Intrusion Detection

with

Login Locator

for

Salesforce.com

Lite Version 1.1

User Guide

Contents

Installation/Settings

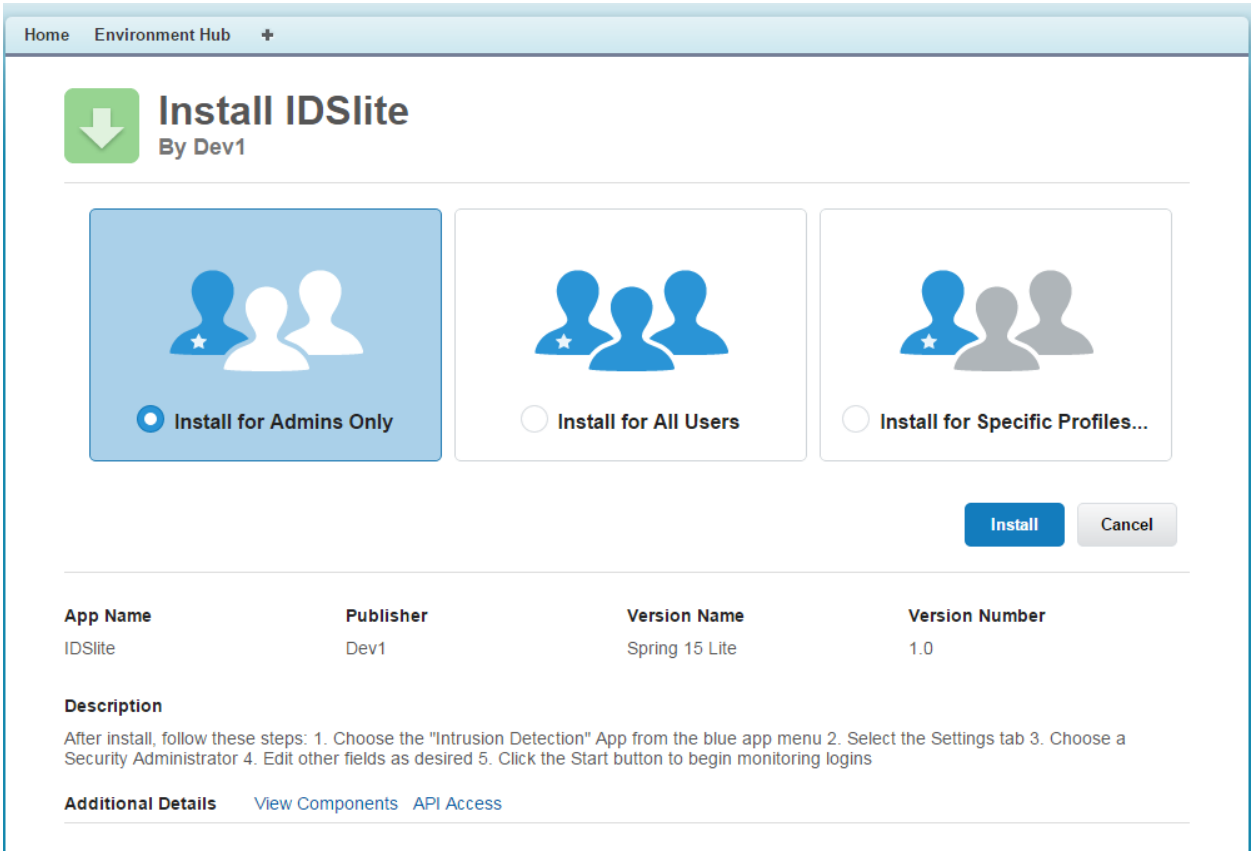
The application can be installed directly from the Salesforce.com AppExchange. It will install directly into your production instance or sandbox.

Prerequisites

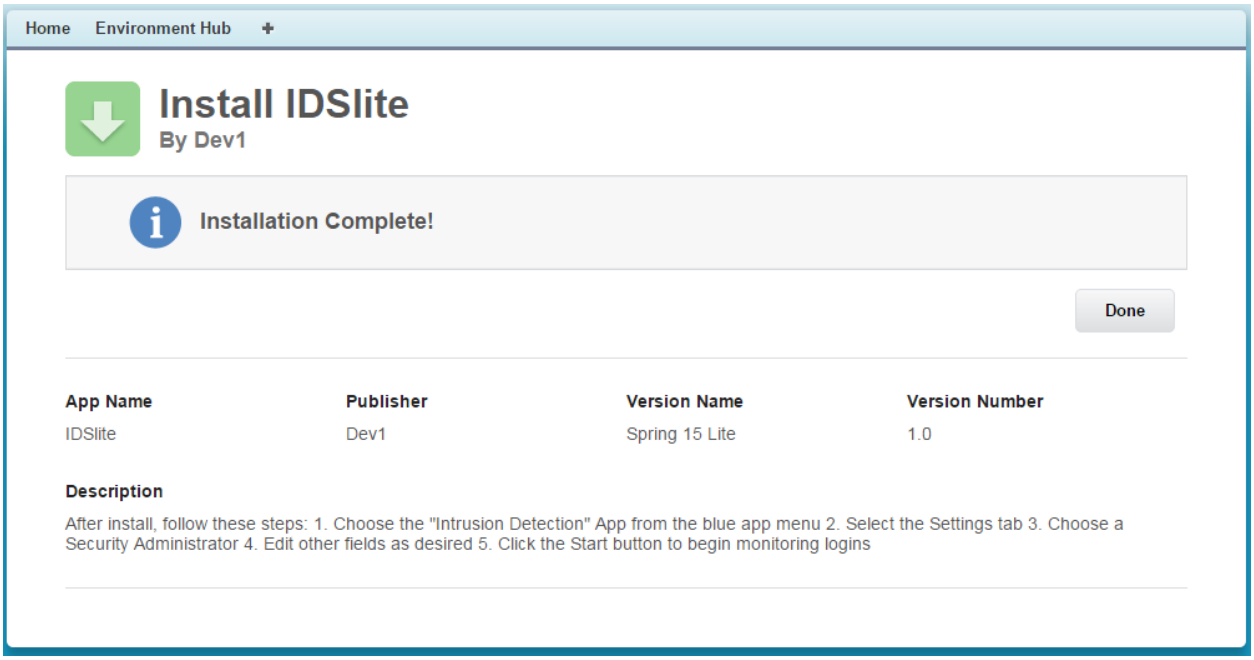
This product will work with all versions of Force.com or Salesforce.com because it works with the common login information. It requires that you are running Summer 2015 or later.

