ScienceLogic

# CrowdStrike Falcon SyncPack

Version 1.0.0

# Table of Contents

# Chapter

# 1

# Introduction to the CrowdStrike Falcon SyncPack

## Overview

This chapter describes how you can configure and use the "CrowdStrike Falcon" SyncPack with the PowerFlow platform to sync SL1 events and CrowdStrike detections.

This SyncPack uses the "CrowdStrike Integration" PowerPack.

This chapter covers the following topics:

# What Can I Do with this SyncPack?

The "CrowdStrike Falcon" SyncPack let you sync SL1 events and CrowdStrike Falcon detections (security events). You can configure the automation policies in the "CrowdStrike Falcon Automation" PowerPack to pull events from CrowdStrike into SL1 for use in event correlation and incident management.

Integration with the CrowdStrike Falcon platform allows security teams to accelerate operations by improving threat detection accuracy through a single interface. When a security detection occurs within the Falcon platform, such as potential malware on a device, the detection will be automatically sent to SL1 as an event. From there, SL1 can simultaneously create an incident to document the issue and trigger a response as defined by rules set by an administrator.

This SyncPack includes the following integrations:

- ***Fetch Detections from CrowdStrike and Send Alert to SL1***. This application acquires tokens and New Detections from CrowdStrike and creates alerts for SL1.
- ***Clear Detection from Cache***. This application acquires and saves event details to send to SL1.

# Contents of the SyncPack

This section lists the contents of the "CrowdStrike Falcon" SyncPack.

## PowerFlow Applications

- ***Fetch Detections from CrowdStrike and Send Alert to SL1***. This application acquires tokens and New Detections from CrowdStrike and creates alerts for SL1.
- ***Clear Detection from Cache***. This application acquires and saves event details to send to SL1.

For more information about how to configure these applications, see *Configuring Applications for the CrowdStrike Falcon SyncPack*.

## Configuration Object

- ***CrowdStrike Sample Configuration***. This configuration object can be used as a template after the SyncPack is installed on the PowerFlow system.

## Steps

The following steps are included in this SyncPack:

- Fetch Detections and Generate Payloads for SL1
- Fetch New Detections from CrowdStrike
- Get Alerted Detections from Cache
- Get Each Detection and Create SL1 Alerts
- Get Event Details and Clear Detections ID

# Chapter 2

# Installing the CrowdStrike Falcon SyncPack

## Overview

This chapter describes the how to install the "CrowdStrike Falcon" SyncPack and the "CrowdStrike Falcon Automation" PowerPack.

This chapter covers the following topics:

# Installing the CrowdStrike Falcon SyncPack

A SyncPack file has the **.whl** file extension type. You can download the SyncPack file from the ScienceLogic Support site.

## Downloading the SyncPack

**NOTE:** If you are installing or upgrading to the latest version of this SyncPack in an offline deployment, see ***Installing or Upgrading in an Offline Environment*** to ensure you install any external dependencies.

To locate and download the SyncPack:

1. Go to the ScienceLogic Support Site at https://support.sciencelogic.com/s/.
2. Click the **[Product Downloads]** tab and select *PowerPacks & SyncPacks*.
3. In the ***Search*** field, search for the SyncPack and select it from the search results. The **Release Version** page appears.
4. On the **[Files]** tab, click the down arrow next to the SyncPack version that you want to install, and select *Show File Details*. The **Release File Details** page appears.
5. Click the **[Download File]** button to download the SyncPack.

After you download the SyncPack, you can import it to your PowerFlow system using the PowerFlow user interface.

## Importing the SyncPack

To import a SyncPack in the PowerFlow user interface:

1. On the **SyncPacks** page (⚙) of the PowerFlow user interface, click **[Import SyncPack]**. The **Import SyncPack** page appears.
2. Click **[Browse]** and select the **.whl** file for the SyncPack you want to install. You can also drag and drop a **.whl** file to the **Import SyncPack** page.
3. Click **[Import]**. PowerFlow registers and uploads the SyncPack. The SyncPack is added to the **SyncPacks** page.
4. You will need to activate and install the SyncPack in PowerFlow. For more information, see the following topic.

**NOTE:** You cannot edit the content package in a SyncPack published by ScienceLogic. You must make a copy of a ScienceLogic SyncPack and save your changes to the new SyncPack to prevent overwriting any information in the original SyncPack when upgrading.

