



Resilient Incident Response Platform

MASTER ADMINISTRATOR GUIDE v26

© 2016 Resilient Systems, Inc. All rights reserved.

This guide and the software described in this guide are furnished under a license accompanying the software and may be used only in accordance with the terms of such license. By using this guide, you agree to the terms and conditions of that license.

Resilient and Resilient Systems are trademarks or registered trademarks of Resilient Systems, Inc. in the United States and other countries. All other product names mentioned herein may be trademarks or registered trademarks of their respective companies.

Published: June 2016

<https://www.resilientsystems.com>

Table of Contents

1.	Introduction	5
2.	Administrator Settings.....	5
2.1.	Users	5
2.2.	Groups	6
2.3.	Timeframes.....	6
2.4.	Network.....	6
2.5.	Organization.....	7
2.5.1.	Details	7
2.5.2.	Settings	7
2.5.3.	Migrate Settings	7
2.6.	Threat Sources	8
2.7.	Notifications	9
3.	Customization Settings.....	10
3.1.	Layouts	10
3.1.1.	New Incident Wizard	10
3.1.2.	Incident Tabs.....	11
3.1.3.	Close Incident	13
3.1.4.	Fields	13
3.1.5.	Views	14
3.1.6.	Data Tables.....	14
3.1.7.	Blocks	15
3.2.	Actions	16
3.2.1.	Message Destinations.....	16
3.2.2.	Manual Actions.....	17
3.2.3.	Automatic Actions	18
3.2.4.	Action Fields.....	18
3.2.5.	Action Scripts	19
3.3.	Phases & Tasks	19
3.4.	Incident Types.....	20
3.5.	Breach	20
4.	Managing LDAP Authentication	22
4.1.	Before Enabling LDAP Authentication	22
4.2.	Enabling LDAP Authentication	23
4.3.	Managing LDAP Users in Groups	24
4.4.	Deleting LDAP Users	24

1. Introduction

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.

2. 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.

2.1. Users

Each person who needs access to the Resilient Incident Response Platform requires a user account.

To set up a new user, go to the Users tab then click **Invite User** and enter the email address of the new user. You then 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.

You can invite users individually using the Invite User button.

If LDAP is enabled for your Organization, the users of the authorized LDAP group are listed and given the Default permission. See [Managing LDAP Authentication](#) for more information.

Next, select the appropriate user permissions:

- **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 also 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 can not 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.

Click **Send Invitation** when you have entered all the information. The new 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.

2.2. 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.

2.3. 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 incident response plans. Go to the **Timeframes** tab and click the **Edit** button to enable changes and then click **Save** when you've 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. Resilient Systems does not provide legal advice. Dates can also be adjusted on a per-task basis within any incident response plan.

2.4. Network

The Network tab allows you to define an approved list of IP addresses that are allowed to connect to the Resilient system for your organization. To specify specific IP addresses or ranges, click on 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.

2.5. 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.

2.5.1. Details

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

2.5.2. 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 Resilient Systems 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.
- **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 Resilient Systems. 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*.

2.5.3. 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 actions, 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, and layouts from the Customize tab, and the actions from the Actions tab. Once you click the **Export** button, the settings are stored in JSON format to a **res** file. These tabs are available under in **Customization Settings**.

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 actions, 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 system performs the following during an import:

- Updates all incident fields, types and data table definitions.
- Since automatic tasks names are not unique even within the same incident type, the system attempts to match automatic 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 manual or automatic actions that have a condition that refers to incident members; for example, an action that is executed only when the incident member list contains a specific user. In this case, the system retains the user if the imported condition contains an exact match of the user. If it is not an exact match, the system 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 actions. 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.

2.6. Threat Sources

When artifacts are added to incidents, the Resilient platform can optionally search for those artifacts in several cyber threat sources which 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 IR 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*.

2.7. Notifications

The notifications tab allows Administrators to customize both email and in-product notifications, as well as create new notifications based on certain criteria. All of the notifications created by the administrator is available to the end users but they can choose to enable/disable them or change the notification mechanism. Note that notifications are suppressed to the user who triggers the action (e.g., 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 on the New Notification button.

