks:** When tasks are created you can set them to be public or private by default, meaning that users (other than administrators) will need specific permission to view them. By setting this default to **On**, all tasks are created as public by default. Switch the indicator to Off if you prefer to have tasks default to private.
- **Incident Deletion:** If enabled, users with administrator permissions can delete incidents and simulations. Deleting an incident does not generate news feed or system notifications, although users can receive an email notification. When a user deletes an incident, the incident's attachments, such as tasks and artifacts, are deleted, and all mention of the incident is removed from the news feed and system notifications. The Resilient platform logs all deletions.
- **LDAP Authentication:** If available, you can enable LDAP authentication to allow LDAP users to authenticate with their LDAP credentials. See [Managing LDAP Authentication](#) for more information.
- **Two Factor Authentication:** If available, you can enable it to enhance your organization's security by adding a second layer of authentication to log in to the Resilient platform. You select an authentication domain (if there is more than one), and determine the Cookie Lifetime, which sets an expiration in days for when a user needs to re-authenticate via the two-factor authentication.

NOTE: If the LDAP Authentication or Two Factor Authentication settings are not available and you wish to have it enabled, contact support if you are a SaaS customer. For on-premises customers, you can enable it using the instructions in the *On-Premises Installation Guide*.

3.5.3. Migrate Settings

The Migrate Settings allows you to import and export settings from one organization to another. It also has a history of all import and export rules, along with a link to each import and export file. This feature is useful for backup and copying settings from one organization to another. For example, you can export your settings from a test environment when it passes the acceptance criteria then import them into the production environment.

To export settings, click **Export**. Incident types, fields and data table definitions are always included in the exported file.

NOTE: Optionally, you can choose to export custom phases and tasks, tab layouts, rules and scripts. Once you click the **Export** button, the settings are stored in JSON format to a **res** file.

Use the **Export History** to view all the exported files with a link to the file itself. The page lists the date and time of the export, user who performed the export, and a link to the file. The page also lists if rules, layouts, phases and tasks are included in the file.

You can import a previously exported file by selecting **Import** then clicking the **Import Settings** button and browsing to the file's location. Before importing, make sure that there are no other users currently logged in.

The platform performs the following during an import:

- Updates all incident fields, types and data table definitions.
- Since task names are not unique even within the same incident type, the platform attempts to match tasks via an internal unique id, and then attempts to match upon name and type. If there is one match only, the system overwrites the task; if there is more than one match, the system creates a new task and displays a warning.
- Checks the message destination and type (queue or topic). The system does not overwrite the message destination unless the name and type matches.
- Ignores the user list when importing message destinations. If importing a new message destination, the user list is empty. If importing an updated message destination, the system ignores the updated user list and keeps the original user list intact.
- Checks for rules that have a condition that refers to incident members; for example, a rule that is executed only when the incident member list contains a specific user. In this case, the platform retains the user if the imported condition contains an exact match of the user. If it is not an exact match, the platform displays a message after the import indicating that the user was removed from the condition.

Use the **Import History** to check the history after each import. Click **View** to list the changes between the existing settings and the imported settings, such as incident fields, layouts and custom rules. The import does not delete items; therefore, the View page provides a list of items that are no longer used, which you can then remove manually.

IMPORTANT: You can only export then import files from the same version of the Resilient platform. You cannot import files that were exported from a different platform version.

3.6. Threat Sources

When artifacts are added to incidents, the Resilient platform can optionally search for those artifacts in several cyber threat sources that have been integrated into the product. If the artifact is found in one or more of these threat sources, it is highlighted in red and additional information about the “hit” is displayed. You can enable and disable the threat sources as you see fit for your company. Threat sources are disabled by default. Note that a subscription to the Resilient Security Module is required to use this feature.

When enabling certain sources, you may be required to agree to the terms and conditions of the 3rd party threat source, or in some cases, optionally add your account information or API key.

You must enable the geolocation threat source if you wish to include geo-location data for the IP Address artifacts.

NOTE: You can also add your own custom threat service, as described in the *Resilient Incident Response Platform Custom Threat Service Guide*.

3.7. Notifications

You can notify specific users when a condition, such as a creation or deletion, occurs for an object. An object can be an incident, note, milestone, task, attachment, or artifact. The Notifications tab allows you to customize both email and in-product notifications, as well as create new notifications. Users can enable or disable notifications, or change the notification mechanism.

A user who invokes the condition does not receive the notification; for example, the user closing an incident does not receive the “Incident Closed” notification.

To customize an existing notification, simply click on it in the list of notifications. To create a new notification, click the New Notification button. Afterwards, perform the following to create or edit the notification:

1. Name your notification. Choose a name that is meaningful and descriptive to the end users when they are deciding whether to enable this notification or not.
2. Select the type of notification. The type relates to the types of objects in the system. Choices include Incident, Note, Milestone Task, Attachment, and Artifact.
3. Select the type of users (as they relate to the object) who should receive the notification. If you select Added Members or Added Owners, those members or owners who are in the process of being added to the object also receive the notification. If you select Removed Member or Owners, those members or owners who are in the process of being removed from the object also receive the notification.
4. Optionally, choose to notify one or more specific users. Click in the field for a list of user names.

A user name in red means that the user is currently deactivated and cannot receive notifications.

5. Choose a condition that causes the system to send the notification. Select only one of the following two options:
 - Send a notification if the object is created or removed.
 - Click **Add Condition**. Selecting a field, the operation to perform, and the value that causes the condition to be true. For example, you can send notifications whenever there is an incident with compromised data by setting the condition to **Data Compromised (field) is equal to (operation) Yes (value)**. You can add multiple conditions, where ALL conditions must be true to generate the notification.

6. If you wish to send an email notification, check the box and enter the text that is to be included in the message body. You can use the substitution variables `${TASK}` and `${INCIDENT}` to reference the task and incident.
7. If you wish to send a system notification, check the box and enter the text that is to be included in the message body. A system notification is an alert in the notification drop-down by the username symbolized with a red circle and a number. You can use the substitution variables `${TASK}` and `${INCIDENT}` to reference the task and incident involved.