Installation Steps

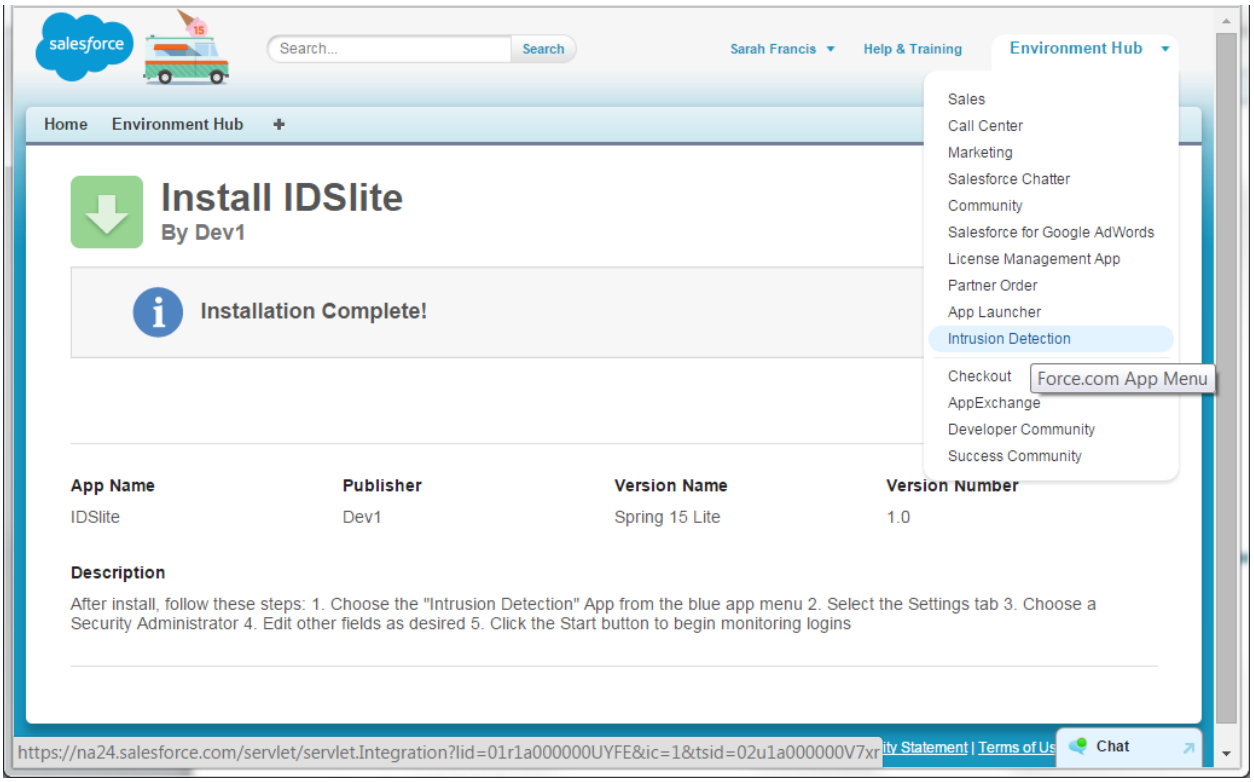
1. After clicking the link to install the application, choose “Install for Admins Only”, and click Install.



