

 Breach Secure Now Partner Guide

— Autotask PSA Integration Setup Notifications, alerts, and client integration

Questions, Concerns? Want a 1-on-1 on-boarding
with our Operations team?

Email: Operations@breachsecurenow.com

Phone: (877) 275 – 4545

Autotask PSA Integration Setup

Table of Contents

Autotask Configuration *configuring settings in the Autotask console*.....pages 3 – 7

Portal Configuration *configuring settings in the partner management portal*.....pages 8 – 13

 Configuration Setup.....pages 8 – 10

 Notification Details & Descriptions.....pages 11 – 12

 Autotask Client Configuration.....pages 13 – 14

Configuring Settings in the Autotask Portal

Create New API User

Within the Autotask portal, navigate to the Menu/Admin/Resources (users) screen and click the **“New”** button.

Under the **“General”** tab, fill in the following information:

First Name: Secure

Last Name: Now

Email Address: operations@breachsecurenow.com

RESOURCE MANAGEMENT - New (Adding a resource may result in additional fees) ★ ?

Save & Close Save Save & Copy Cancel Tabs with * contain required fields

General * Security * HR * Approvers * Associations * Skills Attachments

Prefix

First Name * Secure Middle Initial

Last Name * Now

Title

Suffix

Gender

Primary Internal Location * Headquarters +

Office Phone Extension

Home Phone

Mobile Phone

Email Address * operations@breachsecurenow.com Email Type * Primary

Additional Email Address 1 Email Type

Additional Email Address 2 Email Type

Date Format * MM/dd/yyyy(Location Default)

Time Format * hh:mm a(Location Default)

Change Photo

Configuring Settings in the Autotask Portal

Create API User Credentials

Configure the account credentials. You will utilize these credentials when configuring Autotask within the PII-Protect portal.

Under the “**Security**” tab, fill in the following information:

Username: securenow

Password: Create a password of your choosing

Security Level: API User (system)

Checkboxes: Resource is not required to Submit Timesheets

Under the “**API Tracking Identifier**” section, select:

Integration Vendor: Secure Now – Security, Dark Web & Training

The screenshot shows the 'RESOURCE MANAGEMENT - New' form in the Autotask portal, specifically the 'Security' tab. The form is titled 'RESOURCE MANAGEMENT - New (Adding a resource may result in additional fees)'. It has tabs for General, Security, HR, Approvers, Associations, Skills, and Attachments. The 'Security' tab is active. The form contains several sections: 'CREDENTIALS' with fields for Username (securenow), Password, Confirm Password, and Security Level (API User (system)); a list of checkboxes for permissions; 'Outsourcing Permissions' set to None; 'TWO-FACTOR AUTHENTICATION' with options for AuthNvil, CRYPTOCard Tokens, and TOTP; and 'API TRACKING IDENTIFIER' with a dropdown for Integration Vendor (Secure Now - Security, Dark Web) and a 'Generate' button. Several fields and checkboxes are highlighted with yellow boxes.

RESOURCE MANAGEMENT - New (Adding a resource may result in additional fees)

Save & Close Save Save & Copy Cancel Tabs with * contain required fields

General * Security * HR * Approvers * Associations * Skills Attachments

CREDENTIALS

Username * securenow @yourcompany.com

☒ Active

Password *

Confirm Password *

Security Level * API User (system)

☐ Allow Resource to access links to Datto pages from within Autotask (Datto Integration must be enabled)

☐ Allow Resource To Edit Skills

☐ Allow Resource to Create, Edit, and Delete Knowledgebase Articles

☐ Allow Resource to send bulk emails

☒ Resource is not required to Submit Timesheets

Outsourcing Permissions * None

TWO-FACTOR AUTHENTICATION

☐ Require Two-Factor Authentication for this Resource

Option 1 - AuthNvil
AuthNvil offers a strong authentication platform to cover multiple assets (including Windows network, production devices and web-based software) with a single solution, allowing you to consolidate security management and token use. It also provides a source of new revenue by allowing you to manage strong authentication for client assets on the same platform. To learn more about AuthNvil Two-Factor Authentication or sign up, [click here](#)

Option 2 - CRYPTOCard Tokens

Option 3 - TOTP (Google Authenticator, etc.)
Time-based one-time password

API TRACKING IDENTIFIER

API version 1.6 & later require the use of an API tracking identifier. Once assigned, this cannot be changed.

☒ None

☐ Integration Vendor
Secure Now - Security, Dark Web

☐ Custom (Internal Integration)
Generate

Configuring Settings in the Autotask Portal

Modify the Required HR Tab

This tab is required for integration setup.