3.8. Artifacts

Incidents are related when they share the same artifact. Users can see this relationship in the individual incident Artifacts tab and summary section.

Some artifact types may be included in a large number of incidents, but showing those relationships does not provide useful information to users. For example, you may not want artifacts of type "Email Subject" to relate incidents together because it is irrelevant to your process and not useful in resolving the incident.

The Artifacts tab in Administrator Settings allows you to reduce this type of non-useful information. Click No for those artifact types that can appear in multiple incidents but the relationship information is not useful.

The Artifacts tab sets the default behavior. There may be exceptions where a user needs to see which incidents contain a specific artifact type. There also may be exceptions where the user wants to see fewer relationships to reduce "clutter." Therefore, an incident owner can change the setting for an artifact type at the incident level.

4. Customization Settings

The Customization Settings page includes several tabs that allow you to customize various aspects of your playbook, such as adding your own rules and fields, customizing the incident phases, and modifying the layout and content of the various incident pages.

To access these settings, click on the drop-down arrow near your user name in the upper right corner of the screen, and click **Customization Settings**.

If your organization did not subscribe to the Resilient platform Action Module, the Message Destinations and Script tabs are disabled, as well as the ability to configure a rule to post to a message destination or a run a script.

4.1. Layouts

The Layouts tab allows you to determine the type of information shown for each incident. Specifically, you can control the information and layout in each of the tabs on the incident page, hide tabs, make tabs visible only when the incident meets one or more conditions, and create your own custom tabs. You can also customize the summary information shown in the left navigation pane of the incident page.

In addition, you can determine the type of information prompted by the new incident wizard, and the content of the dialog box that displays to the user when closing an incident.

4.1.1. New Incident Wizard

The New Incident Wizard is the set of steps that prompts a user for information creating a new incident. You can rearrange and modify the steps, add custom fields, and create steps.

The New Incident Wizard page shows each step as a block and in order. In the example below, steps 1, 2, and 3 are Describe the Incident, Date and Location, and Implications, respectively.

The screenshot displays the 'New Incident Wizard' configuration page. At the top, a navigation bar includes tabs for Layouts, Rules, Scripts, Message Destinations, Phases & Tasks, Incident Types, and Breach. The 'New Incident Wizard' tab is active, showing a sidebar with links to 'New Incident Wizard', 'Incident Tabs', and 'Close Incident'. The main workspace is titled 'New Wizard' and contains three steps, each with a list of fields or blocks:

- Describe the Incident:** Includes fields like 'Describe and Name the Incident', 'Incident Type', 'date field', 'bool field', 'NIST Attack Vectors', 'Field 3', 'Incident Disposition', 'Description', and 'Name'.
- Date and Location:** Includes fields like 'Date and Location', 'Date Occurred', 'Date Discovered', 'HTML Block', and 'Address'.
- Implications:** Includes fields like 'Implications', 'Criminal Status View', 'Employee Involvement View', 'Department', and 'Negative PR'.

On the right side, there are three panels: 'Fields' (with a search bar and a list of fields like 'Actual Date Closed', 'Actual Release Date', etc.), 'Views' (with a list of views like 'Address', 'Criminal Status View', etc.), and 'Blocks' (with a list of blocks like 'Header', 'HTML', 'Section'). Buttons for 'Add Step', 'Save', 'Add Field', and 'Add Block' are visible.

Use the up and down arrows in each step to reorder the steps.

Use the wrench icon to name the step and to set conditions. When you set a condition, the wizard displays that step only when the incident meets the condition. Using this feature, you can configure the wizard to show only some steps when certain conditions occur such as particular field values being selected in previous steps. However, the wizard always displays the first step regardless of any conditions.

You can add fields, views, and blocks to each step in the wizard, as described later in this section.

Use the Add Step button to create a new step, drag the appropriate fields, views, and blocks from the right-hand column into the step, click the wrench to name the step and set any conditions, then move the step to its correct position using the down arrow.

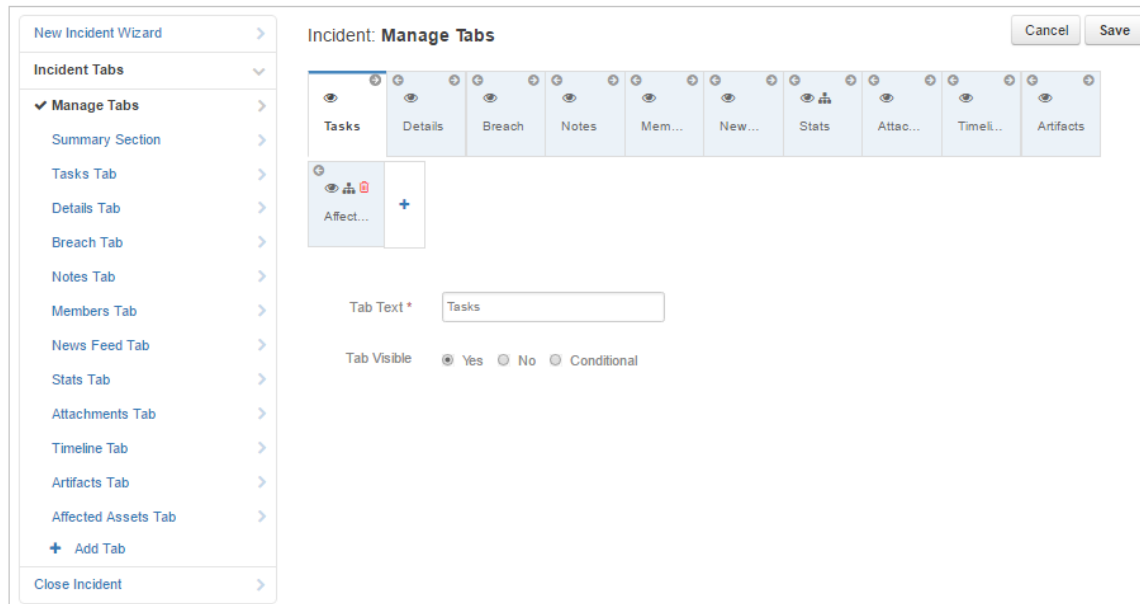
When done, click **Save** to implement your changes.