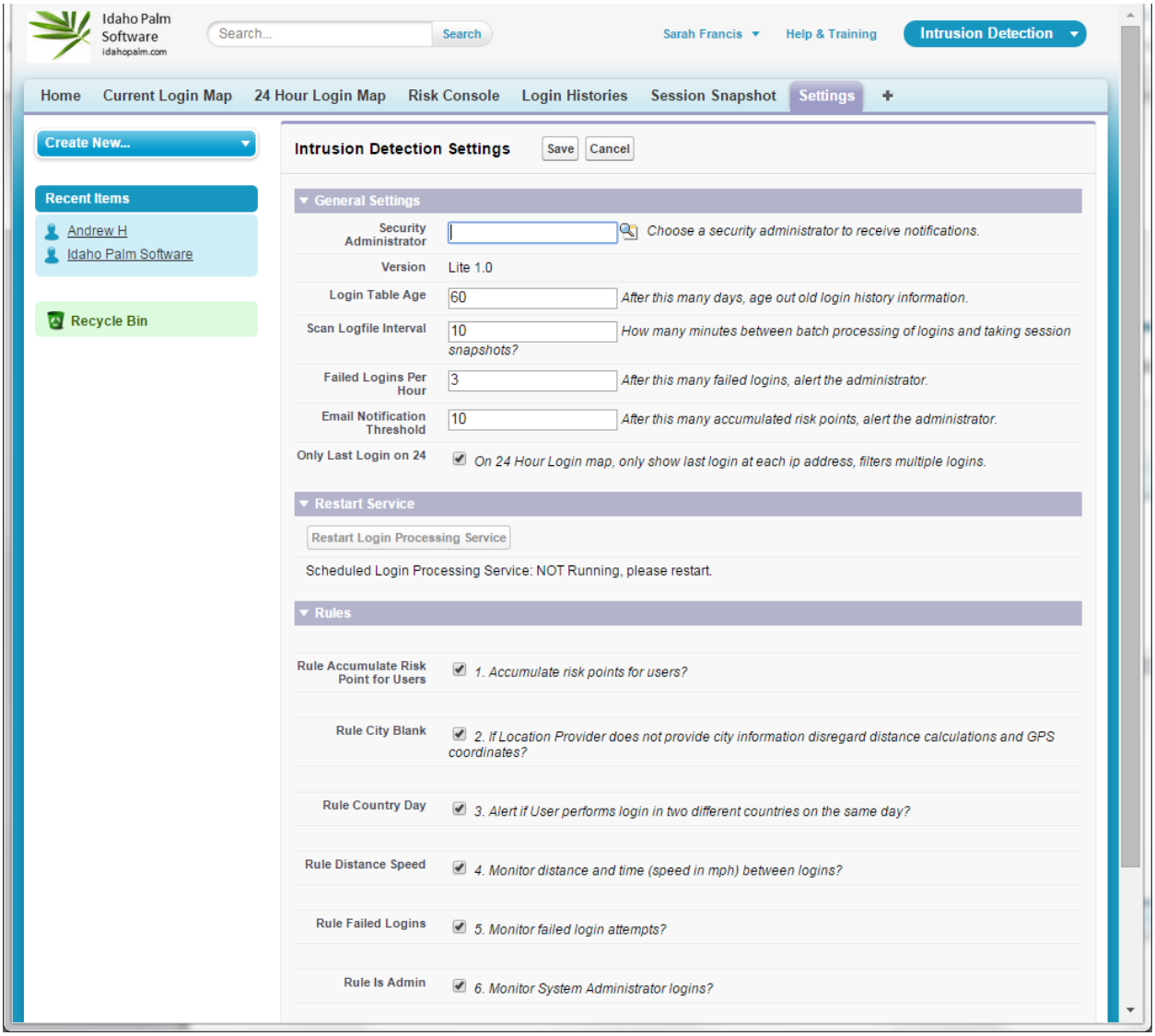
2. After installation is complete, click Done.



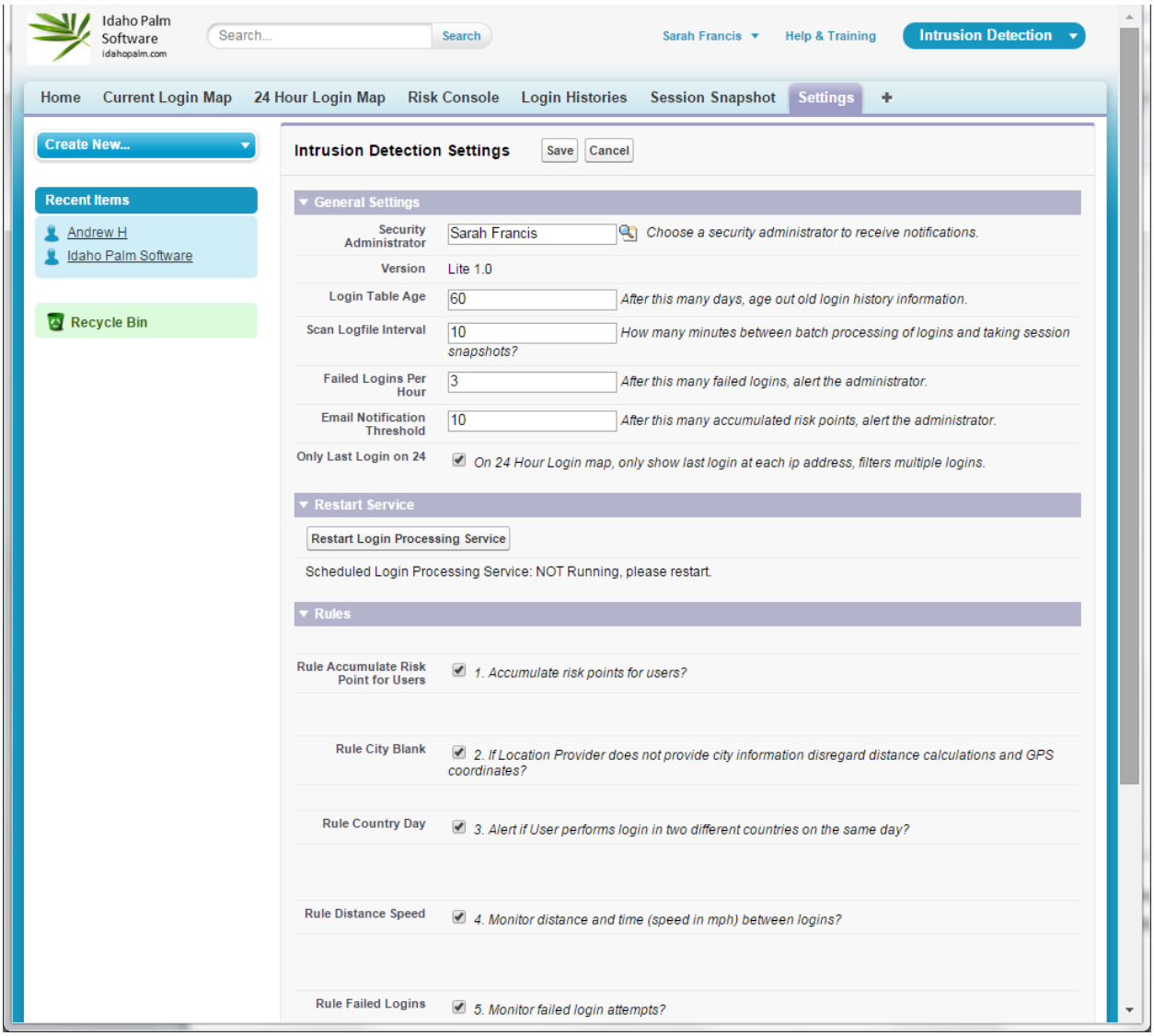
3. Next, from the Application Selection menu in the top right corner, choose “Intrusion Detection”.



