SECURITY GUIDE

How to Protect and Monitor Salesforce

CloudKettle

INTRODUCTION

As the cost and risks associated with data breaches continue to climb, cybersecurity is a topic that should be a priority for every B2B SaaS company. Recently, IBM published that the average cost of a data breach is $3.86 million. With so much at stake, organizations can't afford to ignore security best practices.

With Salesforce being the central hub of information for many SaaS companies, it's no surprise that organizations are focused on keeping their Salesforce instance and integrations secure. The good news is, Salesforce is an extremely secure platform.

However, there are still basic steps all organizations need to take to minimize external threats and breaches caused by employee error or malicious intent.

Is your organization protecting itself against the right threats?

In this eBook, we're going to discuss the top three threat vectors you need to protect your Salesforce instance against:

External Malicious

Example: hackers

Internal Malicious

Example: a sales rep downloading leads before they leave the organization for a competitor.

Internal Non-Malicious

Example: a well-meaning employee authorizing a tool to integrate with Salesforce that results in a GDPR violation.

Contents

Most organizations are primarily focused on protecting against external threats. While it's important to protect against these, what B2B SaaS companies need to focus on *most* is how Salesforce is set up and maintained to decrease exposure to security issues caused by employee error.

> Employee error is the most common cause of data loss and corruption.
>
> bit.ly/sfdataprotect

Security vulnerabilities caused by human error are common, but because they aren't malicious, often organizations don't prioritize protecting against them. As an example, a well-meaning employee gives an instant messaging platform access to Salesforce that violates the organization's HIPAA compliance. This type of error happens often, and the onus is on each organization to make sure Salesforce is configured to minimize their risk exposure.

This eBook was written for Salesforce Admins and Sales or Marketing Ops team members and will cover what basic security measures should be implemented in Salesforce. We hope you and your team find it valuable.

Greg Poirier
PRESIDENT, CLOUDKETTLE

CHAPTER 1

How to Make Logins More Secure: Part I

Protecting Against External Threats

In terms of being protected against external threats, Salesforce does most of the heavy lifting by making the platform incredibly secure. Which leaves the next most obvious method of attack; a hacker gaining access to your Salesforce instance via a stolen username and password. As discussed in the introduction, while malicious attacks aren't the most common cause of data breaches, they still negatively impact your business. As an organization, making logins more secure is the first step in protecting your instance against external threats.

How to Make Logins More Secure

In this chapter we'll cover:

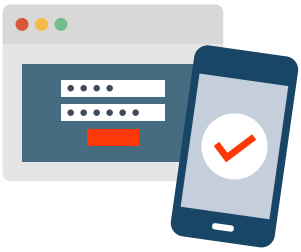
1. How to configure two-factor authentication
2. How to configure network-based security

1. Two-Factor Authentication

Setting up two-factor authentication is another simple way to increase the level of security of your instance. In Salesforce you can enable two-factor authentication on a Profile level or a Permission set level.

Interface Logins

There are two ways two-factor authentication can be leveraged in Salesforce. The most basic way is to enable two-factor authentication for logins. This adds another layer of security by asking each user to verify their identity via an authentication App or text message/call every time they login to Salesforce. Here's a great video on how to setup two-factor authentication for logins in your Org: bit.ly/howto2factor



Add a layer of security by asking users to verify their identity every time they login to Salesforce.

