

Intrusion Detection

with

Login Locator

for

Salesforce.com

Lite Version 1.1

User Guide

Contents

Installation/Settings..... 3

 Prerequisites 3

 Installation Steps..... 3

 Settings..... 7

 Risk Points..... 9

Login Histories..... 10

Login Maps..... 13

 Current Login Map 13

 24 Hour Login Map..... 14

Risk Console 15

Session Snapshot 16

Installation/Settings

The application can be installed directly from the Salesforce.com AppExchange. It will install directly into your production instance or sandbox.

Prerequisites

This product will work with all versions of Force.com or Salesforce.com because it works with the common login information. It requires that you are running Summer 2015 or later.

Installation Steps

1. After clicking the link to install the application, choose "Install for Admins Only", and click Install.

Home Environment Hub +

Install IDSlite

By Dev1

Install for Admins Only

Install for All Users

Install for Specific Profiles...

Install **Cancel**

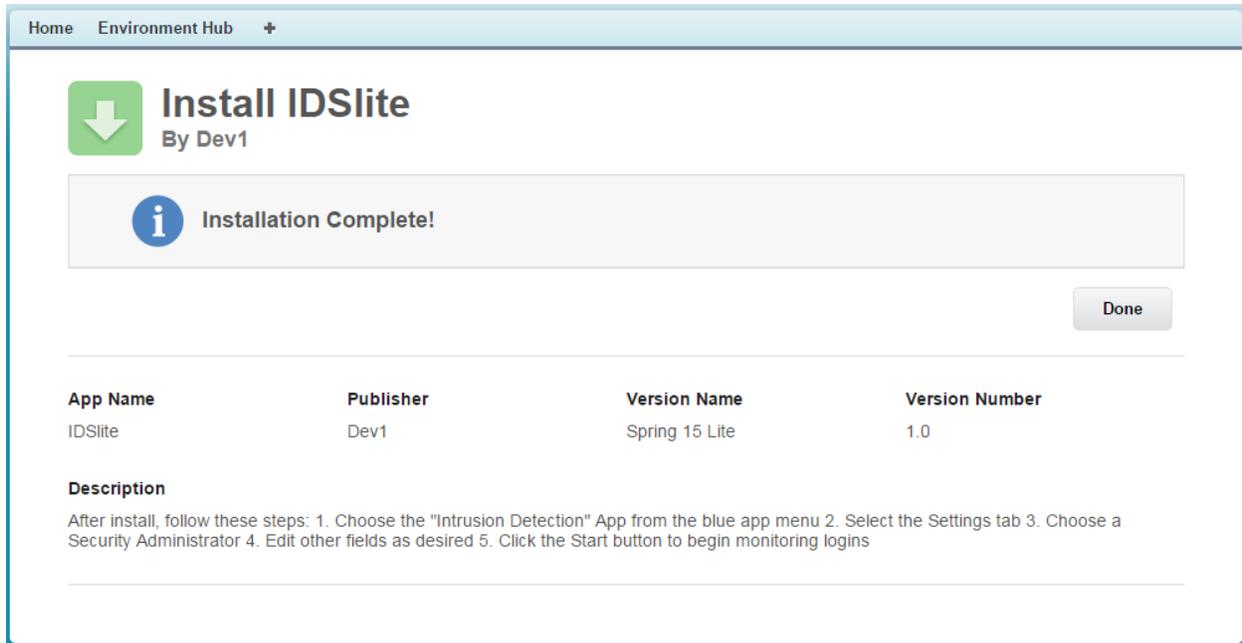
App Name	Publisher	Version Name	Version Number
IDSlite	Dev1	Spring 15 Lite	1.0