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



5. 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.

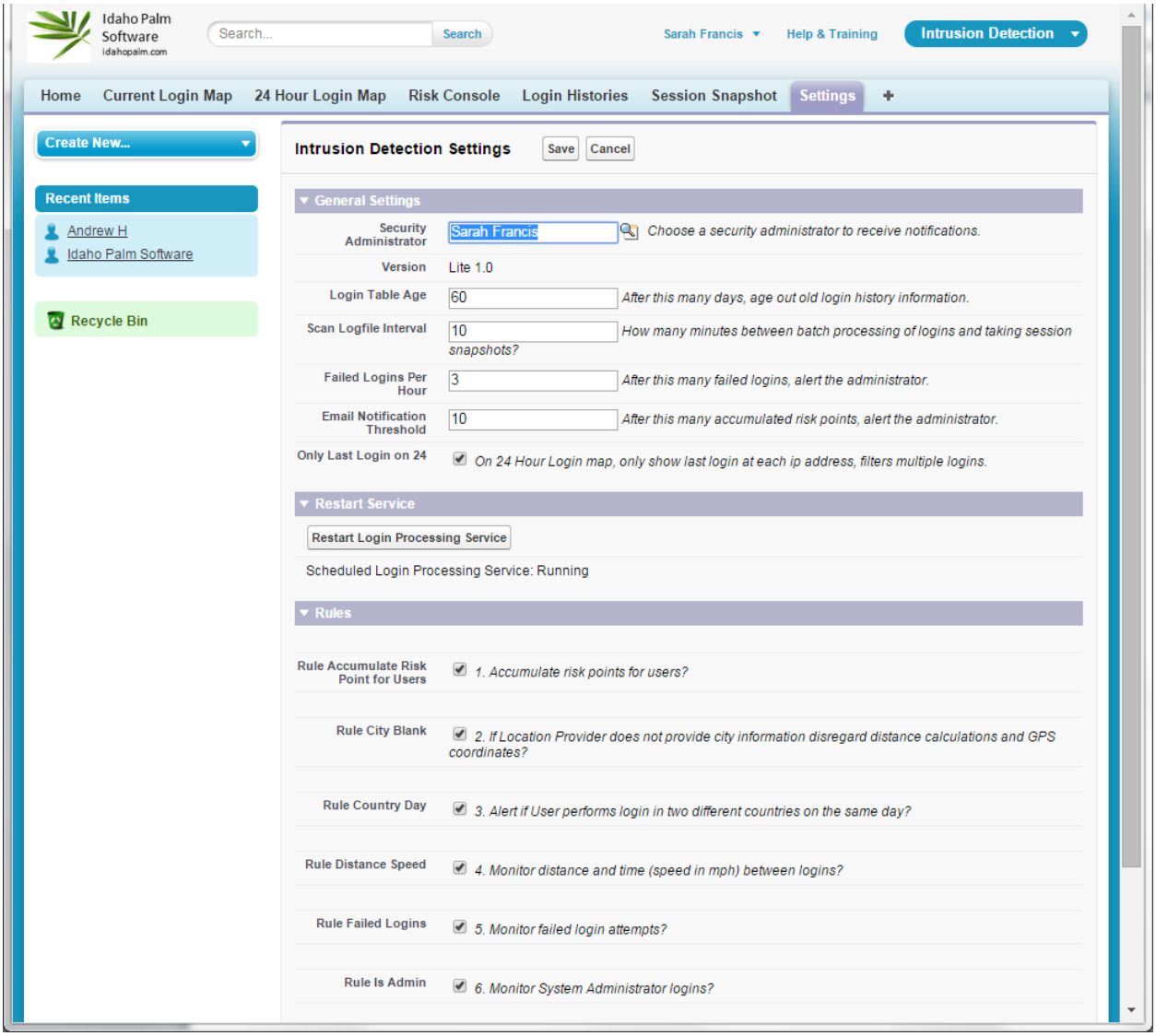


6. After choosing the Security Administrator, then click the “Save” button. Then click the “Restart Login Processing Service”, which is now active.

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.



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.