## Installing the SyncPack

To activate and install a SyncPack in the PowerFlow user interface:

1. On the **SyncPacks** page of the PowerFlow user interface, click the **[Actions]** button ( ⋮ ) for the SyncPack you want to install and select *Activate & Install*. The **Activate & Install SyncPack** modal appears.

   > **NOTE:** If you try to activate and install a SyncPack that is already activated and installed, you can choose to "force" installation across all the nodes in the PowerFlow system.

   > **TIP:** If you do not see the PowerPack that you want to install, click the Filter icon (≡) on the **SyncPacks** page and select *Toggle Inactive SyncPacks* to see a list of the imported PowerPacks.

2. Click **[Yes]** to confirm the activation and installation. When the SyncPack is activated, the **SyncPacks** page displays a green check mark icon (✓) for that SyncPack. If the activation or installation failed, then a red exclamation mark icon (❗) appears.
3. For more information about the activation and installation process, click the check mark icon (✓) or the exclamation mark icon (❗) in the **Activated** column for that SyncPack. For a successful installation, the "Activate & Install SyncPack" application appears, and you can view the Step Log for the steps. For a failed installation, the **Error Logs** window appears.
4. If you have other versions of the same SyncPack on your PowerFlow system, you can click the **[Actions]** button ( ⋮ ) for that SyncPack and select *Change active version* to activate a different version other than the version that is currently running.

# Installing the CrowdStrike Falcon Automation PowerPack

The "CrowdStrike Falcon Automation" PowerPack includes automation policies and action policies that bidirectionally sync jobs, pipeline jobs, and node status between CrowdStrike and SL1. The PowerPack also contains an event policy and SOAP/XML credentials.

You must install and configure the "CrowdStrike Falcon" SyncPack before using the "CrowdStrike Falcon Automation" PowerPack.

> **TIP:** By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

# Chapter

# 3

# Configuring Applications for the CrowdStrike Falcon SyncPack

## Overview

This chapter describes how to set up the PowerFlow applications for the "CrowdStrike Falcon" SyncPack, and how to use the automations in the "CrowdStrike Falcon Automation" PowerPack to pull events from CrowdStrike into SL1 for use in event correlation and incident management.

This chapter covers the following topics:

# Workflow for Configuring the SyncPack

The following workflows describe how to configure SL1 and PowerFlow to work with the "CrowdStrike Falcon" SyncPack.

## Configuring SL1

1. *Enable the CrowdStrike event policy*
2. *Create a SOAP/XML credential to access PowerFlow*
3. *Edit the CrowdStrike run book action*
4. *Enable the CrowdStrike run book automation*

## Configuring PowerFlow

1. *Create a configuration object*
2. *Align the configuration object and configure the PowerFlow applications*
3. *Schedule the PowerFlow applications*

# Configuring SL1

The following topics cover how to set up your SL1 instance to work with the "CrowdStrike Falcon" SyncPack.

## Enabling the CrowdStrike Event Policy

The "CrowdStrike Falcon Automation" PowerPack includes one standard API event policy, "CrowdStrike: Alert to Event", which triggers the events detected by the PowerFlow applications included in the "CrowdStrike Falcon" SyncPack and the associated automation action policy.

To enable the event policy:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Click the Actions menu ( ••• ) for the "CrowdStrike: Alert to Event" event policy and select *Edit*. The **Event Policy Editor** page appears.
3. Click the ***Enable Event Policy*** toggle to enable the event policy and click **[Save]**.

## Creating a SOAP/XML Credential to Access PowerFlow

You must create a SOAP/XML credential so that the action policies included in the PowerPack can access your PowerFlow system. The "CrowdStrike Falcon Automation" PowerPack includes the "PowerFlow CrowdStrike" sample credential that you can edit to use with your SL1 PowerFlow system.

To create a SOAP/XML credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the "PowerFlow CrowdStrike" sample credential, click its **[Actions]** icon ( ··· ), and select ***Duplicate***. A copy of the credential, called **PowerFlow CrowdStrike copy** appears.
3. Supply values in the following fields:
   - ***Name***. Type a new name for the credential.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
   - ***URL***. Type the host name for your PowerFlow system.
   - ***HTTP Auth User***. Type the administrator username for your PowerFlow
   - ***HTTP Auth Password***. Type the administrator password for your PowerFlow system.
4. Click **[Save & Close ]**.
5. Take note of the SL1-assigned ID number for the new credential on the **Credentials** page, in the **ID** column. You will need the ID number when editing the input parameters of the automation actions included in the PowerPack, below.