Description

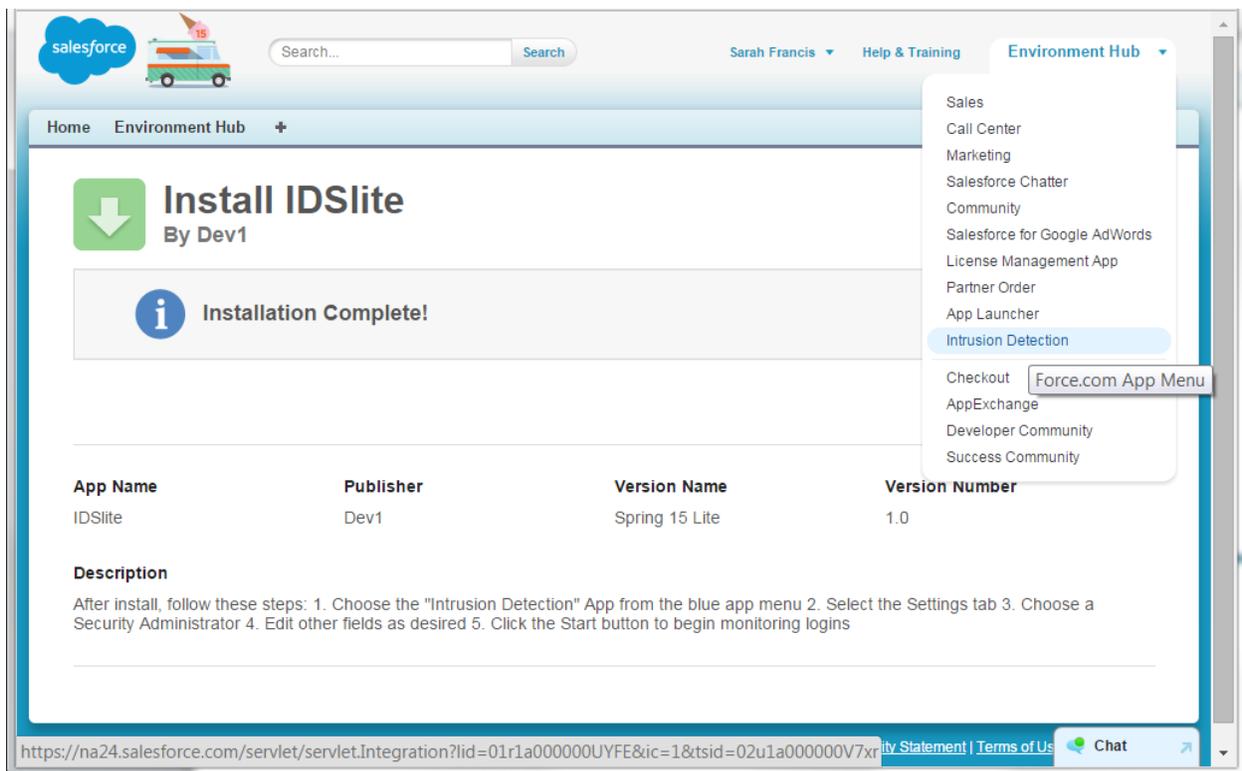
After install, follow these steps: 1. Choose the "Intrusion Detection" App from the blue app menu 2. Select the Settings tab 3. Choose a Security Administrator 4. Edit other fields as desired 5. Click the Start button to begin monitoring logins

Additional Details [View Components](#) [API Access](#)

2. After installation is complete, click Done.



3. Next, from the Application Selection menu in the top right corner, choose "Intrusion Detection".



4. After selecting the "Intrusion Detection" app, click on the Settings tab.

The screenshot displays the 'Intrusion Detection Settings' interface. The top navigation bar includes 'Home', 'Current Login Map', '24 Hour Login Map', 'Risk Console', 'Login Histories', 'Session Snapshot', and 'Settings'. The 'Settings' tab is active, showing the following sections:

- General Settings:**
 - Security Administrator: [Empty field] Choose a security administrator to receive notifications.
 - Version: Lite 1.0
 - Login Table Age: 60 After this many days, age out old login history information.
 - Scan Logfile Interval: 10 How many minutes between batch processing of logins and taking session snapshots?
 - Failed Logins Per Hour: 3 After this many failed logins, alert the administrator.
 - Email Notification Threshold: 10 After this many accumulated risk points, alert the administrator.
 - Only Last Login on 24: On 24 Hour Login map, only show last login at each ip address, filters multiple logins.
- Restart Service:**
 - Restart Login Processing Service
 - Scheduled Login Processing Service: NOT Running, please restart.
- Rules:**
 - Rule Accumulate Risk Point for Users: 1. Accumulate risk points for users?
 - Rule City Blank: 2. If Location Provider does not provide city information disregard distance calculations and GPS coordinates?
 - Rule Country Day: 3. Alert if User performs login in two different countries on the same day?
 - Rule Distance Speed: 4. Monitor distance and time (speed in mph) between logins?
 - Rule Failed Logins: 5. Monitor failed login attempts?
 - Rule Is Admin: 6. Monitor System Administrator logins?

- Before you can start monitoring logins, you must fill out all of the fields in the General Settings section of the Settings tab. All of the settings will have a default value except for the Security Administrator. You must select a Security Administrator before continuing. The Security Administrator is the user which will receive all of the Login Security Notification emails.

The screenshot displays the 'Intrusion Detection Settings' page in the Idaho Palm Software interface. The page is organized into several sections:

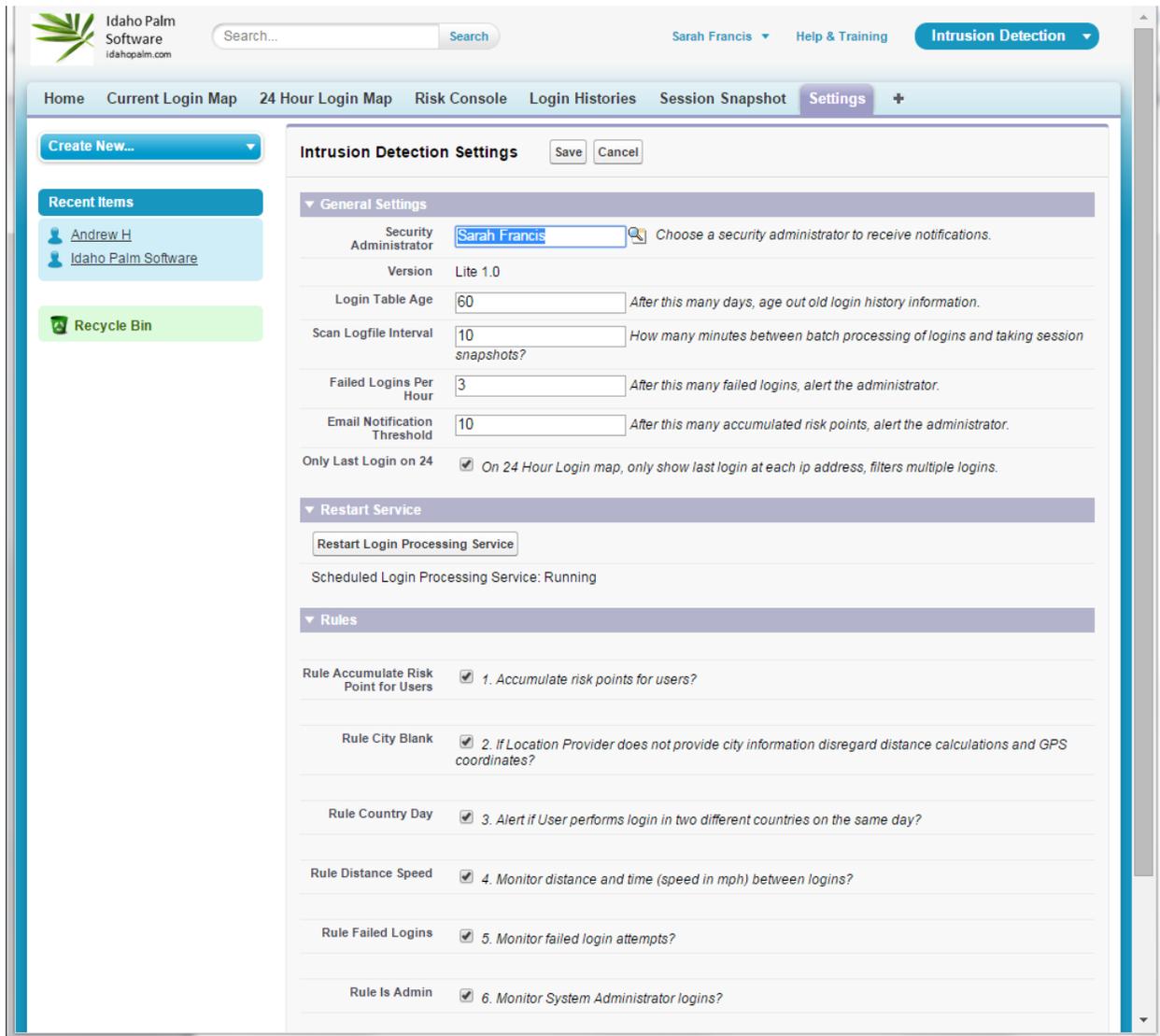
- General Settings:** Includes fields for Security Administrator (Sarah Francis), Version (Lite 1.0), Login Table Age (60), Scan Logfile Interval (10), Failed Logins Per Hour (3), and Email Notification Threshold (10). There is also a checkbox for 'Only Last Login on 24' which is checked.
- Restart Service:** Features a 'Restart Login Processing Service' button and a status message: 'Scheduled Login Processing Service: NOT Running, please restart.'
- Rules:** Lists five rules, all of which are checked:
 - Rule Accumulate Risk Point for Users: 1. Accumulate risk points for users?
 - Rule City Blank: 2. If Location Provider does not provide city information disregard distance calculations and GPS coordinates?
 - Rule Country Day: 3. Alert if User performs login in two different countries on the same day?
 - Rule Distance Speed: 4. Monitor distance and time (speed in mph) between logins?
 - Rule Failed Logins: 5. Monitor failed login attempts?

6. After choosing the Security Administrator, then click the “Save” button. Then click the “Restart Login Processing Service”, which is now active.

The next section will describe each of the other options listed on the settings page, so that you can customize the application according to your security and notification preferences.

Settings

This section will describe each of the settings that can be set on the Settings Tab.



The screenshot shows the 'Intrusion Detection Settings' page in the Idaho Palm Software application. The interface includes a top navigation bar with 'Home', 'Current Login Map', '24 Hour Login Map', 'Risk Console', 'Login Histories', 'Session Snapshot', and 'Settings'. The 'Settings' tab is active. On the left, there is a sidebar with 'Create New...', 'Recent Items' (listing Andrew H and Idaho Palm Software), and a 'Recycle Bin'. The main content area is titled 'Intrusion Detection Settings' and contains three sections: 'General Settings', 'Restart Service', and 'Rules'. The 'General Settings' section includes fields for 'Security Administrator' (Sarah Francis), 'Version' (Lite 1.0), 'Login Table Age' (60), 'Scan Logfile Interval' (10), 'Failed Logins Per Hour' (3), and 'Email Notification Threshold' (10). There is also a checkbox for 'Only Last Login on 24'. The 'Restart Service' section has a 'Restart Login Processing Service' button and shows the service is 'Running'. The 'Rules' section lists six rules, all of which are checked: 'Accumulate Risk Point for Users', 'City Blank', 'Country Day', 'Distance Speed', 'Failed Logins', and 'Is Admin'.

Security Administrator – This is the chosen person who will receive all notification emails from the app. The notifications will automatically be sent to the email address associate with the user specified here.