Set the “**Resource Type**” and “**Payroll Type**” to what makes the most sense for your organization.

Under the “**Internal Cost (Burden Rate)**” section set:

Internal Cost: \$0.00

RESOURCE MANAGEMENT - Secure Now ★ ?

Save & Close Save Save & Copy Cancel Tabs with * contain required fields

General * Security * **HR *** Approvers * Associations * Skills Attachments

Resource Type *
 Contractor

Payroll Type *
 Contractor

Hire Date *
 05/23/2019

Payroll Identifier

Timesheet Start Date *
 05/23/2019

Accounting Reference ID

DAILY AVAILABILITY

Sun	Mon	Tue	Wed	Thu	Fri	Sat	Total
0.00	8.00	8.00	8.00	8.00	8.00	0.00	40.000

Weekly Billable Hours Goal
 0.00

Travel Availability

TIME OFF

Time Off Policy
 None

Effective Date *
 05/23/2019

[view all/manage associated policies](#)

	Additional Time	Annual
Vacation	0.000	0.000
Personal Time	0.000	0.000
Sick Time	0.000	0.000
Floating Holiday	0.000	0.000

	Additional Time	Annual
Vacation	0.000	0.000
Personal Time	0.000	0.000
Sick Time	0.000	0.000
Floating Holiday	0.000	0.000

Annual time represents what a resource may accrue through out the year or receive on January 1st. Time off is not pro-rated for new hires.

INTERNAL COST (BURDEN RATE)

+ New OK Cancel

Start Date ^	End Date	Hourly Rate
		\$0.00

Configuring Settings in the Autotask Portal

Modify the Required Approvers Tab

This tab is required for integration setup.

Set the “**Timesheet Approvers**” and “**Expense Report Approvers**” to what makes the most sense for your organization.

RESOURCE MANAGEMENT - New (Adding a resource may result in additional fees) ★ ?

Save & Close Save Save & Copy Cancel Tabs with * contain required fields

General * Security * HR * **Approvers *** Associations * Skills Attachments

TIMESHEET APPROVERS

+ New OK Cancel

Resource Name ^	Approval Level
Pierce, Pamela** [approver for 12 resources]	Level 1 (First)

Note: Only one resource has to approve the timesheet at each selected approval level. If you do not wish to have multi-level timesheet approvers, set all approval levels to Level 1 (First).

EXPENSE REPORT APPROVERS

+ New OK Cancel

Resource Name ^
Pierce, Pamela** [approver for 11 resources]

Configuring Settings in the Autotask Portal

Modify the Required Associations Tab

This tab is required for integration setup.

Set the required values to what makes the most sense for your organization.

Select the **“Save & Close”** button to save your configuration settings.

RESOURCE MANAGEMENT - New (Adding a resource may result in additional fees) ★ ?

Save & Close Save Save & Copy Cancel Tabs with * contain required fields

General * Security * HR * Approvers * **Associations *** Skills Attachments

LINE OF BUSINESS

A Line of Business can be used to grant access or prevent access to data associated with Contracts, Tickets, Projects, etc. throughout Autotask. It can also be used as a filter on billing/invoicing, reporting and on a resource's Dashboard.

Not Associated

General > IT Services
General > Software Development

Associated

→
←

DEPARTMENTS

+ New OK Cancel

Department Name ^	Role Name	Default Department and Role	Department Lead	Active
Service	IT:Service Manager	✓		✓

SERVICE DESK QUEUES

+ New OK Cancel

Queue Name ^

There are no items to display

SERVICE DESK ROLES

+ New OK Cancel

Configuring Autotask Within the PII Protect Portal

Navigating to the Client View Screen

Actions: [New Client](#) [ESS Dashboard](#) [Configure Messages](#) [Dark Web Monitoring](#) [Switch to Manager](#) **EVA** [TEST DRIVE](#)

2

[Partner Resources](#) [Billing Report](#) [Search](#)

Name	Product Type	Insurance	Manager Code	Employee Code	RA Completed	Registered Users 38/5000	Created	Password Breaches	Active	Actions
Client 1	EVA-MD	Print				0	05/30/19 9:28 pm	1806	Yes	View Edit Consolidate
Client 2	Unlimited Cybersecurity Training	N/A				0	06/04/19 9:56 am	41	Yes	View Edit
Client 3	Breach Prevention Platform (BPP)	Purchase			08/02/18	5	04/17/18 10:16 am	26	Yes	View Edit Consolidate

1. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged in you will be taken to your client list as the home screen (above).
2. Select “**Configure Messages**” to navigate to the Autotask PSA settings.