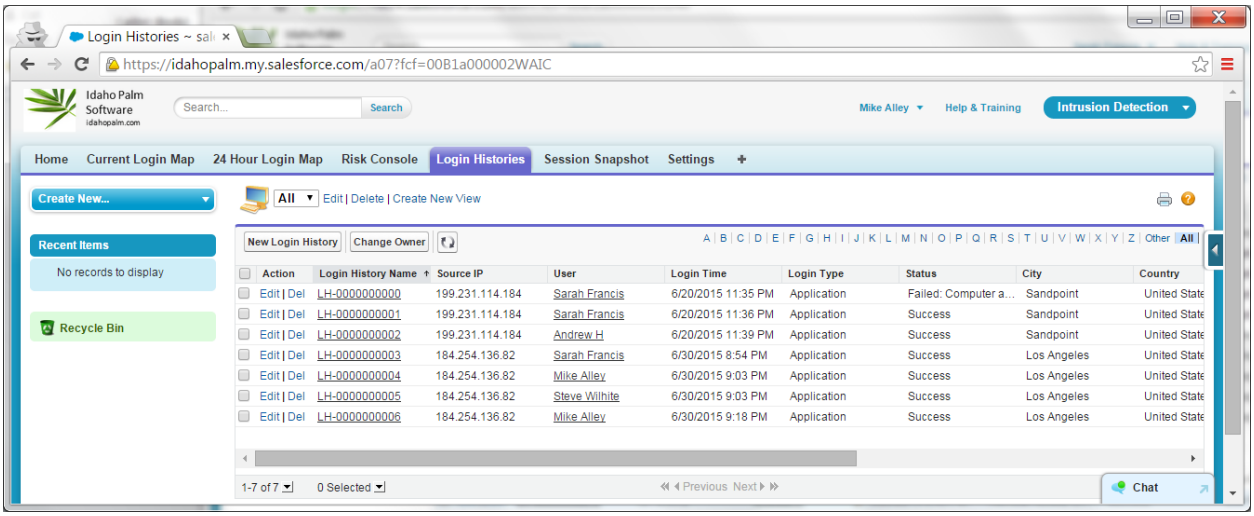
Risk Points

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

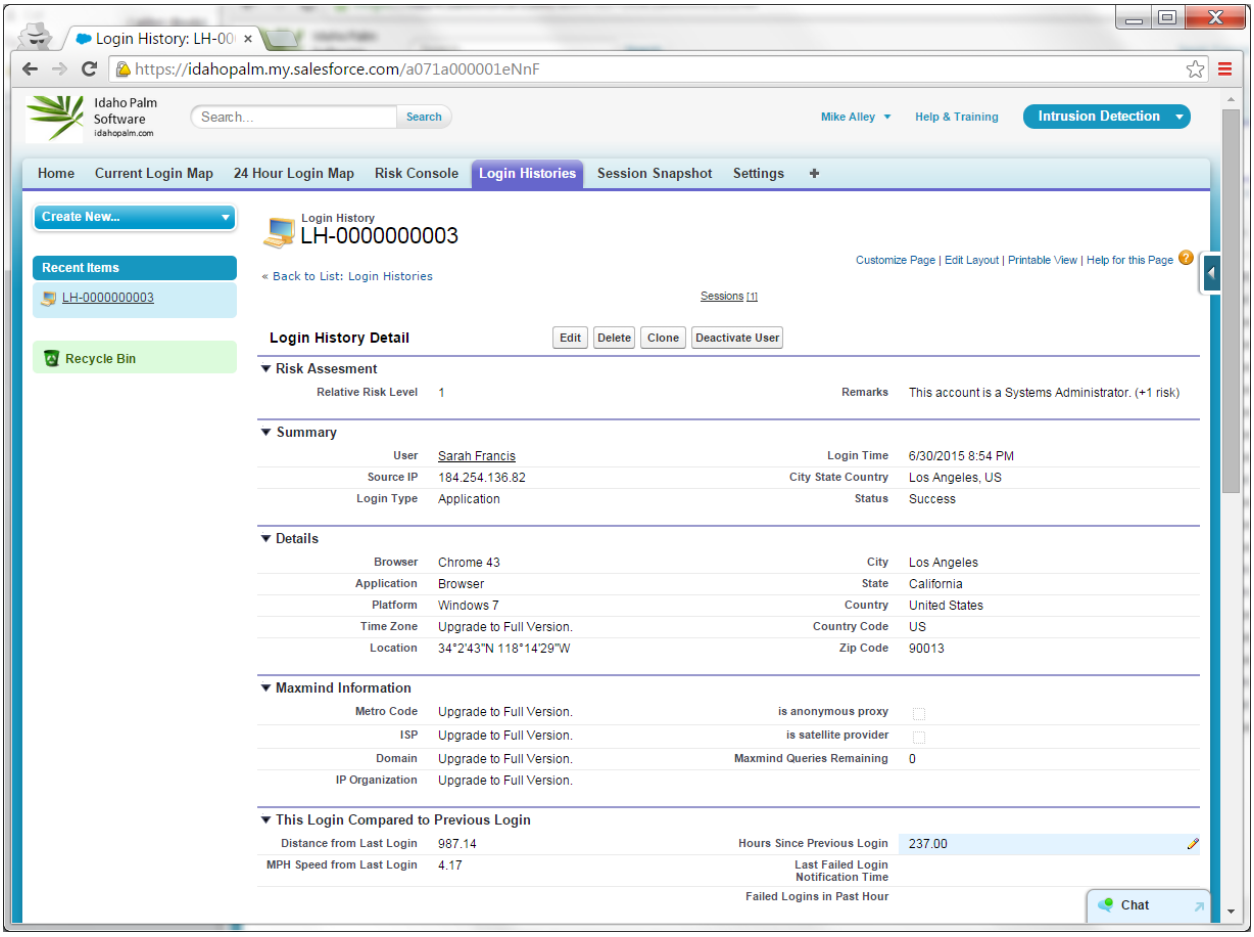
System Admin Login	+1
Speed between logins > 60mph	+5
Login from a different country in same day	+20
Failed logins per hour threshold exceeded	+10(times number of times process runs per hour)