Login Table Age – represents the number of days of login data to keep in the Login Histories tab. The default setting is 60 days.

Scan Logfile Interval – If you keep the default setting of 10, the intrusion detection service will run every 10 minutes to monitor users logins. It is recommended that you set this between 5 and 60 minutes, keep in mind if it were set to 60 minutes, it could possibly be 60 minutes before the app sends a desired security notification.

Failed Logins per Hour – This is the number of failed logins per hour to alert on. The default setting is 3, therefore if someone fails 4 login attempts in a one hour period it will send a Failed Login Attempts Notification to the Security Administrator.

Email Notification Threshold – This is the number of risk points to accumulate per login before sending the Security Administrator a Risk Notification email. The default value is set very low, to 10, and it should be adjusted according to the rules that are chosen in the Rules section. This could be set from 10 to 10,000 or higher. It all depends upon the threshold and the amount interaction that the Security Administrator wants to engage.

Only Last Login on 24 – If this box is checked, the 24 Hour Login map will only show one location for a user if that user logs in multiple times at the same location. This helps the 24 Hour Login map from becoming too cluttered. If you want to see absolutely every login, even when a user logs in multiple times from the same IP address and location, then uncheck this box. The default value is checked.

Restart Login Processing Service Button – this button will be inactive(unclickable) if any of the fields in the General Settings section are blank. Below the button the text will tell you the current status of the service. It will either be running to stopped. If you have stopped the service for any reason, such as for an upgrade or something, you will need to restart the service here.

Rule Accumulate Risk Point for Users – If checked, this enables the tallying of risk points for users, and enables the Risk Notification email to be sent to the Security Administrator if the threshold set in “Email Notification Threshold” setting is passed. If unchecked, this will disable the Risk Notification emails. The default value is checked.

Rule City Blank – If checked, then the risk calculations will disregard calculated risk distance for the Login History entries where the City is unknown. Sometimes IP location data does not have a specific city for the login. For example, if a user is flying on an airplane and logs in most of those IP addresses are set to USA, and no state or city. If checked, this filters out these logins from using distance calculations. The default value is checked.

Rule Distance Speed - if checked, this enable the risk points to calculate the distance between the current login and the previous login, as well as the time difference in order to calculate the speed in miles per hour between logins. This helps to alert administrators if, for example someone were to login in Los Angeles and 10 minutes later login from New York. If your company uses VPNs you may want to disable this setting to avoid false positives. If the speed between logins is greater than 60mph it will add 5 risk points for the login. The default value for this setting is checked.

Rule Failed Logins – if checked, then once a user passes the “Failed Logins Per Hour” threshold, an automatic Failed Logins Notification email will be sent to the Security Administrator. To disable these emails, uncheck this box. The default setting is checked.

Rule Is Admin – if checked, then the system will automatically assign 1 risk point to each user that is a System Administrator for each of their logins. This causes the System Admin logins to “bubble up to the top” of the risk console and gives them higher visibility. The default setting is checked.

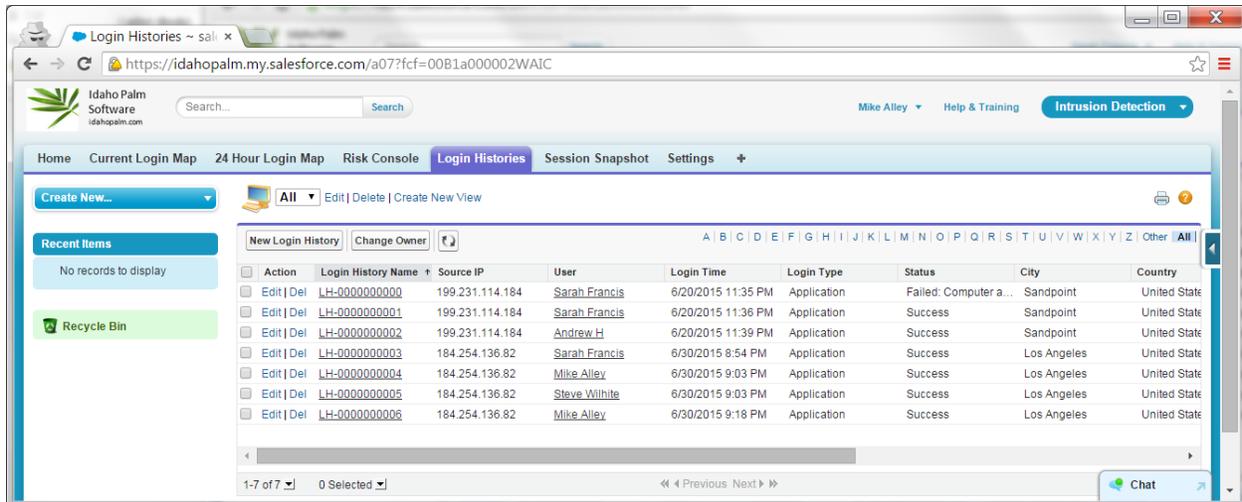
Risk Points

These are the established values for Risk points that accumulate for each login:

System Admin Login	+1
Speed between logins > 60mph	+5
Login from a different country in same day	+20
Failed logins per hour threshold exceeded	+10(times number of times process runs per hour)

Login Histories

The Login Histories tab allows Security Administrators to view a table of all logins. By clicking on the “All” view and the “Go” button, you can see a history of logins.