Configuring Autotask Within the PII Protect Portal

Configure Notification Settings

Home > Customized Messages Profile | Clients | Branded Information

Customized Messages

Actions:

Enter email address(es) to receive Contact Us notification
youremail@domain.com Save

If entering more than 1 email address, please separate with semicolon ';' (no spaces between addresses)
If no email(s) entered, or all have been removed, you will not receive these notifications

Choose PSA system for Integration: **3** Autotask

User Name Password **Connect** **4**

☐ Defer Sending Welcome Message 1 hours Save

Email address to receive directory synchronization errors ^{*}
youremail@domain.com × Save

3. Click the “**Choose PSA system for Integration**” dropdown and select “Autotask”
4. Enter the User Name and Password created on [page 4](#) and click “**Connect**”.

Once you hit Connect, our portal will connect to your Autotask PSA. There may be a delay for the configuration settings to appear.

Configuring Autotask Within the PII Protect Portal

Configure Notification Settings

Choose PSA system for Integration:

Autotask

6

Disconnect

5

☒ Auto Phish - Campaign Ending

☒ Auto Phish - Campaign Notification

☒ Dark Web Monitoring - Breach Report

☒ Dark Web Monitoring - Large Breach Notice

☐ Directory Sync - Digest

☐ Email - Bounced Report

☐ Email - Not Delivered Report

☐ Email - Spam Report

☐ Email - Unsubscribed Report

☐ Purchase - Notification

Select Associated Queue

Select Associated Queue

Select Associated Queue

Dark Web Alerts

Select Associated Queue

Select Associated Queue

Select Associated Queue

Select Associated Queue

Select Associated Queue

Select Associated Queue

☐ Enable Email Notification

☐ Enable Email Notification

☐ Enable Email Notification

☐ Enable Email Notification

☒ Enable Email Notification

☒ Enable Email Notification

☒ Enable Email Notification

☒ Enable Email Notification

☒ Enable Email Notification

☒ Enable Email Notification

7

8

Save Associations

Not sure which notification to setup?

Jump to [pages 13 – 14](#) for more details on the notifications and their descriptions.

Once Autotask has connected to the PII Protect portal, you will be able to configure notification settings.

5. Click the **checkbox** next to the notification(s) you would like to enable. For more details on these notification settings and descriptions, see [page 13](#).
6. Click the **“Select Associated Queue”** dropdown next to the desired notification to associate it with a pre-existing queue from Autotask.
7. If you would NOT like to receive an email notification in addition to the Autotask notification, uncheck the **“Enable Email Notification”** box next to the associated notification.
8. Click **“Save Association”** to save your changes.
9. Jump to [page 15](#) for client notification setup.

Configuring Autotask Within the PII Protect Portal

Configure Notification Settings – Notification Details & Descriptions

5

Choose PSA system for Integration:

Autotask

Disconnect

☒ Auto Phish - Campaign Ending

☒ Auto Phish - Campaign Notification

☒ Dark Web Monitoring - Breach Report

☒ Dark Web Monitoring - Large Breach Notice

☐ Directory Sync - Digest

☐ Email - Bounced Report

☐ Email - Not Delivered Report

☐ Email - Spam Report

☐ Email - Unsubscribed Report

☐ Purchase - Notification

Select Associated Queue

Enable Email Notification

Select Associated Queue

Enable Email Notification

Select Associated Queue

Enable Email Notification

Dark Web Alerts

Enable Email Notification

Select Associated Queue

Enable Email Notification

Select Associated Queue

Enable Email Notification

Select Associated Queue

Enable Email Notification

Select Associated Queue

Enable Email Notification

Select Associated Queue

Enable Email Notification

Select Associated Queue

Enable Email Notification

Save Associations

AutoPhish – Campaign Ending: Get an alert when a scheduled AutoPhish phishing campaign has ended.

AutoPhish – Campaign Notification: Get an alert 2 days before a scheduled AutoPhish phishing campaign is about to be initiated.

Dark Web Monitoring – Breach Report: Get an alert when your customer has been involved in a data breach

Dark Web Monitoring – Large Breach Notice: Running a scan on a domain with over 5,000 results takes a few moments to process. Get notified once your large breach report is ready.

Directory Sync – Digest: Get a summary report of your Azure AD, On-Premise, or Bulk Upload results and any associated errors.

Details & descriptions continued on next page.