4.1.2. Incident Tabs

Each incident page has a number of tabs. You can modify the standard tabs, add your own custom tabs, and determine which tabs are visible. You can also set conditions that determine when to display a tab.

In addition, each incident page has a navigation pane on the left side of the page that provides additional information, which you can customize.

To view the list of tabs available for each incident page, click **Incident Tabs** then **Manage Tabs**. For example:



The following describes each component of Incident Tabs:

- **Manage Tabs**

This area allows you to determine which tabs are available to users when viewing incidents. You can add tabs as well as reorder, rename, make conditional, and hide tabs.

The icon in each tab represents its visibility. In the following example, all tabs are visible except Stats which is conditional, and News which is hidden, and Affect... which is a user-created tab and conditional.

Incident: **Manage Tabs** Cancel Save

Tab	Visibility Icon	Reorder Handle
Tasks	Eye	Arrows
Details	Eye	Arrows
Breach	Eye	Arrows
Notes	Eye	Arrows
Mem...	Eye	Arrows
News...	Eye with slash	Arrows
Stats	Eye with slash	Arrows
Attac...	Eye	Arrows
Timeli...	Eye	Arrows
Artifacts	Eye	Arrows

Affect... +

Tab Text *

Tab Visible ☒ Yes ☐ No ☐ Conditional

To set a condition on a tab, click the tab and select the **Conditional** button then select **Add Condition**. You can then select a field and determine the condition that allows the tab to be shown. You can have multiple conditions, where all conditions must be satisfied before the tab is shown.

To add a custom tab, click **Add Tab** in the navigation pane on the left or the plus icon at the right then enter a name and select its visibility. You can then add fields, views, data tables, and/or blocks to the incident. These items are described later in this section.

To delete a custom tab, click the delete icon, which is next to the visibility icon. In the previous example, **Affect...** is a custom tab. You can delete custom tabs only. You can rename or hide the default tabs, but not delete them.

To reorder the tabs, click and drag the tab or use the left and right arrows at the top of each tab.

NOTE: Data in tabs that are configured as not visible are not included in reports; however, data in tabs that may be hidden by a condition are always included in reports.

TIP: You can create a tab specifically to gather data for reports but never have it visible to users by creating a condition that can never occur then making that tab visible only when that condition is true.

- **Summary Section**

Each incident page has a summary section on the left side that contains useful information. This section displays on the page regardless of the tab selected.

You can customize the section by dragging the components from the column on the right into the areas on the left. To display groups of fields only under certain conditions, add a Section (under Blocks) to the layout then drag the corresponding fields into the section. You can then configure the conditions necessary for that section to be displayed by clicking the wrench in the top right corner of the section. When adding multiple conditions, note that the individual conditions are AND'ed together so that the section displays only when all of the individual conditions are met. Within a single condition involving a multi-select field, multiple selected values are considered to be OR'ed, where that specific condition is met if any of the values selected in the condition are selected in a specific incident.

To modify the order in which fields appear, drag and drop the various components to the desired order. You can modify or remove certain fields by using the "pencil" icon or the small "x" found near the field name. When finished, click **Save**.

You can add new fields, views, data tables, and blocks to the incident. These items are described later in this section.

To remove customization and return to the default view, click **Restore Defaults** at the bottom of the page.

- **Various tabs**

Click a tab name in the left navigation pane to display its content and format.

You can customize the tab by dragging the components from the column on the right into the areas on the left. To display groups of fields only under certain conditions, add a Section (under Blocks) to the layout then drag the corresponding fields into the section. You can then configure the conditions necessary for that section to display by clicking the wrench in the top right corner of the section. When adding multiple conditions, note that the individual conditions are AND'ed together so that the section displays only when all of the individual conditions are met. Within a single condition involving a multi-select field, multiple selected values are considered to be OR'ed, where that specific condition is met if any of the values selected in the condition are selected in a specific incident.

To modify the order in which fields appear, drag and drop the various components to the desired order. You can modify or remove certain fields by using the "pencil" icon or the small "x" found near the field name. When finished, click **Save**.

You can add new fields, views, data tables, and blocks to the incident. These items are described later in this section.

To remove customization and return to the default view, click **Restore Defaults** at the bottom of the page.

4.1.3. Close Incident

The Close Incident view determines if a dialog should be presented to the user when they close an incident. A dialog always displays when a user closes an incident that has required fields that have not been filled.

This section allows you to control the layout and to prompt the users for additional fields, which are not strictly required on close. You configure this section in the same fashion as the other incident tabs.

4.1.4. Fields

The Fields section lists all the possible fields available for the wizard or incidents. Most fields are self-explanatory, but here is a description of a few fields:

- **Source of Data:** In the recording of an incident, you can specify a custom source of data loss, such as a specific name of a database or business application. This information becomes useful when analyzing trends.
- **Exposure Source/Vendor:** In the recording of an incident, you can specify a custom name for a vendor or other third party to your organization that may be involved in a data exposure.
- **Department:** In the recording of an incident, you can specify a custom internal department name within your organization that may be involved in a data exposure.

You can edit each field to customize it to your own needs. To use a field in your incident, drag it to the desired location in the Incident column.

In addition, you can create new data fields for tracking, reporting, and documentation purposes. To create a custom field, click **Add Field** and enter the desired parameters. When adding a field, you can determine if it is required. If not required, mark it as **Optional**. Use **Always** to make it a required field when opening an incident. Use **On Close** to make it required when closing an incident. When a user creates a new incident, fields marked as Always show up with an asterisk in the UI indicating it is required. When a user closes an incident, the system prompts the user with a dialog displaying any fields that are marked On Close but have not yet been set.

When creating a field of the type Select, you can set a default value. When creating a field of the type Multiselect, you can set a default value; however, that is relevant only for the new incident wizard. When the field is used in other places, the default value is not shown.