The screenshot displays the Salesforce interface for the 'Login Histories' tab. The page includes a navigation bar with tabs for 'Home', 'Current Login Map', '24 Hour Login Map', 'Risk Console', 'Login Histories', 'Session Snapshot', and 'Settings'. The 'Login Histories' tab is active, and the 'All' view is selected. The main content area shows a table of login records with columns for Action, Login History Name, Source IP, User, Login Time, Login Type, Status, City, and Country. The table contains seven rows of data, including failed and successful login attempts for users Sarah Francis, Andrew H, Mike Alley, and Steve Wilhite.

Action	Login History Name	Source IP	User	Login Time	Login Type	Status	City	Country
Edit Del	LH-0000000000	199.231.114.184	Sarah Francis	6/20/2015 11:35 PM	Application	Failed: Computer a...	Sandpoint	United State
Edit Del	LH-0000000001	199.231.114.184	Sarah Francis	6/20/2015 11:36 PM	Application	Success	Sandpoint	United State
Edit Del	LH-0000000002	199.231.114.184	Andrew H	6/20/2015 11:39 PM	Application	Success	Sandpoint	United State
Edit Del	LH-0000000003	184.254.136.82	Sarah Francis	6/30/2015 8:54 PM	Application	Success	Los Angeles	United State
Edit Del	LH-0000000004	184.254.136.82	Mike Alley	6/30/2015 9:03 PM	Application	Success	Los Angeles	United State
Edit Del	LH-0000000005	184.254.136.82	Steve Wilhite	6/30/2015 9:03 PM	Application	Success	Los Angeles	United State
Edit Del	LH-0000000006	184.254.136.82	Mike Alley	6/30/2015 9:18 PM	Application	Success	Los Angeles	United State

By clicking on a single line, in the Login History Name column, you can bring up the details for a particular login.

Idaho Palm Software
idahopalm.com

Search... Search

Mike Alley Help & Training Intrusion Detection

Home Current Login Map 24 Hour Login Map Risk Console **Login Histories** Session Snapshot Settings

Create New... Recent Items LH-0000000003 Recycle Bin

Login History LH-0000000003

Back to List: Login Histories Sessions [1]

Customize Page | Edit Layout | Printable View | Help for this Page

Login History Detail Edit Delete Clone Deactivate User

Risk Assessment

Relative Risk Level	1	Remarks	This account is a Systems Administrator. (+1 risk)
---------------------	---	---------	--

Summary

User	Sarah Francis	Login Time	6/30/2015 8:54 PM
Source IP	184.254.136.82	City State Country	Los Angeles, US
Login Type	Application	Status	Success

Details

Browser	Chrome 43	City	Los Angeles
Application	Browser	State	California
Platform	Windows 7	Country	United States
Time Zone	Upgrade to Full Version.	Country Code	US
Location	34°2'43"N 118°14'29"W	Zip Code	90013

Maxmind Information

Metro Code	Upgrade to Full Version.	is anonymous proxy	<input type="checkbox"/>
ISP	Upgrade to Full Version.	is satellite provider	<input type="checkbox"/>
Domain	Upgrade to Full Version.	Maxmind Queries Remaining	0
IP Organization	Upgrade to Full Version.		

This Login Compared to Previous Login

Distance from Last Login	987.14	Hours Since Previous Login	237.00
MPH Speed from Last Login	4.17	Last Failed Login Notification Time	
		Failed Logins in Past Hour	

Chat

The top portion of the Login History detail page shows the relevant data for this login.

The screenshot shows a Salesforce user profile page for 'Steve Wilhite'. The page is divided into several sections:

- Previous Login Attempts for this User:** A table with columns: Logins, Login Time, IP Address, Status, Location, Distance from Last Login, IP Organization, and Platform. It lists three login attempts: two successful ones from Los Angeles, US and Sandpoint, US, and one failed attempt from Sandpoint, US due to 'Computer activation required'.
- Failed Logins:** A table with the same columns as above, listing one failed login attempt from Sandpoint, US.
- User Information:** Shows 'Created By: Steve Wilhite, 6/30/2015 9:17 PM' and 'Last Modified By: Steve Wilhite, 6/30/2015 9:17 PM'. Below this are buttons for 'Edit', 'Delete', 'Clone', and 'Deactivate User'.
- Sessions:** A section with a 'New ip_Sessions' button and a 'Sessions Help' link. It contains a table with columns: Action, ip_Sessions Name, ISP, IP Organization, Login Type, Location, Session Type, Snapshot Time, is anonymous proxy, and is satellite provider. One session is listed with 'ip_Sessions Name: IPS=0000000031', 'ISP: Upgrade to Full Version.', 'IP Organization: Upgrade to Full Version.', 'Login Type: Application', 'Location: Los Angeles, California United States', 'Session Type: UI', and 'Snapshot Time: 6/30/2015 10:38 PM'.

At the bottom of the page, there is a 'Back To Top' link, a note 'Always show me more records per related list', and a 'Chat' button.