Creating a notification consists of the following steps:

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 of notification should relate to the types of objects in the system. Choices include Incident, Task, Artifact, or Milestone.
3. Select the type of individual (as they relate to the object) who should receive the notification.
4. Optionally, select whether to notify specific named users.
5. Select optional triggers. An optional trigger is used when an object (such as a task) is added or removed from an incident. You can also add field specific triggers. Field specific triggers are used to alert users when a set of criteria is met, such as when an incident severity is set to high, data compromised is selected as true, and similar. You can add any number of field specific triggers to a notification. When multiple triggers are added, they are AND'ed together. In other words, they must all be true in order to generate the notification.
6. Select the checkbox if an email alert should be sent, and fill in the text that should be included in the message body. You can use the substitution variables \${TASK} and \${INCIDENT} to reference the task and incident.
7. Select this checkbox if a system notification should be created. A system notification is an alert in the notification drop-down by your username symbolized with a red circle and a number. Also, fill in the text that should be included in the body of the notification. You can use the substitution variables \${TASK} and \${INCIDENT} to reference the task and incident involved.

3. Customization Settings

The Customization Settings page includes several tabs that allow you to customize various aspects of the Resilient platform. This includes modifying certain built-in fields, adding your own custom fields, modifying or creating task lists or runbooks, customizing the 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**.

3.1. 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 one or more conditions are met, and create your own custom tabs. You can also customize the 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.

3.1.1. New Incident Wizard

You can rearrange and modify the steps of the New Incident Wizard, 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 First Details, Privacy Details, and Describe the Incident, respectively.

The screenshot displays the 'New Incident Wizard' configuration page. The top navigation bar includes tabs for 'Layouts', 'Actions', 'Phases & Tasks', 'Incident Types', and 'Breach'. The 'Layouts' tab is active, showing a sidebar with 'New Incident Wizard', 'Incident Tabs', and 'Close Incident'.

The main content area is titled 'New Wizard' and contains three sections:

- FIRST Details:** A list of fields including 'FIST Details', 'FIST - \$ Impact', 'Country', and 'Key Contacts'.
- Privacy Details:** A list of fields including 'Section', 'Required Privacy Information', 'Incident/Type Nature', 'Supplier Name', and 'Supplier #'.
- Describe the Incident:** A list of fields including 'Describe and Name the Incident', 'Name', 'Data Encrypted', and 'Source of Data'.

On the right side, there are two panels:

- Fields:** A search bar and a list of fields including '(MSTIC) Alert End', '(MSTIC) Alert Start', '(MSTIC) Assess & Analyze End', '(MSTIC) Assess & Analyze Start', '(MSTIC) Discovery End', '(MSTIC) Discovery Start', '(MSTIC) Mobilization End', and '(MSTIC) Mobilization Start'.
- Views:** A list of views including 'Address', 'Criminal Status View', 'Data Types', 'Employee Involvement View', 'HIPAA Form', 'Membership Chooser', 'PII Fields View', 'Record Count', and 'Regulators'.

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 condition is met. 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. These items are 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.

3.1.2. 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 screenshot shows the 'Incident: Manage Tabs' configuration window. On the left, a sidebar lists various incident components, with 'Manage Tabs' selected under the 'Incident Tabs' category. The main panel displays a horizontal row of tabs for the incident, including 'Tasks', 'Details', 'Breach', 'Notes', 'Members...', 'News...', 'Attac...', 'Stats', 'Timeli...', and 'Artifa...'. Below the tabs, there are controls for 'Tab Visible' (radio buttons for Yes, No, Conditional) and a 'Tab Text' input field containing the text 'Tasks'.

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 Breach and Stats, which are conditional. The Notes and Reqs tabs are hidden. Reqs is also a user-created tab.

Incident: **Manage Tabs** Cancel Save

Tasks	Details	Breach	Notes	Memb...	News...	Attac...	Stats	Timeli...	Artifa...