Login Histories

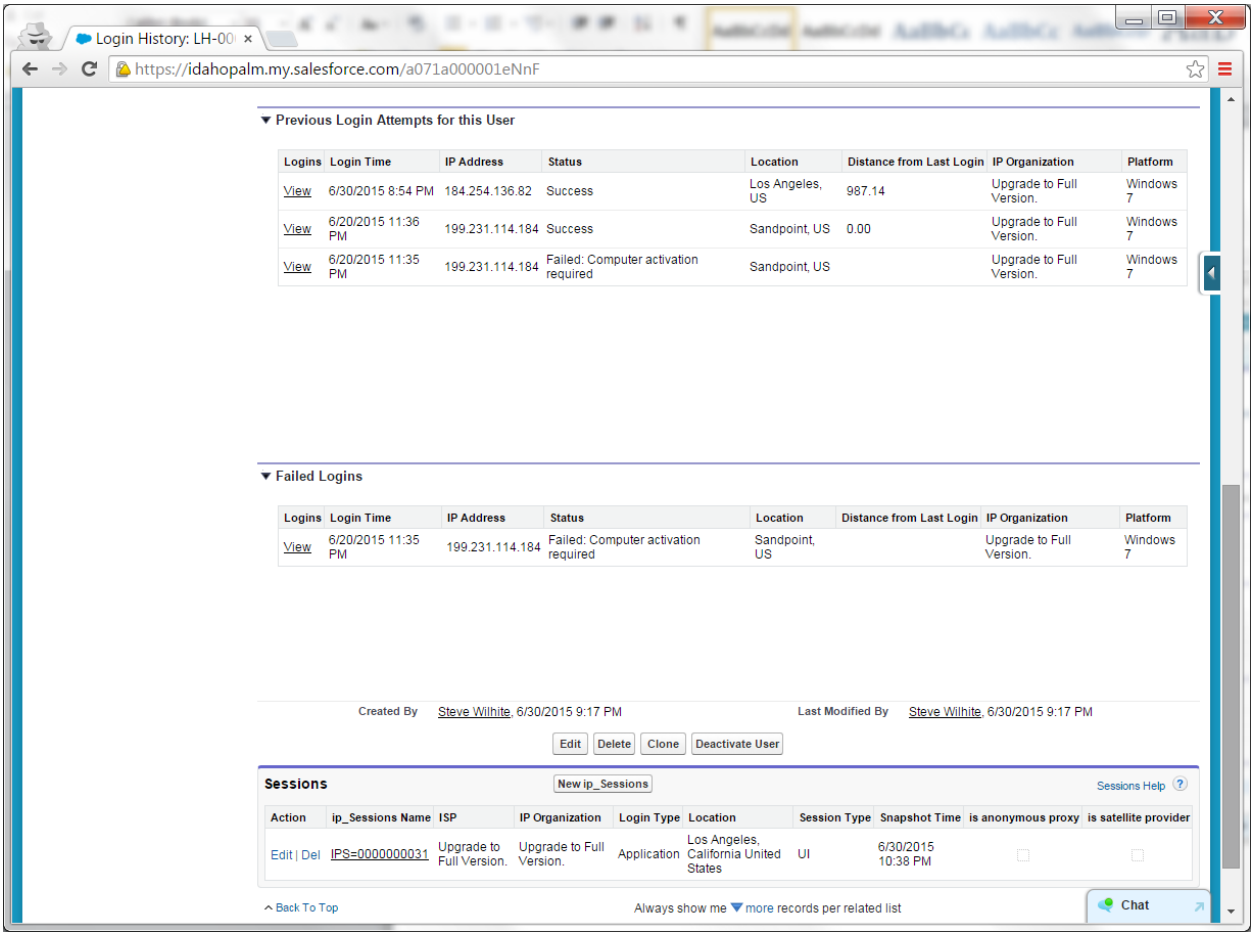
The Login Histories tab allows Security Administrators to view a table of all logins. By clicking on the "All" view and the "Go" button, you can see a history of logins.



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



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



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.

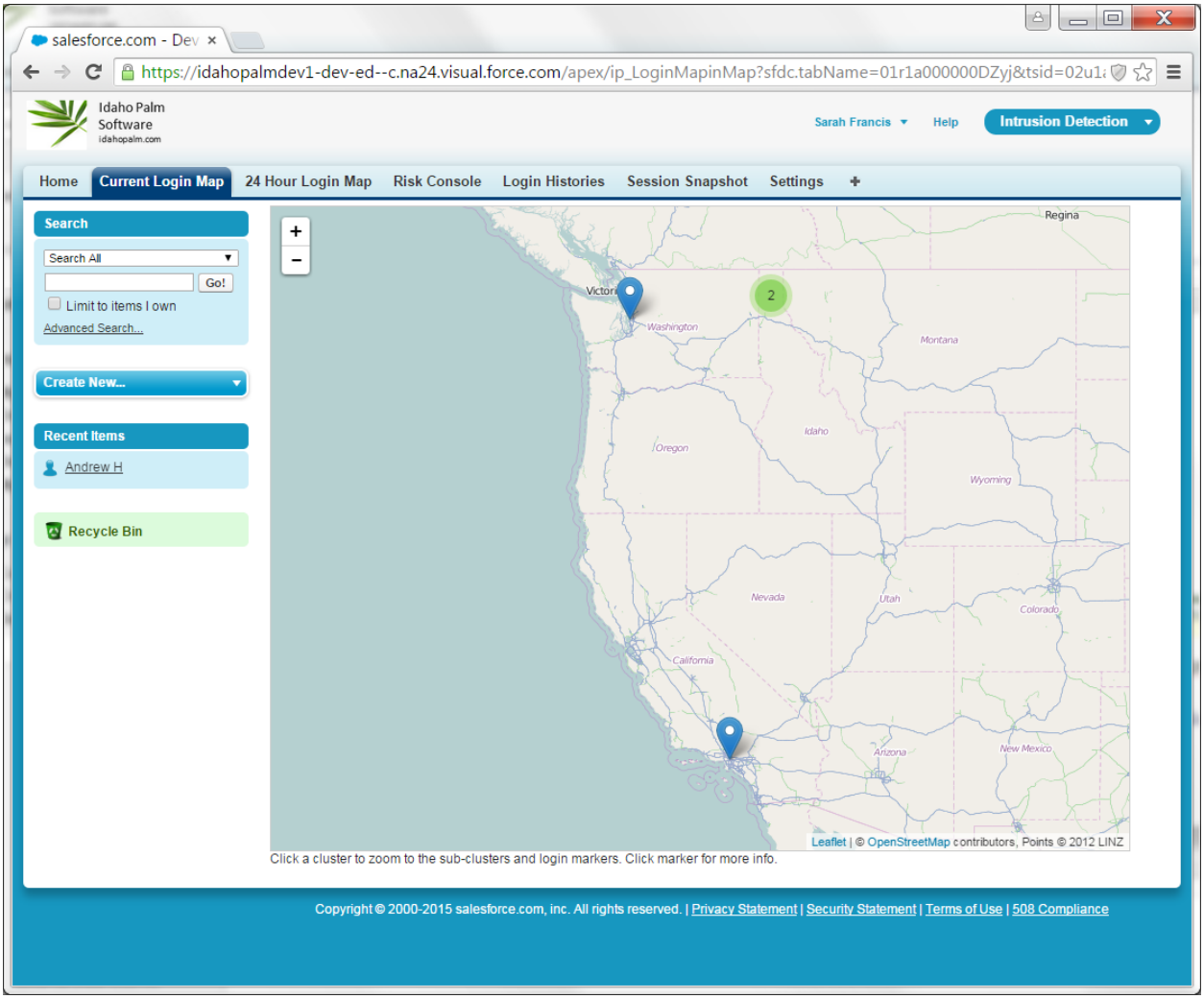
Also, if you click on a View link you can go directly to the login detail page for the referenced login.