The bottom portion of the details page, has related logins and session information for this user. This allows you to see the recent login history of this user in one place. If fraud is detected, then Security Administrators may choose to click the “Deactivate User” button at the top of the page which will immediately cancel all sessions that the user is currently using, and prevent them from logging back in until a System Administrator goes to their User profile and make them “Active” again.

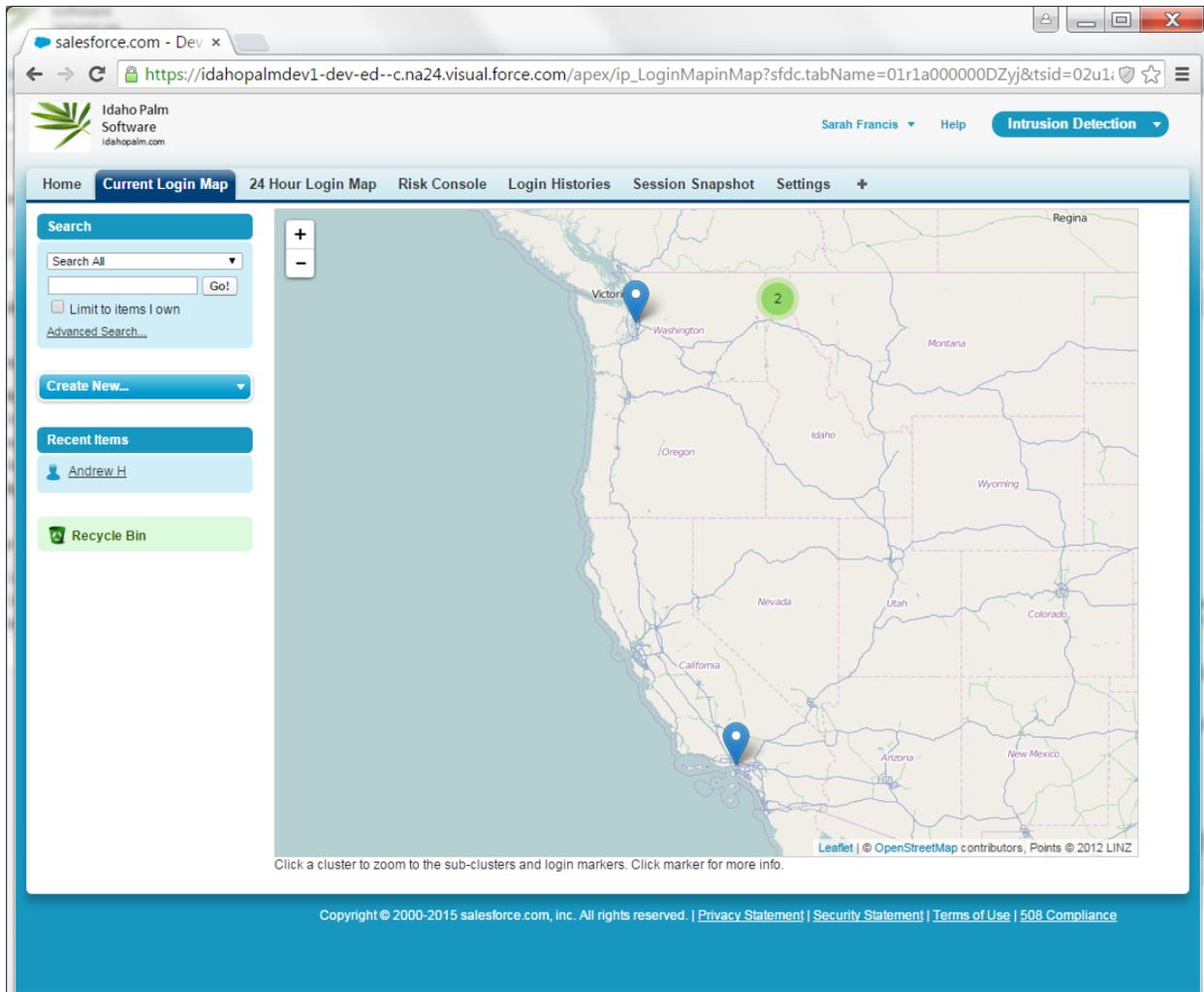
Also, if you click on a View link you can go directly to the login detail page for the referenced login.