Configuring Autotask Within the PII Protect Portal

Configure Notification Settings – Notification Details & Descriptions

Choose PSA system for Integration: Autotask

Disconnect

<input checked="" type="checkbox"/> Auto Phish - Campaign Ending	Select Associated Queue	<input type="checkbox"/> Enable Email Notification
<input checked="" type="checkbox"/> Auto Phish - Campaign Notification	Select Associated Queue	<input type="checkbox"/> Enable Email Notification
<input checked="" type="checkbox"/> Dark Web Monitoring - Breach Report	Select Associated Queue	<input type="checkbox"/> Enable Email Notification
<input checked="" type="checkbox"/> Dark Web Monitoring - Large Breach Notice	Dark Web Alerts	<input type="checkbox"/> Enable Email Notification
<input type="checkbox"/> Directory Sync - Digest	Select Associated Queue	<input checked="" type="checkbox"/> Enable Email Notification
<input type="checkbox"/> Email - Bounced Report	Select Associated Queue	<input checked="" type="checkbox"/> Enable Email Notification
<input type="checkbox"/> Email - Not Delivered Report	Select Associated Queue	<input checked="" type="checkbox"/> Enable Email Notification
<input type="checkbox"/> Email - Spam Report	Select Associated Queue	<input checked="" type="checkbox"/> Enable Email Notification
<input type="checkbox"/> Email - Unsubscribed Report	Select Associated Queue	<input checked="" type="checkbox"/> Enable Email Notification
<input type="checkbox"/> Purchase - Notification	Select Associated Queue	<input checked="" type="checkbox"/> Enable Email Notification

Save Associations

Purchase – Notification: Get notified when one of your Partner Administrators makes a purchase in the portal

Email delivery notifications for automated security tip or welcome emails:

Email Bounced Report: Receive a notification each time an email bounces, contains user details.

Email Not Delivered Report: Receive a notification each time an email cannot be delivered, contains user details.

Email Spam Report: Receive a notification when a user marks an email as spam, contains user details.

Email Unsubscribed Report: Receive a notification when a user unsubscribes from the email list, contains user details.

This can be turned back on in the portal.

1. On the client list (home screen) click “**View**” on the Client account the user is associated with.
2. Scroll down to the **User Details** table
3. Click **Edit** on the unsubscribed user, uncheck the “**Don't send Micro-Training/Monthly Newsletter**” and click **Submit** to re-subscribe them.

Autotask Client Configuration

Setup Autotask Notifications for a Client

Clients

Actions: [New Client](#) [ESS Dashboard](#) [Configure Messages](#) [Dark Web Monitoring](#) [Switch to Manager](#) **EVA** **TEST DRIVE**

[Partner Resources](#) [Billing Report](#) [Search](#)

Name	Product Type	HSN Branding	SRA Consulting	Insurance	Manager Code	Employee Code	RA Completed	Registered Users 49/5000	Created	Password Breaches	Active	Actions
Test EVA MD Client Update	EVA MD	No	No	Print				0	05/30/19 9:28 pm	2230	Yes 1	View Edit Autotask Consolidate
Test Cleint Update	HIPAA Compliance	No	No	Print				4	06/04/19 9:56 am	46	Yes	View Edit Autotask
Test UT Client Upgrade	Unlimited Cybersecurity Training	No	No	N/A				5	04/17/18 10:16 am	26	Yes	View Edit Autotask

1. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged in you will be taken to your client list as the home screen (above).
2. Under the “Actions” column, click the “**Autotask**” button for a client you’d like to configure Autotask notifications for.

Autotask Client Configuration

Setup Autotask Notifications for a Client

The screenshot shows the 'Autotask Client Associations' modal window. It contains the following elements with numbered callouts:

- 3**: A checkbox labeled 'Enable Autotask PSA' which is checked.
- 4**: A text input field labeled 'Enter Client'.
- 5**: A dropdown menu labeled 'Select template to test' with 'Select Template' as the current selection.
- 6**: A blue button labeled 'Test'.

3. Click the “**Enable Autotask PSA**” checkbox to configure and test the notification settings for this client.
4. Click the “**Enter Client**” dropdown to sync your PII Protect client account with the associated Client Name in Autotask. This list will populate based off client accounts already setup in your Autotask console.
5. Click the “**Select Template**” dropdown to choose the notification type you would like to test.
6. Click “**Test**” to send a test notification to your Autotask PSA system!

That’s it! You’ve just configured Autotask notification for this client! Repeat steps 2 – 6 on [pages 13 – 14](#) for each client you wish to setup!

The Autotask button on the home screen will be outlined in green for each client that has been successfully configured (see page 13 for example of home screen and Autotask button).



You're All Set!

_____ Your Autotask PSA Integration Setup is complete!

_____ Questions? Comments? Want a 1-on-1 onboarding with our Operations team?

Email: Operations@breachsecurenow.com

Phone: (877) 275 – 4545