Reqs

Tab Visible ☒ Yes ☐ No ☐ Conditional

Tab Text *

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 then 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, Reqs is a custom tab. You can delete custom tabs only. You can rename or hide the default tabs, but not delete them.

- **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 is displayed 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 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 is displayed 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.

3.1.3. Close Incident

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

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

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 within your organization's UI 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.

3.1.5. 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.

3.1.6. 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 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 "Preview & Confirm" step is currently active. 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

3.1.7. 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 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.

3.2. Actions

The Actions allows administrators to configure an optional module of the Resilient platform known as the Custom Action Framework. The custom action framework (CAF) enables organizations to define and implement custom behaviors in response to user-defined conditions arising within the Resilient platform. If your organization has not purchased this feature, the tab simply contains a message explaining so. Custom actions can be configured as automatic actions or manual actions. As the name implies, automatic actions are executed automatically when a condition is met without any involvement by a user. Manual actions require that a user explicitly invoke the action by clicking a button that appears in the Resilient user interface. An example of an automatic action is to query an internal user directory whenever a User Account artifact is added to an incident, and automatically update the artifact with additional information about the user account. An example of a manual action is to insert a button on User Account artifacts to allow a Resilient user to disable the account directly from the Resilient platform. There are many use cases for custom actions including querying threat data sources, pulling data from other security components such as SEIMs and IDS systems, submitting trouble tickets to IT helpdesk systems, querying asset or user databases, etc.

There are three main steps in setting up a custom action:

1. Configure a “message destination” to transport messages about a custom action condition to the code or script, which processes it.
2. Configure the action within the Resilient platform, which includes defining the condition that triggers the action.
3. Create and execute the script or program, which connects to the message destination, pulls messages from it and processes them to achieve some result.

3.2.1. Message Destinations

The first step in setting up custom actions is to define the message destination that is used to communicate messages to the program or script which performs the desired processing. The message includes all of the details related to the Resilient object which is the subject of the action (e.g., an incident, task or artifact). To define a message destination, navigate to the Actions tab on the administration screen, select the Message Destination tab along the left and then click on Add Message Destination. In the resulting Create Message Destination dialog, fill in or select the following values.

- **Type:** Message destinations are either of type Topics or Queue. The difference lies in what should happen if a condition is fired and a message is placed on the message destination, but no action script is listening to it. If the message destination is of type Queue, the message stays on the message destination waiting for an action script to connect to it and pull the message off. If the type is Topic, it is discarded. Another difference is that if multiple actions scripts are listening to the same message destination, if it is of type Topic all of the action scripts are handed a copy of the message, but if it is of type Queue only one actions script receives it.
- **Name:** This is just a text field for naming the destination. Give it a name that is descriptive of the purpose of the message destination. As you enter the name, the system automatically generates the programmatic name which is used by the action script when connecting to the destination.
- **Programmatic Name:** This field is automatically filled in by the system based on the Name field. Action script developers need to use this programmatic name when creating scripts that connect to the destination to execute the behaviors of the custom action. It is displayed here for informational purposes.

- **Expect Acknowledgement:** Some action scripts are expected to consume messages from message destinations and silently process them without returning any indication of progress or status. Other action scripts return an acknowledgement when they have completed the processing of a message. When a destination is configured to Expect Acknowledgement, the list of executed actions in the Resilient UI show these items as “Pending” until the expected acknowledgement is received.
- **Users:** Action scripts that connect to a message queue must authenticate using a Resilient account. Message destinations limit which accounts are authorized to connect to them and receive messages. Specify the one or more accounts authorized to connect to this message destination. You will typically want to create specific accounts for the purposes of using the API's rather than using existing user accounts.

3.2.2. Manual Actions

Manual actions are actions that are executed as a result of a user explicitly invoking them. Configuring a manual action results in an action option being displayed in an action menu in the appropriate place in the Resilient user interface. For example, if you configure a manual action on notes for escalating the note to an external ticketing system, then when users are viewing notes they see an option on the note's action menu to invoke that action. Like automatic actions, invoking a manual action results in a message being placed on a message destination that will then be consumed by an action script to execute the desired processing. To define a manual action, navigate to the Actions tab on the administration screen, select the Manual Actions tab along the left and then click on Add Manual Action. In the resulting Create Manual Action dialog fill in or select the following values.