Login Maps

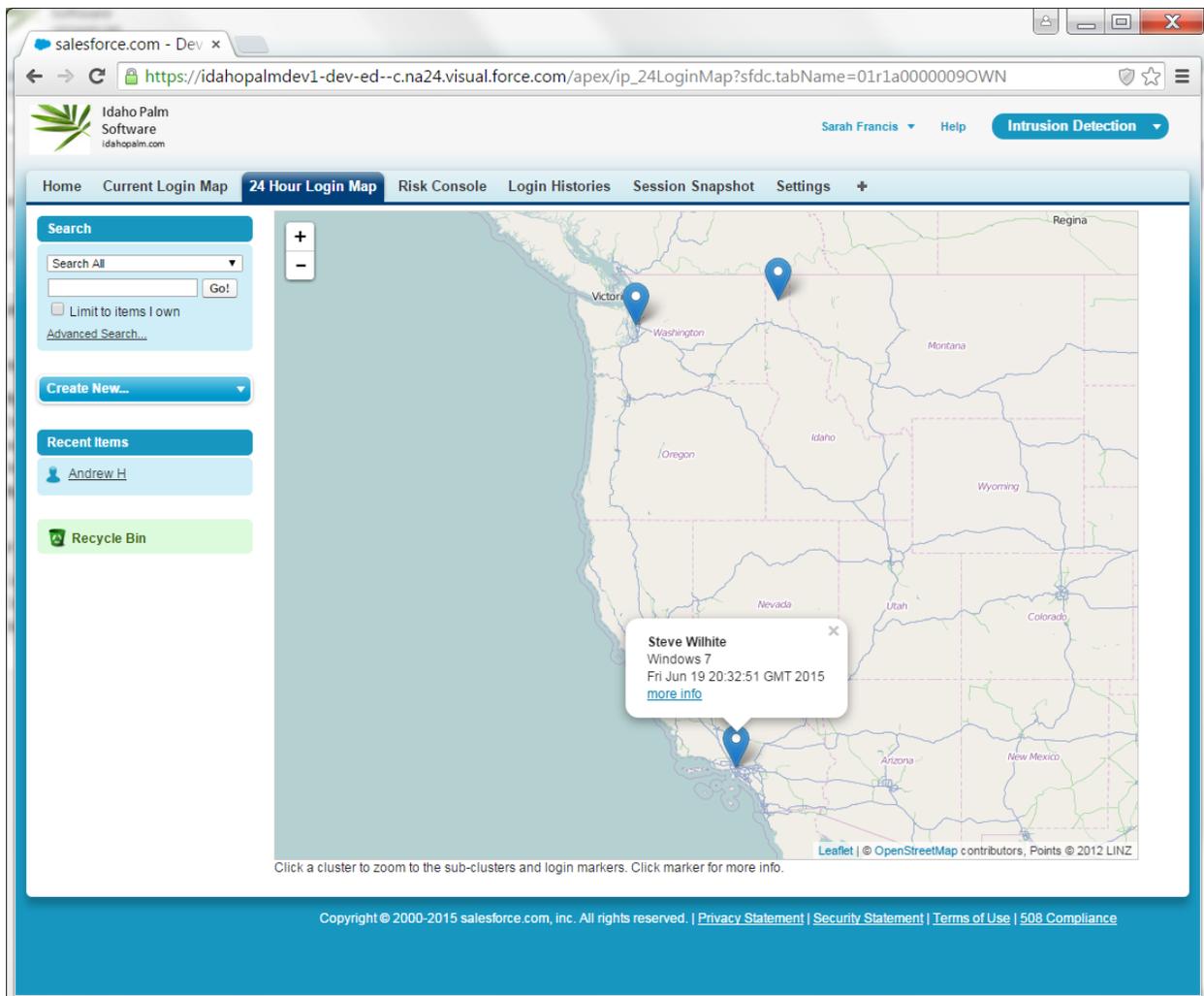
There are two Login map tabs. One will display the current users who are logged into the system, and the other shows user logins within the last 24 hours.

Current Login Map

The Current Login Map tab shows a map of all users currently logged into the system. It uses a clustering interface that helps to keep down the clutter on the map. If you click on a green cluster, then the map will zoom in and the underlying blue pins will become visible. Each blue pin represents a login.



Clicking on a blue pin will bring up some limited information about the login, but clicking on the view button will take you to the Login Histories tab and the login detail page for that login.



24 Hour Login Map

The 24 Hour Login Map tab works in similar fashion, however it will display logins that have happened over the last 24 hours. This provides a quick way to see if, for example, someone logged in from a foreign country over the past day.

Risk Console

The Risk Console tab displays all users with a cumulative risk level that is greater than zero. It displays them in descending risk level order. This allows Security Administrators to see the most suspect users at the top of the list. By clicking on the View link, it will bring up the last login detail page for that user, where a Security Administrator can choose to deactivate a user.