4.1.5. Views

Views are pre-built modules that combine multiple fields and provide additional logic. Views are not editable. To use a view in your incident, drag the view to the desired location.

4.1.6. Data Tables

You can organize information in a tabular format, using rows and columns. Incident response users can then add information to this table.

To create a data table, click **Add Table** in the Data Tables section. When you choose to add a table, a wizard walks you through the following process:

- **Table Definition.** You add a label, which is a descriptive name for the table. The API Access Name is, by default, the same as the label with underscores instead of spaces.
- **Layout Table.** Determine the number of columns you need and enter a title for each column. If you add a column but do not enter a title, the column is not created. You can reorder the columns by dragging them as needed.
- **Configuring Column (N of X).** There is a page for each column. Choosing **Always** as a Requirement requires the user to fill in this column whenever the user adds a row.
- **Preview & Confirm.** Review the table. Optionally, you can resize the columns. The **Reset Column Widths** button resizes the columns so that they are approximately equal width. Use the Back button to make any changes or Save to save the table.

As an example, you can create a data table to list all users impacted by the incident. In this example, all the columns are of type text except for the column titled 'Fixed', which is of type boolean. The following screenshot is an example of a previewed table with sample data.

The screenshot shows a modal window titled "Editing Data Table" with a progress bar at the top indicating four steps: Table Definition, Layout Table, Configure Table Fields, and Preview & Confirm (the current step). Below the progress bar, the table is titled "Impacted Users" and includes a search bar. The table has five columns: User Name, User ID, Mgr Name, Organization, and Fixed?. The first row contains sample data: lorem ipsum, lorem ipsum, lorem ipsum, lorem ipsum, and Yes. Below the table, it says "Displaying 1 - 1 of 1". At the bottom left is a "Reset Column Widths" button, and at the bottom right are "Cancel", "Back", and "Save" buttons.

User Name	User ID	Mgr Name	Organization	Fixed?
lorem ipsum	lorem ipsum	lorem ipsum	lorem ipsum	Yes

The following is an example of a table where a user edited an incident and added a row.

The screenshot shows the "Impacted Users" table interface. It includes a search bar and a "+ Row" button. The table has five columns: User Name, User ID, Mgr Name, Organization, and Fixed?. The first row contains input fields with the values: SmithJ, 654321, JonesR, Sales, and Unknown. Below the table, it says "There is no data for this table". At the bottom, it says "Showing 0 to 0 of 0 entries".

User Name	User ID	Mgr Name	Organization	Fixed?
SmithJ	654321	JonesR	Sales	Unknown

4.1.7. Blocks

Blocks are special components that you can use to further design your incident. To use these blocks, drag the block to the desired location column then edit it.

There are three types:

- **HTML.** Allow you to custom HTML code.
- **Header.** Allows you to add header text in the incident.
- **Section.** Allows you to organize fields. Drag it to the Incident column then drag the desired fields into the section. Optionally, you can edit the section to make it visible only upon a specific condition.

4.2. Rules

A *rule* is a set of conditional statements that, when satisfied, run pre-defined activities.

An *activity* is the function that the rule executes when the appropriate conditions are satisfied. Activities include setting values in various fields and adding tasks in an incident. If your organization has the Action Module, you can also create script activities and integrate with other systems by posting messages to message destinations.

There are two types of rules, automatic and menu item. An automatic rule executes without user involvement when its conditions are satisfied. A menu item rule displays as an action in the object's **Actions** drop-down menu and executes only when a user invokes it.

The Rules tab allows you to view, edit, and create rules. The tab provides the following information:

- **Order.** Automatic rules have numbers, which denotes the order the rules run when a condition invokes multiple rules. The ordering can be important especially when different rules affect the same fields, or changes made by one rule impact another rule. You can change the order by dragging the rules. Menu Item rules do not have numbers since they run only when a user invokes them.
- **Name.** Click the name of a rule to view its details or edit the rule. When editing or creating a rule, you should enter a name that is descriptive of the rule's purpose.
- **Process Type.** Automatic and Menu Item.
- **Object Type.** You assign a rule to one type of object, such as incident, note, milestone, task, attachment, artifact or data table.
- **Conditions.** A condition is a statement that checks a field for a value using an operator, such as *equal to*. Conditions are used to determine when to invoke the rule. The Rules tab lists the conditions, if any, attached to the rule.

NOTE: A condition in red indicates an invalid condition. The reason could be that a selected object or field is disabled or hidden.

A rule is evaluated when there is a change to an instance of an object, which is of the type specified in the rule's object type. Therefore, a rule is evaluated every time an object of the associated type is created or updated. When a rule is evaluated, its conditions are checked, and if satisfied, the rule is invoked.

Rules are re-evaluated and can be invoked again when a rule creates a new object or changes the state of an object. To guard against infinite loops, the Resilient platform limits the rule creation of new objects to 500 while processing rules.

TIP: If you see a message stating that the number of rule evaluations in a single session has been exceeded, make sure that the rule has not inadvertently created an infinite loop.

4.2.1. Conditions

When creating or editing a rule, you define the conditions that invoke the rule. If you do not specify any conditions, then the rule is invoked every time an object of the associated type is created or updated.

When creating a new rule, you must first select the rule's object type before you can specify any conditions. Click the **Add New** link to start adding conditions. The object type determines which fields are available as conditions. The following example shows a new rule with an object type of incident and the Address field.

Create Menu Item Rule

Display Name *

Object Type Incident

Conditions Add custom conditions for when Menu Item will display. [Clear All](#)

Address is equal to

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include *Add Tasks and Set Field*. [Add New](#)

Cancel Create

Click in the first box to select a field. Click in the second box to select the equation. Click in the last box to select or enter a value. The rule is invoked when this condition becomes a true statement (unless there are other conditions).

Click the plus icon (+) to add conditions.

Some object types allow you to select fields from their parent object; for example, you can select incident fields for a rule that has a task or notes object type.