- **Display Name:** This is the name of the manual action that is displayed to the user in the appropriate action menu in the user interface.
- **Object Type:** Select the object type to which this action will be associated. For example, if the action is to be associated with changes to artifacts then select Artifact from the drop-down. This dictates which action menus the manual action are shown.
- **Destinations:** Select one or more message destinations to place messages onto when the action is invoked by a user.
- **Conditions:** Define the conditions under which the action should be displayed in the corresponding action menu. In this way, the administrator can control under what conditions a manual action is exposed to users. For example, a given manual action may only be appropriate when the incident type is Phishing and the incident severity is High. If you do not specify any conditions then the manual action is always displayed in the action menu of objects of the associated type. If the condition refers to a select or multi-select field and you choose multiple values for that field, it evaluates to true whenever any of those values are present (they are OR'ed together). If you add multiple conditions, the overall result evaluates to true only when all individual conditions evaluate to true (they are AND'ed together).
- **Layout:** In some cases, in order to execute manual actions you need to collect additional information from the user. For example, in order to generate an IT ticket from a task note you may need to ask the user to select a ticket queue and specify a priority. The manual action layout allows you to define the layout of dialog box that is displayed to the user in order to collect this additional information. You can drag and drop action fields (discussed below) as well as insert headers and html markup on the layout panel to define how that dialog box is organized. If you leave the layout empty, no dialog box is displayed when the action is invoked by the user.

3.2.3. Automatic Actions

Automatic actions are executed without any direct invocation by a user. They are associated with a particular object type in the system and are automatically triggered by some condition being met. When you define an automatic action, you are really just describing the conditions under which a message is placed on a message destination, which is then consumed by an action script to execute the desired processing. To define an automatic action, navigate to the Actions tab on the administration screen, select the Automatic Actions tab along the left and then click on Add Automatic Action. In the resulting Create Automatic Action dialog, fill in or select the following values.

- **Display Name:** This is a text field for naming the automatic action. Give it a name that is descriptive of the purpose of the action.
- **Object Type:** Select the object type to which this action will be associated. For example, if the action will be associated with changes to artifacts then select Artifact from the drop-down.
- **Destinations:** Select one or more message destinations to place messages onto when the action conditions are met.
- **Conditions:** Define the conditions under which the action should be triggered, resulting in a message being placed on the selected destination(s). If you do not specify any conditions, the action is triggered every time an object of the associated type is created or updated. If the condition refers to a select or multi-select field and you choose multiple values for that field, it evaluates to true whenever any of those values are present (they are OR'ed together). If you add multiple conditions, the overall result evaluates to true only when all individual conditions evaluate to true (they are AND'ed together).

3.2.4. Action Fields

Action fields provide the mechanism to ask users for additional information when they invoke a manual action. In order to prompt a user for additional information, you must first define the fields on the Actions Field tab which is displayed, and then you must add the fields to the layout of the appropriate manual actions (see Manual Actions above). To define a new action field, navigate to the Actions tab on the administration screen, select the Action Fields tab along the left and then click on New Field. In the resulting Create Action Field dialog fill in or select the following values.

- **Label for the Field:** Enter the display name for the field.
- **API Access Name:** The API access name is the name that must be used when interacting with this field from the API. It is automatically generated by the system based on the display name.
- **Field Type:** Select the type of the field that best matches its purpose.
- **Requirement:** Select a requirement disposition. If you select Required, the user can not execute the action without specifying a value for the field.
- **Tooltip:** If you enter a tooltip, there is an information icon next to the field when it is displayed to users. When the user hovers over the information icon, the tooltip is displayed.
- **Placeholder:** If you enter a placeholder this value is automatically displayed in the field when it is displayed to provide a hint to the user.