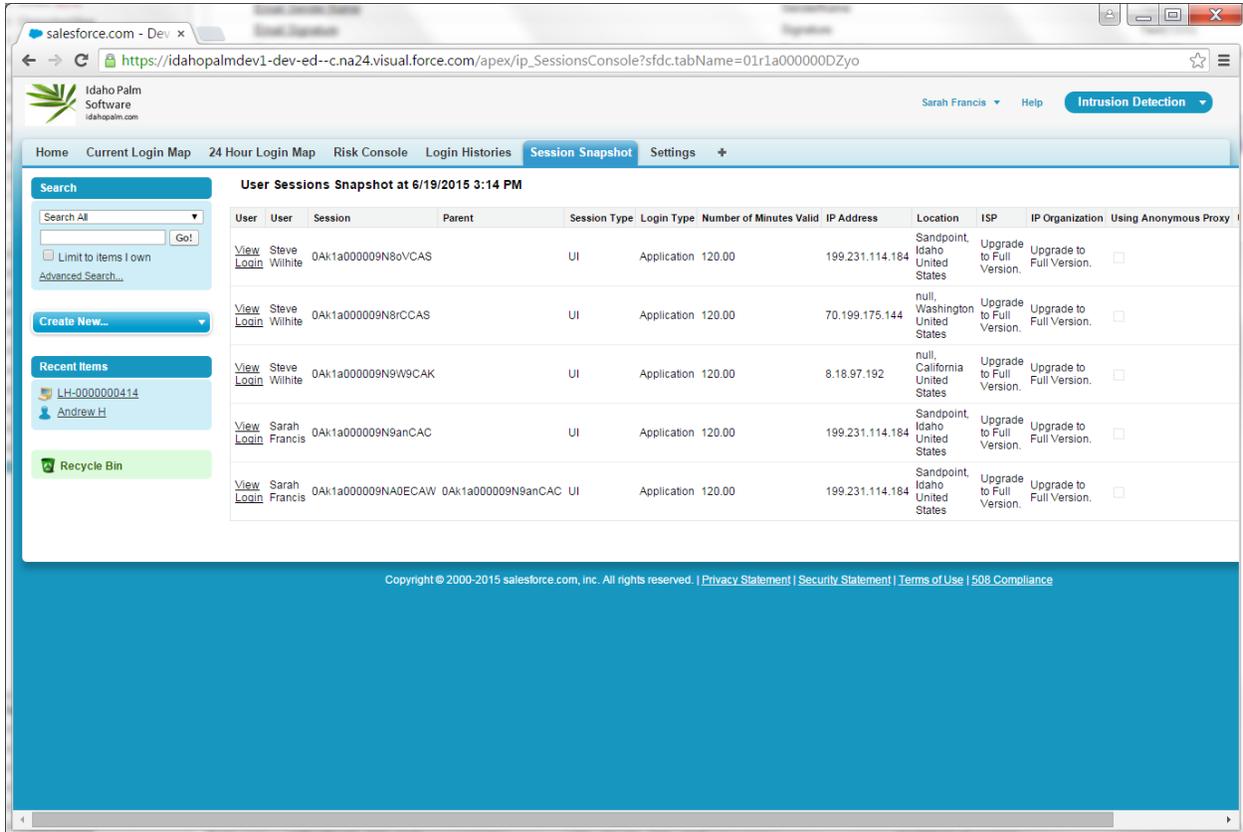
The screenshot shows the 'Intrusion Detection User Console' interface. The page includes a search bar, a 'Reset all Risk levels to Zero' button, and a table of users with their accumulated risk levels and last login details.

User	Accumulated Risk Level	Last Login	Last Login Time	Location
Steve Wilhite	58	View	6/19/2015 1:32 PM	California United States
Mike Alley	35	View	6/19/2015 1:24 PM	Sandpoint, Idaho United States
David Turvan	34	View	6/19/2015 1:26 PM	Sandpoint, Idaho United States
Sarah Francis	1	View	6/19/2015 1:34 PM	Sandpoint, Idaho United States

The “Reset all Risk levels to Zero” button will set all of the user levels back to zero. It is a good idea for Security Administrators to view this screen on a regular basis and then click the button after suspect logins have been investigated. Security Administrators will want to set the threshold in the Settings tab high enough to match their cadence of checking and resetting in this console.

Session Snapshot

The Session Snapshot tab is a table that lists what users are currently logged in right now. It is set to only show users that are logged in via a User Interface (not integration users).



The screenshot displays the Salesforce Session Snapshot interface. The page title is "User Sessions Snapshot at 6/19/2015 3:14 PM". The interface includes a search bar, a "Create New..." button, and a "Recent Items" section. The main table lists active sessions with the following columns: User, Session, Parent, Session Type, Login Type, Number of Minutes Valid, IP Address, Location, ISP, IP Organization, and Using Anonymous Proxy. The table contains five rows of session data.

User	Session	Parent	Session Type	Login Type	Number of Minutes Valid	IP Address	Location	ISP	IP Organization	Using Anonymous Proxy
View Login Steve Wilhite	0Ak1a000009N8oVCAS		UI	Application	120.00	199.231.114.184	Sandpoint, Idaho United States	Upgrade to Full Version.	Upgrade to Full Version.	<input type="checkbox"/>
View Login Steve Wilhite	0Ak1a000009N8rCCAS		UI	Application	120.00	70.199.175.144	null, Washington United States	Upgrade to Full Version.	Upgrade to Full Version.	<input type="checkbox"/>
View Login Steve Wilhite	0Ak1a000009N9W9CAK		UI	Application	120.00	8.18.97.192	null, California United States	Upgrade to Full Version.	Upgrade to Full Version.	<input type="checkbox"/>
View Login Sarah Francis	0Ak1a000009N9anCAC		UI	Application	120.00	199.231.114.184	Sandpoint, Idaho United States	Upgrade to Full Version.	Upgrade to Full Version.	<input type="checkbox"/>
View Login Sarah Francis	0Ak1a000009NA0ECAW	0Ak1a000009N9anCAC	UI	Application	120.00	199.231.114.184	Sandpoint, Idaho United States	Upgrade to Full Version.	Upgrade to Full Version.	<input type="checkbox"/>

A user may have multiple sessions per login, if they have multiple browser windows for example. There are a few fields show here which are only available in the "Full" version(coming soon) and not the "Lite" version.

To see Login History details for a particular session, click on the View Login links.