NOTE: The rule is evaluated only when there are changes to an instance of object type selected in the rule. The conditions selected, whether from the object type or parent object type, do not affect when the systems evaluates the rule.

If a rule has multiple conditions, you can determine how the conditions are to be satisfied before invoking the rule as follows:

- Select **All** to invoke the rule only when all individual conditions evaluate to true (they are AND'ed together).
- Select **Any** to invoke the rule when any one of the conditions is true (results are OR'ed).
- Select **Advanced** to define your own logical statement using the AND, OR, and NOT operators. You can also use their respective symbols, &&, || and !. For example, 1 OR (2 AND 3) means that condition 1 set to true invokes the rule, and conditions 2 and 3 both set to true invoke the rule. To avoid unexpected results, make sure to use parentheses when using complex expressions.

4.2.2. Activities

An activity is invoked when the rule conditions are satisfied. You can view a rule's activities by editing the rule. The activities are listed under the Activities Heading.

If creating a rule, there are no activities. Click the **Add New** link under the Activities heading. This brings up a default Set Field activity. You can change the activity type by clicking the **Set Field** button and choosing the activity type from the drop-down menu. For example:

Create Menu Item Rule

Display Name *

Object Type Incident

Conditions Add custom conditions for when Menu Item will display. [Add New](#)

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include *Add Tasks*, *Run Script*, and *Set Field*. [Clear All](#)

▲ ▼ 1 Set Field Incident: BankNumber + 🗑️

Destinations Set Field is posted to Message Destinations after all Ordered Activities complete.

Select Destinations [Show Activity Fields](#)

Cancel Create

You can add an activity by clicking the plus (+) icon. You delete an activity by clicking the trash can icon.

There are three types of activities:

- **Add Tasks.** Select the tasks you wish to have the rule invoke. Select **Add Tasks** then click in the field to list the tasks, which are listed by incident phase and in order of priority. You can choose one or more tasks. Optionally, you can create a new task. See the procedure in [Phases & Tasks](#) for details.

NOTE: If editing a rule, any task shown in red denotes that the task has been deleted.

- **Run Script** (requires the Action Module). Executes a script. Select **Run Script** then click in the field to list the scripts.
- **Set Field.** You can select one of the object's fields and set a value. Some object types allow you to specify fields from their parent object; for example, task rules can set incident fields. You can clear a field by setting it to no value.

When a rule has multiple activities, the rule executes each activity serially. You can determine the order.

4.2.3. Destinations

As described in [Message Destinations](#), a rule can send information in a message to a *message destination*, which is the location where the message is stored and made accessible to external scripts and programs. You would only specify a destination to provide information to such a script or program. You can select one or more message destinations.

For menu item rules only, you can also configure activity fields, which allow you to create a dialog box to collect information from the user, where this information is also sent to the message destination. The user sees the dialog box after selecting the action from the Actions menu. For example, you may require the user to select a ticket queue and specify a priority when generating an IT ticket from a task note.

To create a dialog box, click the **Show Activity Fields** link when creating or editing a menu item rule. You can drag and drop fields as well as insert headers and html markup on the layout panel to organize the dialog box. In addition, you can create new fields by clicking **Add Field** then configuring the following values:

- **Type of Field:** Select the type of the field that best matches its purpose.
When creating a field of the type Select, you can set a default value. When creating a field of the type Multiselect, you can set a default value; however, that is relevant only for the new incident wizard. When the field is used in other places, the default value is not shown.
- **Label for the Field:** Enter the display name for the field.
- **API Access Name:** The platform automatically generates the API access name, based on the display name. NOTE: Software developers use the name to interact with this field from the API.
- **Placeholder:** If you enter a placeholder, this value is automatically displayed in the field to provide a hint to the user.
- **Requirement:** Enter **Always** to make it a required field, where the user cannot execute the rule (as an action) without specifying a value for the field. Select **On Close** to make it required when closing an incident. Select **Optional** if the user is not required to enter or select a value.
- **Tooltip:** Optionally enter descriptive text or a helpful hint. This displays an information icon next to the field. Your text displays when a user hovers over the icon.

4.2.4. Considerations for Creating a Rule

Consider the following before writing a rule:

- Determine the object type and the purpose of the rule.
- Determine the activities. If there are multiple activities, determine the order of those activities.
- Determine if the rule is to be invoked automatically or by a user from a menu item.
- Determine the conditions, if any, which must be satisfied before invoking the rule. If there are multiple conditions, determine whether any one or all conditions must be satisfied.
- Determine the order of the automatic rules. When invoking multiple rules, they are invoked in the assigned order.
- If you wish to communicate information to other processes, make sure to choose one or more destinations. This function requires the Action Module.
- If you wish to run a script, make sure to choose or create the appropriate script. You create scripts in the **Scripts** tab. This function requires the Action Module.

IMPORTANT: When developing and testing your rules, we recommend that you include a condition that prevents the activities from inadvertently being invoked against production data until you are sure they are ready. One simple way to do so would be to include an additional clause in the rule conditions such as "Simulation Equals True" or the equivalent. In this way, the rule would only invoke activities against simulations and not open incidents.

4.3. Scripts

You can write and edit scripts that allow you to customize incidents and retrieve information on incidents and other object types. You can then invoke a script from a rule.

You must be familiar with writing scripts using Python 2.7, and the scripts feature requires the Action Module.

The Scripts tab allows you to view, edit, and create scripts. The tab provides the following information:

- **Name.** Click on the name of a script to view its details or edit the script. When editing or creating a script, you should enter a name that is descriptive of the script's purpose.
- **Description.** Text to describe the script.
- **Object Type.** You assign a script to one type of object, such as incident, note, milestone, task, attachment, artifact or data table. The object type determines the context of the data that is provided to the script.
- **Rules.** A list of rules that call the script.
- **Trash can icon.** Click to delete the script. If a script is referenced in a rule, you must remove it from the rule before you can delete it.

4.3.1. Scope

The scripts in the Script tab are not the same as action processors. Scripts can modify incident data, and add tasks, notes, milestones, artifacts, etc. Action processors can implement custom business logic and interact with external systems, as described in the *Resilient Action Module Programmers Guide*.