Login Maps

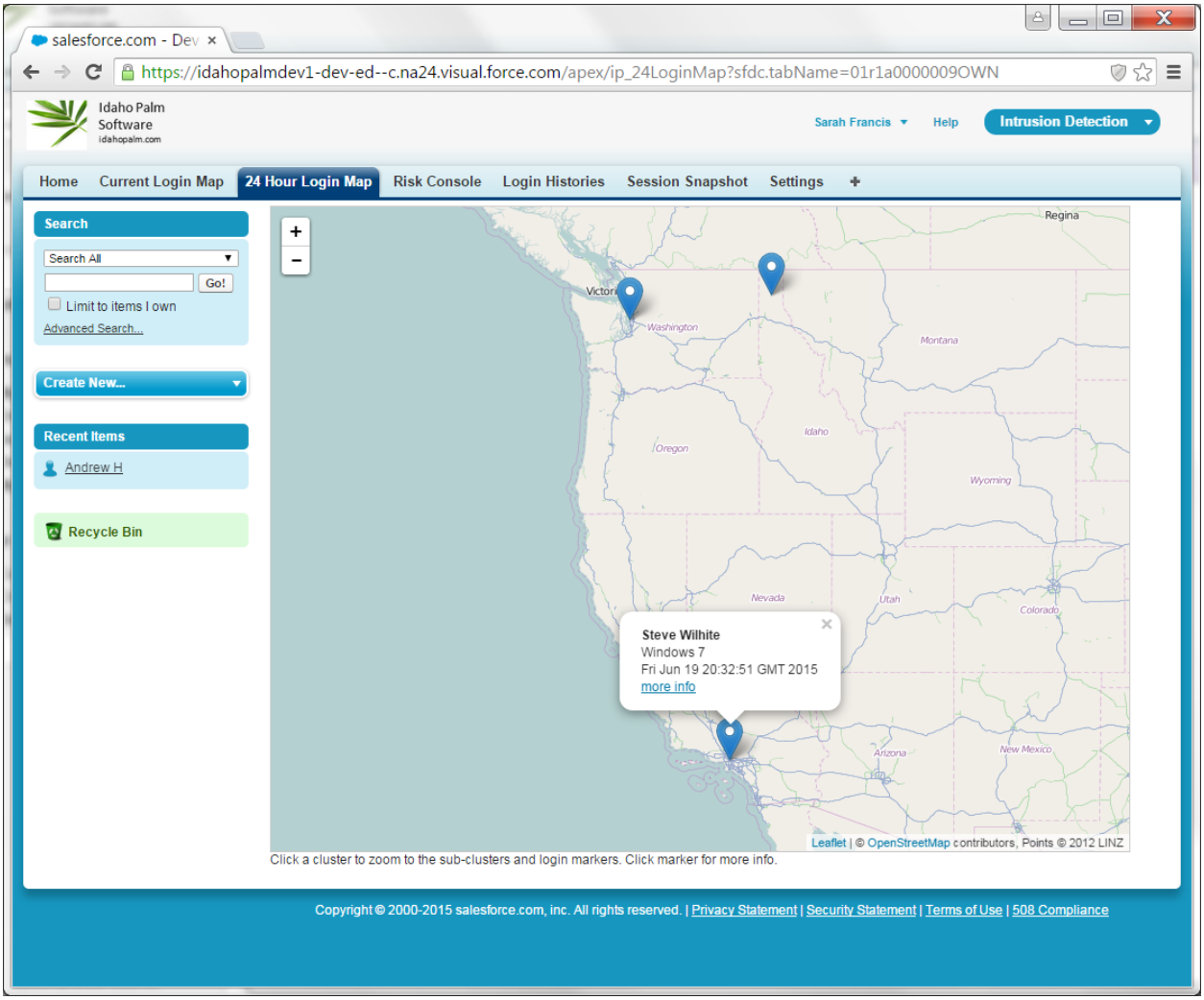
There are two Login map tabs. One will display the current users who are logged into the system, and the other shows user logins within the last 24 hours.

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 with 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.