## Editing the CrowdStrike Run Book Action

The "CrowdStrike Falcon Automation" PowerPack includes one action policy that uses the "Run Integration Service Application" action type to trigger the PowerFlow application that collects data from CrowdStrike. You can specify the credential ID in a JSON structure that you enter in the ***Input Parameters*** field in the **Action Policy Editor** modal.

To edit the run book actions included in the PowerPack:

1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Locate the action policy that you want to use, and then click its wrench icon (🔧). The **Editing Action** page appears.
3. In the ***Input Parameters*** field, change the values of the following parameters:
   - ***credential_id***. Change the value to the credential ID that you noted earlier whencreating a credential for your PowerFlow system in the previous procedure. This parameter is required.
   - ***include_event***. Leave the value as "true".
   - ***application_name***. Leave the default application value.
   - ***params***. Leave the default parameter value.
4. Make sure the ***Action State*** is set to *Enabled*, and then click **[Save]**.

## Enabling the CrowdStrike Run Book Automation

The "CrowdStrike Falcon Automation" PowerPack includes the "Crowdstrike: Clear Detection ID" automation policy that updates the SL1 event with the state of the associated CrowdStrike job. When a node is offline, a failure occurs, or a major event is detected in CrowdStrike, an SL1 event is created and the associated event is updated with any job details.

To enable the run book automation:

1. In SL1, go to the **Automations** page (Registry > Run Book > Automation).
2. Locate the "Crowdstrike: Clear Detection ID" automation policy and click its wrench icon (🔧). The **Automation Policy Editor** page appears.
3. Update the following fields:
    - ***Policy State***. Select *Enabled*.
    - ***Policy Priority***. Select *High* to ensure that this PowerFlow automation policy is added to the top of the queue.
    - ***Available Actions***. If it is not already selected, select "Run Integration Service Application: CrowdStrike: Clear Detection ID" and click the arrows to move it to ***Aligned Actions***.

WARNING: ScienceLogic highly recommends that you do not make changes to the ***Policy Type***, ***Repeat Time***, or ***Align With*** fields or the *And event is NOT acknowledged* setting.

4. Click **[Save]**.

# Configuring PowerFlow

The following topics cover how to set up your PowerFlow instance to work with the "AWS Incident Manager" SyncPack.

## Creating a Configuration Object

A ***configuration object*** supplies the login credentials and other required information needed to execute the steps for a PowerFlow application. The **Configurations** page (⚙) of the PowerFlow user interface lists all available configuration objects for that system.

You can create as many configuration objects as you need. A PowerFlow application can only use one configuration object at a time, but you can use (or "align") the same configuration object with multiple applications.

For this SyncPack, you should make a copy of the "CrowdStrike Sample Configuration" configuration object, which is the sample configuration file that was installed with the "CrowdStrike Falcon" SyncPack.

**TIP:** The "CrowdStrike Sample Configuration" configuration object contains all of the required variables. Simply update the variables from that object to match your SL1 and CrowdStrike settings.

To create a configuration object based on the "CrowdStrike Sample Configuration" configuration object:

1. In the PowerFlow user interface, go to the **Configurations** page (⚙).
2. Click the **[Actions]** button (⋮) for the "CrowdStrike Sample Configuration" configuration object and select *Edit*. The **Configuration** pane appears.
3. Click **[Copy as]**. The **Create Configuration** pane appears.
4. Complete the following fields:
   - ***Friendly Name***. Type a name for the configuration object that will display on the **Configurations** page.
   - ***Description***. Type a brief description of the configuration object.
   - ***Author***. Type the user or organization that created the configuration object.
   - ***Version***. Type a version of the configuration object.
5. In the ***Configuration Data*** field, update the default variable definitions to match your PowerFlow configuration:
   - ***sl1_host***. Type the hostname or IP address of the SL1 system the alerts will synchronize with.
   - ***sl1_password***. Type the password for your SL1 system.
   - ***sl1_user***. Type the username for your SL1 system.
   - ***crowdstrike_url***. Enter the URL for your CrowdStrike system.
   - ***crowdstrike_username***. Type the username for your CrowdStrike system.
   - ***crowdstrike_password***. Type the password for your CrowdStrike system.
   - ***job_name***. Type the name for your CrowdStrike job.
   - ***receiver_mail***. Type the email address that you want to receive updates on SL1 events and your CrowdStrike jobs.
   - ***sender_mail***. Type the email address that you want updates on SL1 events and your CrowdStrike jobs to send from.
   - ***sender_mail_password***. Type the password for the sender email address that you entered.
   - ***mailserver***. Type the server for your sender email.
   - ***mailserverport***. Type the port for your sender email.