The scripting feature supports Python 2.7 only, and has the following language feature and security limitations in place to prevent unwanted actions:

- You can import only the `java.util.Date` Java language class. You cannot import python libraries, including `os`, `subprocess`, `sys`, and `threading`.
- Network access is not allowed in order to prevent unwanted or unauthorized access to the network.
- Access to the underlying filesystem is not allowed to prevent unwanted or unauthorized access to the filesystem.

4.3.2. Writing Scripts

You can access the following Resilient objects when writing a script. These objects reflect the action object data and some contain helper methods. In the script context, all SELECT/MULTISELECT field values are referred to by names. TEXTAREA fields are referred to by the objects handle format.

To write a script, go to the Scripts tab and perform the following:

1. Click the **New Script** button.
2. Enter a descriptive name for the script.
3. Provide a description of the script's purpose.
4. Select an object type:
 - Incident
 - Task
 - Note
 - Milestone
 - Artifact
 - Attachment
 - Data Table, then select the specific table.
5. Write the script utilizing the object type context provided to the script. The following table describes the object type contexts and the operations that can be utilized when those contexts are selected.

Object	Description	Operations
incident	Available in every script. It contains the incident data and additional helper methods. The incident data contains only incident field data; it does not contain its notes, task, milestones, artifacts, or attachments.	<pre>addTask(name, phase_id, instr_text)</pre> Add an adhoc task to the incident with the given name, phase, and instructions. Returns a Task script object for further customization. <pre>addMilestone(title, description, date)</pre> Add a milestone to the incident with the given title, description, and instructions. Returns a Milestone script object for further customization. <pre>addArtifact(type, value, description)</pre> Add an artifact to the incident with the given type, value, and description. Returns an Artifact script object for further customization. <pre>addRow(name)</pre> Add a row to the named Data Table on the incident. Returns a Row script object for further customization. <pre>addNote(text)</pre> Add a note to the incident with the given text. Returns a Note script object for further customization.

Object	Description	Operations
task	Available for Task scripts and may be present for Note/Attachment scripts if the note/attachment is a task note/attachment. It contains the task data and additional helper methods. The task data contains only task field data; it does not contain its notes or attachments.	<code>addNote (text)</code> Add a note to the task with the given text. Returns a Note script object for further customization. <code>getParentObject ()</code> Return the Incident script object that owns this task.
note	Available for Note scripts. It contains the note data and additional helper methods. The task object may be available for Note scripts that are invoked by a task note rule.	<code>addNote (text)</code> Add a reply to the note with the given text. Returns a Note object for further customization. <code>getParentObject ()</code> Return the Incident/Task script object that owns this note.
milestone	Available for Milestone scripts. It contains the milestone data and additional helper methods.	<code>getParentObject ()</code> Return the Incident script object that owns this milestone.
artifact	Available for Artifact scripts. It contains the artifact data and additional helper methods.	<code>getParentObject ()</code> Return the Incident script object that owns this artifact.
attachment	Available for Attachment scripts. It contains the attachment data and additional helper methods. The task object may be available for Attachment scripts that are invoked by a task attachment rule. The attachment data contains only attachment fields and metadata; it does not contain the attachment content.	<code>getParentObject ()</code> Return the Incident/Task script object that owns this attachment.
row	Available for Data Table scripts. It contains the row data and additional helper methods.	<code>getParentObject ()</code> Return the Incident script object that owns this row.
log	Available for all scripts. It contains the following helper methods for returning messages to display in the action status.	<code>info (message)</code> Add an action status message at the INFO level. <code>warn (message)</code> Add an action status message at the WARN level. <code>error (message)</code> Add an action status message at the ERROR level. <code>debug (message)</code> Add a message at the DEBUG level. Only returned when the script is being debugged. These messages are not persisted as action status messages.

Object	Description	Operations
helper	Available for all scripts. It contains additional utility helper methods for scripts.	<pre>createRichText(text)</pre> Create a rich text object that can be used for fields that support a rich text format. This is used to set TEXTAREA field values permitting rich text. <pre>createPlainText(text)</pre> Create a plain text object that can be used for fields that support a rich text format. This is used to set TEXTAREA field values that may or may not permit rich text. <pre>fail(message)</pre> This method has the ability to fail the execution of a script for custom business validation and return a message. The whole transaction is canceled and changes are not saved.

NOTE: You can use HTML tags to enter rich text for fields; however, you cannot use HTML tags with script tags. If you do, the HTML tags are stripped and the script may return invalid data.

4.3.3. Testing Scripts

Once you have written a script, you can test your script against an existing object. For example, if the script's object type is Milestone, you run the script against a milestone within an incident.

IMPORTANT: To run a script, you must enter a valid incident ID. A script can and will cause changes to the data. When testing your script and you are not in a development environment, you should use a simulated incident ID to run your script against simulations and not open incidents.

To test your script:

1. Click the **Run** button.
2. Enter a valid incident ID. You can find the ID by going to the incident page and looking at the Summary section.
3. Select an object within the incident. Only those objects of the type assigned to the script are shown.
4. Click **Finish**.

The script runs and a console window displays with the results. It is slightly transparent so that underlying content can be slightly visible.

If you want to view information at specific points in the script, make sure to include in the script the log info method described in the previous table. For example:

```
log.info("The value of x is {}".format(x))
```

Log messages are the last set of information reported after each run. You can filter the log messages by changing the Log Level choice in the Console Window header area.

Because the system is designed to execute concise scripts, "stepping-through" the code is not available.

If you make changes and wish to rerun the script using the same incident and object, click **Run Again**. You do not need to save the script to run the script again.

NOTE: It is important to test your scripts fully to verify that the results are as expected. The Resilient platform cannot fully verify script logic.

4.4. Message Destinations

When a rule's conditions are satisfied, it can optionally send a message to a *message destination*, which is the location where the message is stored and made accessible to external scripts. The message includes details about the object and the activity taken. The external script processes the information as desired. You can configure rules to send messages to one or more message destinations.