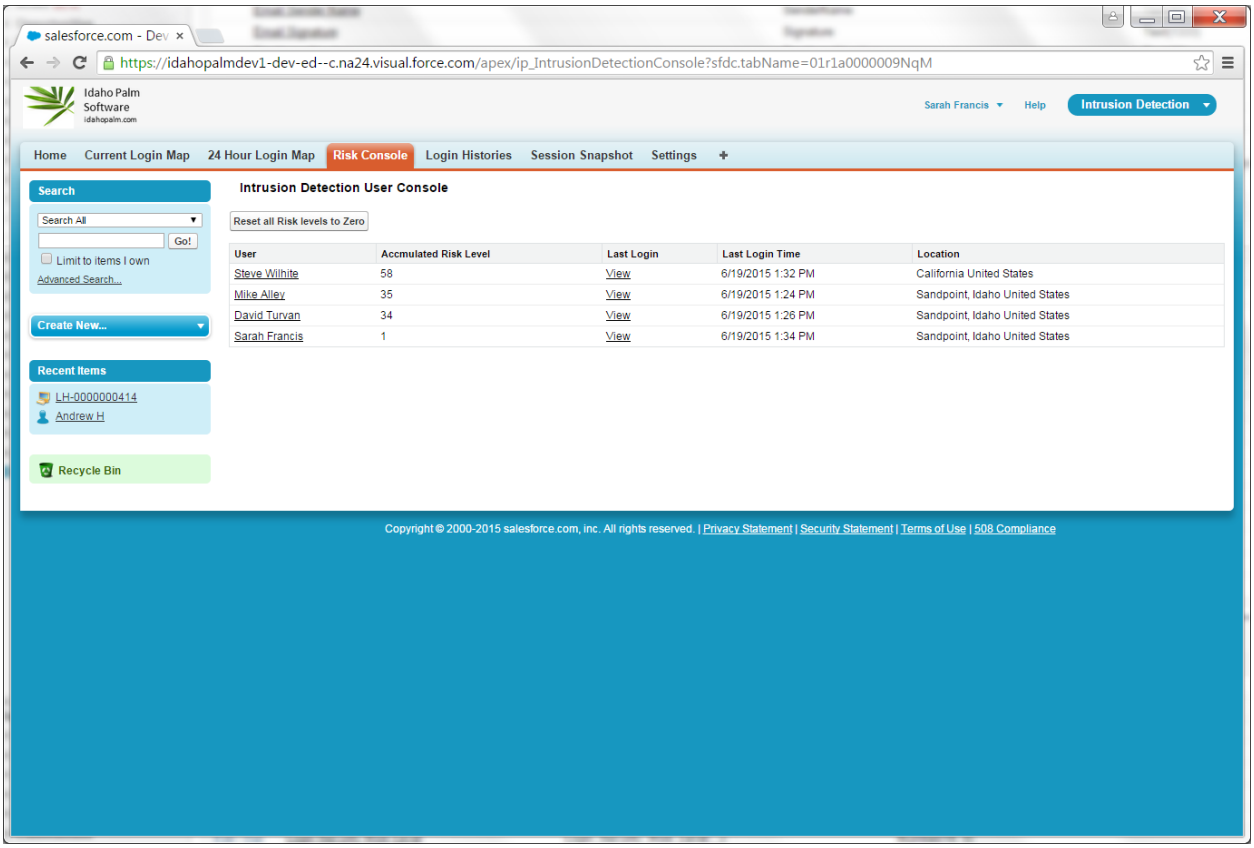


24 Hour Login Map

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

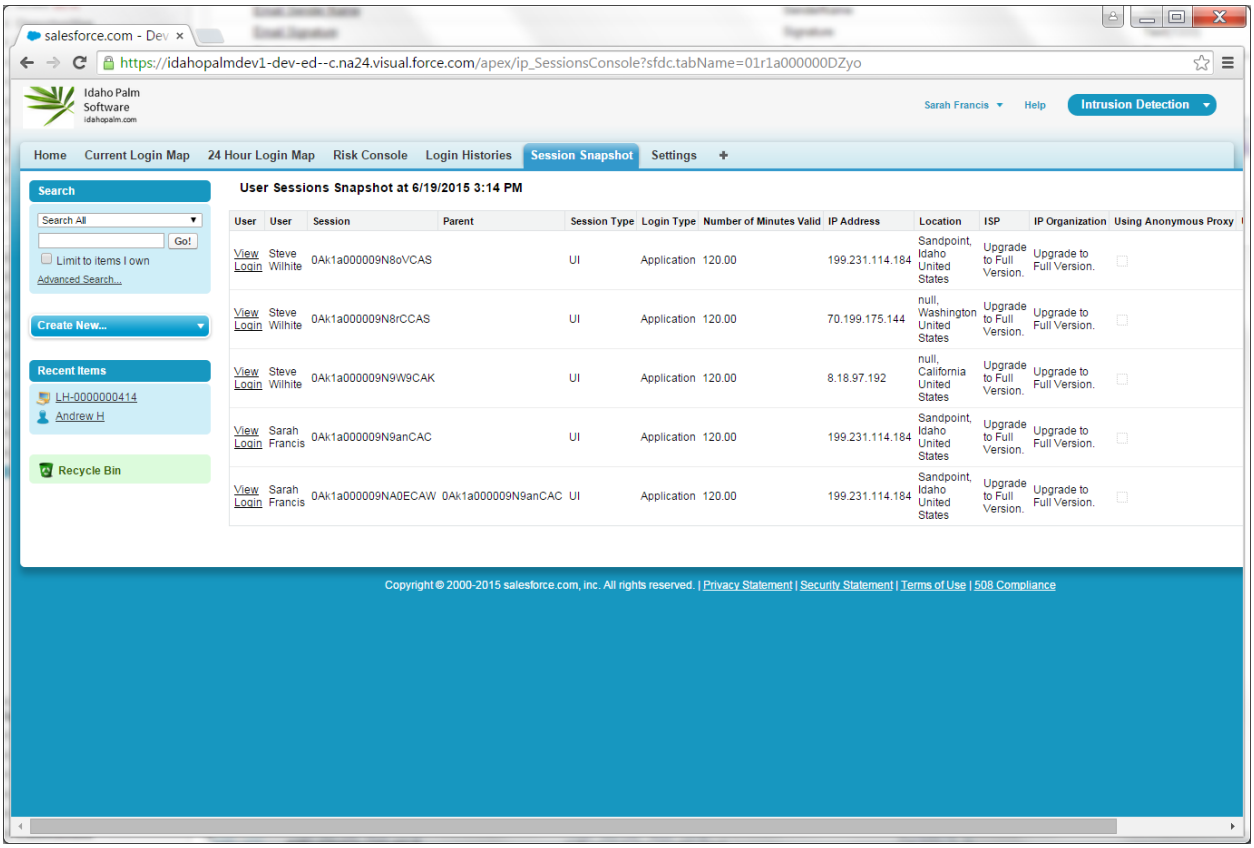
The Risk Console tab displays all users with a cumulative risk level that is greater than zero. It displays them in descending risk level order. This allows Security Administrators to see the most suspect users at the top of the list. By clicking on the View link, it will bring up the last login detail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



The “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).



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.