IBM Resilient

Incident Response Platform

Release Notes V31.1

Release Date: December 2018

IBM Resilient Incident Response Platform on Cloud and IBM Resilient Incident Response Platform V31.1 (on-premises licensed version) orchestrate and automate the people, processes, and technology that are associated with incident response. Purpose-built for either cloud or on-premises environments based on your business needs, these Resilient Incident Response Platform solutions streamline incident response and privacy response management to provide an automatic, fast, and flexible way for organizations to react to events and incidents.

FEATURES AND ENHANCEMENTS

The V31.1 release of the Resilient Incident Response Platform introduces a number of new features and enhancements. All changes and bug fixes from the previous releases are included.

The following new features and enhancements are provided in Resilient V31.1:

- **Privacy**:
  - The following new regulators were added to the Privacy Module:
    - Bermuda
    - Canada – The rules defined in the Personal Information Protection and Electronic Documents Act (PIPEDA) are now available in new Resilient organizations. To apply these rules to existing organizations, you must update the New Incident Wizard and the Incident Breach Tab, as described in Updating Privacy Rules.
    - Virginia (Income Tax Preparers)
  - The following regulators were updated in the Privacy Module:
    - Belgium
    - Colorado
    - New York (Department of Financial Services)
    - Iowa
- **Logging**: The client access log now includes the user's email address for each logged entry.
- **Organization settings**: For exported settings, the organization name is included in the file name.
- **Optional packages**: The `net-snmp-utils` package, from the Net-SNMP project, is available as an optional update.

- **Incidents list**: The column names can be filtered when modifying the Incidents page layout.

UPDATING PRIVACY RULES

As an existing customer, your **New Incident Wizard** layout remains unchanged during installation, to retain any customizations. The **Breach** tab has been updated automatically to include the PIPEDA Breach Risk Assessment. If you would like to add this assessment to the New Incident Wizard, follow the instructions below.

Note: Your current layout might be different to the layout described below, depending on your version of Resilient or your customization settings.

Update the New Incident Wizard

If you do not want to retain any customizations in the New Incident Wizard, you can apply the latest updates as follows:

1. In the system menu, click **Customization Settings**.
2. Click **Layouts > New Incident Wizard** to open the New Wizard page.
3. Click **Restore to Default**.
4. Click **OK** to confirm.

If you want to retain customizations in the New Incident Wizard, apply the latest updates manually as follows:

1. In the system menu, click **Customization Settings**.
2. Click **Layouts > New Incident Wizard** to open the New Wizard page.
3. In the **Fields** list, search for the **Was personal information or personal data involved?** field. If the field does not exist, complete the following steps:
    a. In the **Fields** list, search for the **Data Compromised** field.
    b. Select the field and click the edit icon to open the Edit Incident Field window.
    c. In the **What is the label for this field** section, replace the existing text with the following text:
    Was personal information or personal data involved?
    d. In the **Tooltip** section, replace the existing text with the following text:
    Determine whether personal information/data was foreseeably involved, disclosed, compromised, accessed, altered, destroyed, damaged, lost or inaccessible.
    e. Click **Save** to close the Edit Incident Field window.
4. Add the **PIPEDA Breach Risk Assessment** step as follows:
    a. Click **Add Step**.
    b. In the new step, click the **Move Down** icon repeatedly to move the step to the end of the page.
    c. Click the **Step Settings** icon to open the Edit Step window.
        i. In the **Step Label** field, add the following text:
        PIPEDA Breach Risk Assessment
        ii. Click **Add Condition**. From the conditions list, select **Was personal information or personal data involved?** From the comparisons list, select **is equal to**. From the options list, select **Yes**.

iii. Click **Add Condition**. From the conditions list, select **Regulators**. From the comparisons list, select **has one of**. From the options list, select **PIPEDA**.

iv. Click **OK** to close the Edit Step window.

d. From the **Blocks** section, drag a **Header** block to the new PIPEDA Breach Risk Assessment step.

i. In the new header block, click the **Edit** icon to open the Edit Value window.

ii. In the value field, add the following text:
PIPEDA Breach Risk Assessment

iii. Click **OK** to close the Edit Value window.

e. From the **Views** section, drag a **PIPEDA Form** view to the new PIPEDA Breach Risk Assessment step, and insert the view under the header block.

5. At the top of the New Wizard page, click **Save** to apply all of the modifications.

KNOWN ISSUES

Tracking Code	Issue
RES-12501	Sorting PIPEDA fields on the Incidents page hides incidents without PIPEDA field values

CORRECTED ISSUES

Tracking Code	Issue
RES-10271	Unclear error message when importing settings with conflicting roles
RES-10572	Filter options for hierarchical incident types are not available on the Incidents page
RES-11345	Timeout errors when rescanning artifacts
RES-11487	Unclear error message when importing settings with conflicting message destinations
RES-11519	Column focus lost while editing data table
RES-11525	Cannot import organization settings with conditional layouts that refer to workspaces
RES-12193	Incident History Report cannot be generated in some cases
RES-12264	Number validation does not work in Internet Explorer 11