   The following fields are required only if you choose to manually create a virtual device for your CrowdStrike instance:

     - ***device_class_id***. Type the device class ID for your CrowdStrike instance.
     - ***collector_group_id***. Type the collector group ID for your CrowdStrike instance.

    - ***device_id***.Type the device ID for your CrowdStrike instance.

6. Click **[Save]**. You can now align this configuration object with one or more applications.

NOTE: For more information about the CrowdStrike terms and concepts in this section, see the CrowdStrike documentation.

## Aligning a Configuration Object and Configuring PowerFlow Applications

You will need to align the following "CrowdStrike Falcon" SyncPack applications with the configuration object you just created in PowerFlow:

- "Fetch Detections from CrowdStrike and Send Alert to SL1"
- "Clear Detection from Cache"

To align the configuration object with the relevant PowerFlow applications:

1. On the **Applications** page of the PowerFlow user interface, open one of the PowerFlow applications listed above and click **[Configure]**. The **Configurations** pane for that application appears.
2. From the ***Configurations*** drop-down, select the configuration object you want to use.

NOTE: The values for **sl1_hostname** and the other parameters that appear in the **Configuration** pane with a padlock icon (🔒) are populated by the configuration object you aligned with the application. Do not modify these values. If you encounter an error, make sure your configuration object is configured properly.

3. Update any other fields on the **Configuration** pane for the application as needed.
4. Click **[Save]**.
5. Repeat this process for the remaining PowerFlow application.

## Scheduling PowerFlow Applications

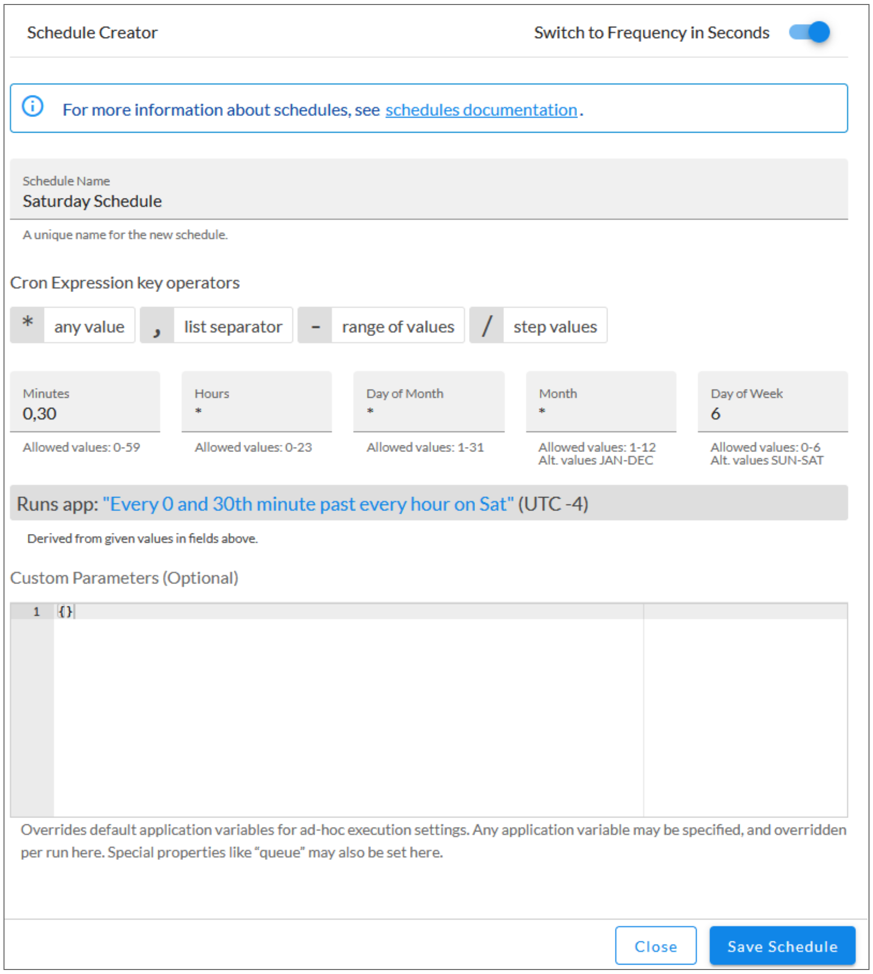
ScienceLogic recommends that you schedule the following PowerFlow applications:

- "Fetch Detections from CrowdStrike and Send Alert to SL1": every 60 seconds
- "Clear Detection from Cache": at least once a week

You can create one or more schedules for a single application in the PowerFlow user interface. When creating each schedule, you can specify the queue and the configuration file for that application.

To create a schedule:

1. On the **Applications** page (▤), click the **[Schedule]** button for the application you want to schedule. The **Scheduler** window appears.
2. In the **Schedule List** pane, click the down arrow icon (⌄) next to an existing schedule to view the details for that schedule.
3. In the **Schedule Creator** pane, complete the following fields for the default ***Frequency*** setting:
   - ***Schedule Name***. Type a name for the schedule.
   - ***Frequency in seconds***. Type the number of seconds per interval that you want to run the application.
   - ***Custom Parameters***. Type any JSON parameters you want to use for this schedule, such as information about a configuration file or mappings.
4. To use a cron expression, click the ***Switch to Cron Expression*** toggle to turn it blue. If you select this option, you can create complicated schedules based on minutes, hours, the day of the month, the month, and the day of the week:



Schedule Creator

Switch to Frequency in Seconds

For more information about schedules, see schedules documentation.

Schedule Name
Saturday Schedule
A unique name for the new schedule.

Cron Expression key operators

| * any value | , list separator | - range of values | / step values |
|---|---|---|---|

| Minutes | Hours | Day of Month | Month | Day of Week |
|---|---|---|---|---|
| 0,30 | * | * | * | 6 |
| Allowed values: 0-59 | Allowed values: 0-23 | Allowed values: 1-31 | Allowed values: 1-12<br>Alt. values JAN-DEC | Allowed values: 0-6<br>Alt. values SUN-SAT |

Runs app: "Every 0 and 30th minute past every hour on Sat" (UTC -4)

Derived from given values in fields above.

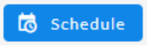
Custom Parameters (Optional)

```
{}
```

Overrides default application variables for ad-hoc execution settings. Any application variable may be specified, and overridden per run here. Special properties like "queue" may also be set here.

As you update the cron expression, the **Schedule** window displays the results of the expression in more readable language, such as *Runs app: "Every 0 and 30th minute past every hour on Sat*", based on 0,30 in the ***Minutes*** field and 6 in the ***Day of Week*** field.

5. Click **[Save Schedule]**. The schedule is added to the **Schedule List** pane. Also, on the **Applications** page, the **[Schedule]** button now displays with a dark blue background:



NOTE: After you create a schedule, it continues to run until you delete it. Also, you cannot edit an existing schedule, but you can delete it and create a similar schedule if needed.

To view or delete an existing schedule:

1. On the **Applications** page, click the **[Schedule]** button for the application that contains a schedule you want to delete. The **Scheduler** window appears.
2. Click the down arrow icon (⌄) to view the details of an existing schedule.
3. To delete the selected schedule, click the Actions icon ( ⋮ ) and select**[Delete]**.

TIP: On the **Scheduler** window for a PowerFlow application, you can click the **[Copy as]** button from the **Schedule List** pane to make a copy of an existing schedule.

NOTE: When either multiple SL1 instances or multiple CrowdStrike instances are involved with PowerFlow, you should create an individual configuration object for each SL1 or CrowdStrike instance. Next, create an individual schedule for each configuration object. Each schedule should use a configuration object that is specific to that single SL1 or CrowdStrike instance. Creating copies of a PowerFlow application from a SyncPack for the purpose of distinguishing between domains is not supported, and will result in issues on upgrades.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

## Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

## Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010