3.2.5. Action Scripts

The final step for implementing a custom action is to create and execute an action script that connects to a message destination, pulls off messages that are posted to it, and processes them accordingly. This may also include leveraging the Resilient REST API to update incidents in the Resilient platform based on the results of the processing. The term, *actions scripts*, is used here to refer to any script or programs that connect to a Resilient message destination for the purposes of receiving messages and processing them. The Resilient Custom Action Framework is accessible by two different standard protocols, JMS and STOMP. As such, developers can write their actions scripts in any programming or scripting language that supports bindings for one of these two protocols. For details on creating action scripts along with examples, refer to the *Resilient Custom Action Programmers Guide*.

3.3. Phases & Tasks

Master administrators have the ability to customize phases, create automatic tasks, modify or override system-generated tasks, and change the order in which tasks are listed in the incident response plan.

The Automatic Tasks feature allows for the creation of tasks that are unique to your organization. Once created, automatic tasks are incorporated into future incident response plans generated for the organization.

To create an automatic task, click the **Create Automatic Task** button and assign a name to the task. Select the appropriate choices for each field. To apply the automatic tasks to specific incident types, select those types from the field labeled **Incident Types**. If a specific incident type is not selected, the automatic task is applied to all incidents. When finished, click **Create**.

To edit an existing automatic task, click on the “pencil” icon for that task which brings up the Editing Automatic Task dialog. Make the necessary changes and click **Save**. Automatic tasks can be deleted by selecting the particular task and then clicking the trash can icon.

System-generated tasks can be modified to reflect the organization’s processes and workflows. To make modifications, click the appropriate task category and then select the task that you wish to modify. Make the desired changes to the name of the task or its instructions. Next, select if you would like to apply the changes to existing open incidents as well as future incidents, or future incidents only. If you wish to entirely disable a task so that it does not appear in future incident response plans, select **No** for **System Task Enabled**. Once the changes are complete, click the **Create** button. This creates an override of the system task.

To make changes to a previously modified task, select it from the list under the appropriate category, make the necessary edits, and click **Save**. If you wish to remove modifications so future instances of the task display the original system-generated text, select the appropriate task from the list and then click the trash can icon to delete the override. **NOTE:** This only removes the modification from future instances of the task; it does not remove it from existing incident response plans.

You may set the order in which custom automatic and system tasks are shown in your incident response plans. To modify the order, go to the phase containing the task you wish to modify, then drag and drop the tasks into the order you’d like them to appear in that phase. You can move tasks to a different phase by editing the task and selecting the desired phase.

You can also create, edit, reorder, and delete phases. To create a new phase, click the **Create Phase** button, specify a name, and save your changes. You can edit the name by clicking the “pencil” icon next to the phase. To delete, click the small “x” icon. If there are any existing tasks in the phase being deleted, the system prompts the user to move them to another phase. You can reorder phases by selecting a phase and then dragging and dropping it to the desired position.

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

3.4. Incident Types

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 custom automatic tasks in response plans. By building up hierarchies of incident types and associating them with detailed custom automatic tasks, you can create very precise incident response plans 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.

3.5. 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 IR Module, you can still configure breach settings but breach-related tasks are not generated within an incident response plan.

- **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 response plans.

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 incident response plans.

- **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’ve 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've made the desired selections. Jurisdictions not indicated here can be added during incident creation if necessary.

4. 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.

4.1. 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

4.2. 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.

Administrator Settings

The screenshot displays the 'Administrator Settings' interface 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' with an 'ON' toggle and 'Attachments Used Size: 0 B'; 'Default Tasks' with an 'OFF' toggle; and 'Enable LDAP authentication' with an 'ON' toggle. Below the LDAP section, there is a search bar and a table of LDAP groups. The table has columns for 'Group Name' and 'Actions'. One group, 'Infosec', is listed with a right-pointing arrow next to its name. In the 'Actions' column for 'Infosec', there is a blue link labeled 'Authorize Group'. A 'Close' button is located at the bottom right of the settings panel.

© 2015 Resilient Systems, Inc.

All 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 set 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.

4.3. 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.

4.4. 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