The Message Destinations tab allows you to view, edit, add and delete message destinations. To add a new destination, click the **Add Message Destination** button. To view, edit or delete a destination, click on the destination name in the table.

Each destination has the following properties:

- **Type:** The type determines what happens when a rule sends a message to the destination. You can choose the type only when creating a message destination. You cannot change the type for an existing destination.
 - **Queue:** If there are multiple scripts, only the first script to request it receives the message. When there is no script, the message stays on the message destination.
 - **Topic:** If there are multiple scripts, all of the scripts retrieve a copy of the message. When there is no script, the message is discarded.
- **Name:** Name of the destination. When adding or editing, use a name that describes the purpose of the message destination.
- **Programmatic Name:** Generated by the system and based on the Name field. Script developers use this programmatic name when creating external scripts that connect to the destination. It is displayed for informational purposes.
- **Expect Acknowledgement:** When set to Yes, the destination expects the script to return an acknowledgement when it has completed processing the message. Set the field to No if you do not require an acknowledgement or you expect the scripts to silently process messages without returning any indication of progress or status.

If expecting an acknowledgement, the Action Status for the action is listed as Pending until the acknowledgement is received. If an acknowledgement is not received within a day, the status for the action changes to Timed Out.

- **Users:** External scripts that connect to a message destination must authenticate using a Resilient account. Specify one or more accounts authorized to connect to this message destination. You should create specific Resilient accounts for this purpose instead of using Resilient user accounts.

4.5. Phases & Tasks

The Resilient platform defines distinct stages, called *phases*, for all incidents, which is useful for tracking progress. Each phase contains a number of tasks to perform before going to the next phase. This tab allows you to define and order the phases, as well as the tasks in each phase.

4.5.1. Phases

The phases are listed in the order of execution. The tasks within a phase are also listed in the order of execution.

You can manage phases as follows:

- To create a new phase, click the **Add Phase** button, specify a name, and save your changes.
- You can edit the name of the phase by clicking the “pencil” icon next to the phase.
- To delete phase, first remove its tasks then click the “x” icon.
- You can reorder phases by clicking and dragging the  icon next to the phase. You cannot move the first phase.
- You can also reorder the tasks within a phase by dragging them. You cannot drag a task from one phase to another.
- Use the filters, such as Rules, Phase, and Name, at the top of the list of phases to show different views. Use the **More** button to select additional filters. You can deactivate a filter by clicking the **x** icon. **Hint:** To better visualize your playbook, select a rule in the Rules filter to show the tasks that are associated with the rule.

To save your changes to the reordered tasks or phases, click the **Save Order** button.

4.5.2. Tasks

You can click the pencil icon in a task row to edit a task or click **Create Task** to create a new task. In either case, you can manage the following properties:

- Task Name. Any text you choose. It should be descriptive.
- Phase. Select the phase where the task is to appear.
- Rules Using this Task: Lists the rules that invoke this task. It is the same set of rules that appears for the task in the Associated Rules column of the main Phases & Tasks tab. If you wish to add this task to additional rules, click in the field to list the available rules then select the desired rules. This action is the equivalent of using the Add Tasks activity field when creating or editing a rule. To remove the task from a rule, click the **x** icon by the rule name.
- Required. Select Mandatory if the task must be performed before the incident can enter the next phase. Otherwise, select Optional.
- Enabled. If Disabled, the task does not appear in all future incidents.
- Due Date. To impose a deadline, select Yes then determine the number of days, hours or minutes that the user must perform the task.
- Instructions. Provide any instructions that would be helpful to the user performing the task. You can insert links and images. The instructions appear when a user hovers over the task name in the Tasks tab of an incident.

- **Incident Fields.** You can add fields and data tables for the users to enter information. Drag the fields and data tables to the layout section. This function is the same as described in [Fields](#) and [Data Tables](#).

To delete a task, click the pencil icon in a task row then click **Delete**.

When you edit a task, the changes apply only to future instances of the task; it does not apply to existing incidents.

4.6. Incident Types

The Resilient platform organizes incidents by types. Rules are assigned to incident types so only those rules germane to the incident are available.

Click **Add Type** to create custom incident types. You can also customize the details of an existing incident type. When creating/editing incident types, you can create incident type hierarchies. For example, there may be general activities your organization executes for any lost laptop but also some specific activities performed for a lost HR laptop differently than a lost Sales laptop, due to the nature of the data that is on the device. To provide this distinction, click **Add Type** and assign a name such as “Lost HR Laptop”, and select “Lost Laptop/PC” as the parent. These incident types can be used to control the inclusion of rules in playbooks. By building up hierarchies of incident types and associating them with rules, you can create very precise playbooks to meet your specific needs.

If you choose to make the incident type hidden, it is not available for selection when entering a new incident. Only the more detailed option appears in the drop-down menu. This prevents users from choosing the broader category and forces them to choose the more detailed option.

4.7. Breach

This tab contains the privacy breach-related configuration settings and customizable features for your organization. It is essential that the configuration settings be completed so that the Resilient platform is an effective tool to help your organization respond properly to a data breach.

NOTE: If your organization subscribes only to the Security Module, you can still configure breach settings but breach-related tasks are not generated within a playbook.

- **Regulators:** Specify which regulators govern your organization. By selecting the appropriate regulators, the system can generate the appropriate regulatory required tasks in the case of a data breach. In addition, this is where you select which best practices should be applied when generating playbooks.

Click the **Edit** button to enable changes, and then select one or more industries that apply to your organization. Depending on the industry selected, the system highlights regulators that are typically involved in regulating your industry, in addition to potentially influencing liability estimates and recommended tasks. Check off the regulators you wish to enable; you are not required to adhere to highlighted options. Once you have made your selections from each list, click **Save**.

Regarding EMEA, AsiaPac, and Latin America: Only those countries in which the corporate establishment or data processing is material to a particular incident should be selected. This may also be done at the time the incident is being created. Refer to each country's tool tip for additional detail.

Incident owners have the option to adjust which regulators apply to a particular incident during incident creation. Doing so does not change the default regulators selected by the master administrator.

You can also select Data Breach Best Practices on the Regulators page if desired. These are suggested non-regulatory activities for responding to breaches of PII.

If your organization is an Experian customer, you may select that option under **Resilient Partners**. This generates Experian-related tasks in appropriate playbooks.

- **Data Types:** Choose the data types that the company generally captures and/or stores. All fields are available during the recording of an incident but the fields selected here are highlighted. Click the **Edit** button to enable changes and then click **Save** when you have made the desired selections.
- **Jurisdictions:** Select all jurisdictions for which your organization has records. For example, you should select California even if your organization does not have an office in California, but stores information related to residents of that state. The selected states appear in a list for each incident, and the user selects the states for which information was lost during the specific incident. Click the **Edit** button to enable changes and then click **Save** when you have made the desired selections. Jurisdictions not indicated here can be added during incident creation if necessary.

5. Managing LDAP Authentication

The LDAP authentication feature is available only for on-premises configuration.

You can use the LDAP authentication feature to grant members of an LDAP group access to the Resilient platform, and control the membership from your Active Directory.

The Resilient platform supports Active Directory only; therefore, you must have an Active Directory Server. Refer to the *Resilient Incident Response Platform On-Premises Installation Guide* for the procedure to configure the Resilient platform for LDAP authentication. Once configured, a master administrator can enable LDAP authentication for the organization.

5.1. Before Enabling LDAP Authentication

Once LDAP authentication is enabled, you can view all the LDAP groups from within the Resilient platform. However, the Resilient platform allows you to authorize only one LDAP group, where the members of that group have access to your Resilient organization and can be assigned incidents and tasks, and added to Resilient groups. Therefore, you should request that the Active Directory manager create an LDAP group containing all the members who require access to the Resilient platform; for example, an Incident Response group.

When creating a Resilient group, you can link the group to any LDAP group. The result is that any members of that LDAP group who are also members in the authorized group are added to the Resilient group. Any membership changes in the LDAP group are reflected automatically in the Resilient group.

This feature allow you the flexibility to create numerous groups for specific tasks or duties. For example, you could request that the Active Directory manager also create a Security Breach LDAP group, where you can select those members to be in a Resilient group that is responsible for security breach incidents.

The LDAP authentication feature does not exclude the invite user feature in the Users tab. Therefore, you can create groups that have a mix of LDAP users and invited users.

NOTE: A single user can be both an invited and a member of the authorized LDAP group. If the user has the same email address in both places, that user can only use the LDAP credentials to log in to the Resilient platform.

The following icons represent the invited users and the LDAP users:

: Invited user

: LDAP user

5.2. Enabling LDAP Authentication

Perform the following to enable and configure LDAP authentication for your Resilient organization.

1. Click the **Organization** tab.
2. Click the button to On next to **Enable LDAP Authentication**. Once enabled, you see a list of LDAP groups.

If the Enable LDAP Authentication field is not present, the platform is not configured for LDAP authentication. See the *Resilient Incident Response Platform On-Premises Installation Guide*.

3. Locate the LDAP group to authorize. This group should contain all the members that require access to the Resilient platform.
4. Click the **Authorize Group** link.

The screenshot shows the 'Administrator Settings' page with the 'Organization' tab selected. On the left, there are navigation links for 'General' (Details, Settings) and 'Migrate Settings' (Import, Import History, Export, Export History). The main content area is titled 'Organization Settings' and contains several sections: 'Attachments' (toggle ON, size 6 KB), 'Default Tasks' (toggle OFF), 'Incident Deletion' (toggle OFF), and 'Enable LDAP Authentication' (toggle ON). Below the 'Enable LDAP Authentication' section, there is a search bar with the text 'Incident response team' and a 'Search' button. A table below the search bar lists the 'Incident Response Team' group with an 'Authorize Group' link in the 'Actions' column.

All new LDAP users in the authorized group can access the Resilient platform using their LDAP credentials, and are granted the Default permission. You can change the permission in the Users tab.

Typically, LDAP users must first log in to the Resilient platform before they appear in the Users tab. The users may also appear in the Users tab if they are assigned to a notification condition or message destination.

IMPORTANT: Deauthorizing an LDAP group deauthorizes all LDAP users so that they cannot access the system or receive notifications. If an LDAP user is the owner of an incident, you are prompted to reassign the incident the next time you save it.

5.3. Managing LDAP Users in Groups

You can link a Resilient group to an LDAP group. This action adds authorized members of the LDAP group to the Resilient group; however, the LDAP group membership is controlled by the Active Directory manager. Any changes to the LDAP group membership are reflected in the Resilient group membership.

The following shows an example of creating a group linked to an Incident Response Team LDAP group.

Create Group

Group

Name * IR Team

☐ Allow Incident Ownership ⓘ

Link LDAP Group ⓘ

Linked Group
Incident Response Team

[Change](#) [Remove](#)

Members

Select Members

Name	Actions
Charles Davis	
Deborah Parker	
Paul Jones	
Robert Perez	
Sharon Campbell	

[Cancel](#) [Create](#)

If a linked LDAP group contains authorized and unauthorized members, only the authorized members are shown and added to the Resilient group. To be an authorized member, the member must belong to the LDAP group that is authorized in the Organization tab.

Should you edit a Resilient group that is linked to an LDAP group, you can remove the users that you explicitly added but you cannot remove those LDAP users who are part of the linked group. Instead, you must unlink the LDAP group.

NOTE: Make sure that all authorized members of a linked group log in to the Resilient platform before associating the group to any incidents. Members of a linked group who have not logged in cannot receive email notifications.

5.4. Deleting LDAP Users

You cannot delete an LDAP user directly. If you attempt to delete an LDAP user, a warning displays.

To remove an LDAP user, that user must first be removed from the Active Directory. After which, unlink the user using the **resutil resetuser** command and then delete the user from the platform. For details on the resetuser command, type the following:

```
$ sudo resutil resetuser -help
```

END OF DOCUMENT