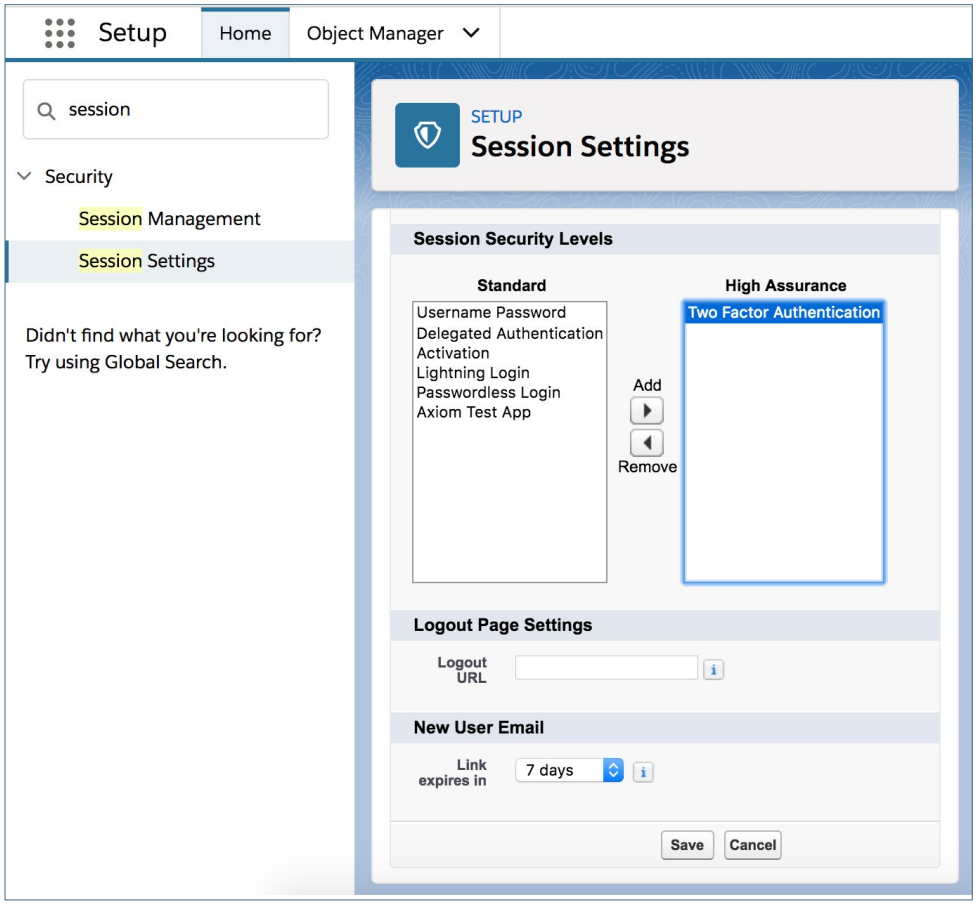
Two-Factor Authentication for Reports

Two-factor authentication can also be leveraged in Salesforce to protect access to reports. To turn on two-factor authentication for users accessing reports, in Setup under “Session Security Levels”, the Admin(s) can “Raise the session level to High Assurance” as seen in the screenshot on the following page. This will prompt users trying to access reports to verify their identity through two-factor authentication.

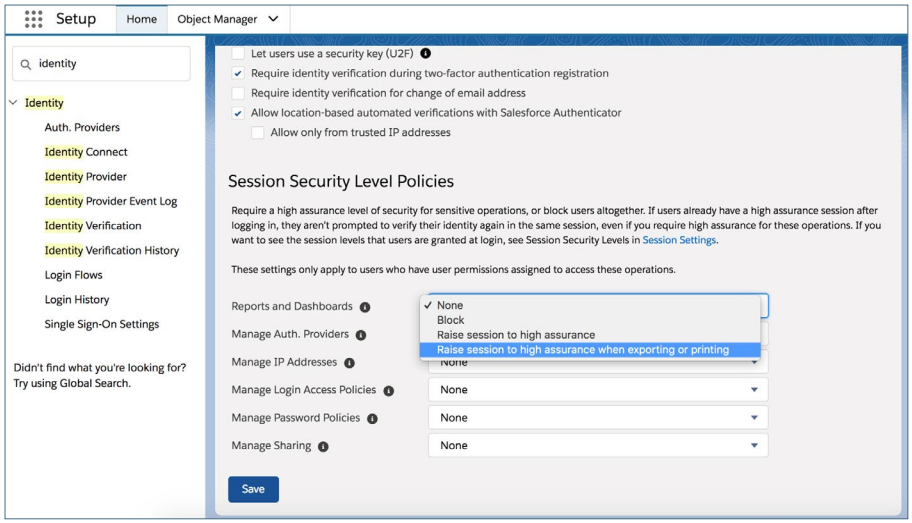
Salesforce can also be configured to prompt users to verify their identity only when exporting or printing reports. To do this, in Setup type in “Identity Verification” and under “Security Level Policies” enable “Raise the Session to High Assurance” which will prompt users to authenticate when they try to export data or access certain reports.

Salesforce can be configured to prompt users to verify their identity when exporting or printing reports.

How to Control Access to Reports



How to Control Access to Printing and Exporting Reports



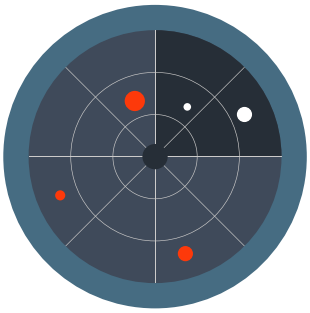
2. Configure Network Based Security

There are two ways to configure your Salesforce IP settings to increase the security of your instance.

Org-wide configuration

Ensure the Trusted IP range feature is configured in Salesforce. A trusted IP range is a list of safe or known IP addresses Salesforce users can login from. An organization's trusted IP range usually includes office locations and other private networks that employees access. Once you set up a trusted IP range, users that login outside of that range are challenged to verify their identity to access Salesforce. For example, if an employee had a demo at a prospect's office, when logging into Salesforce they'd be forced to use two-factor authentication.

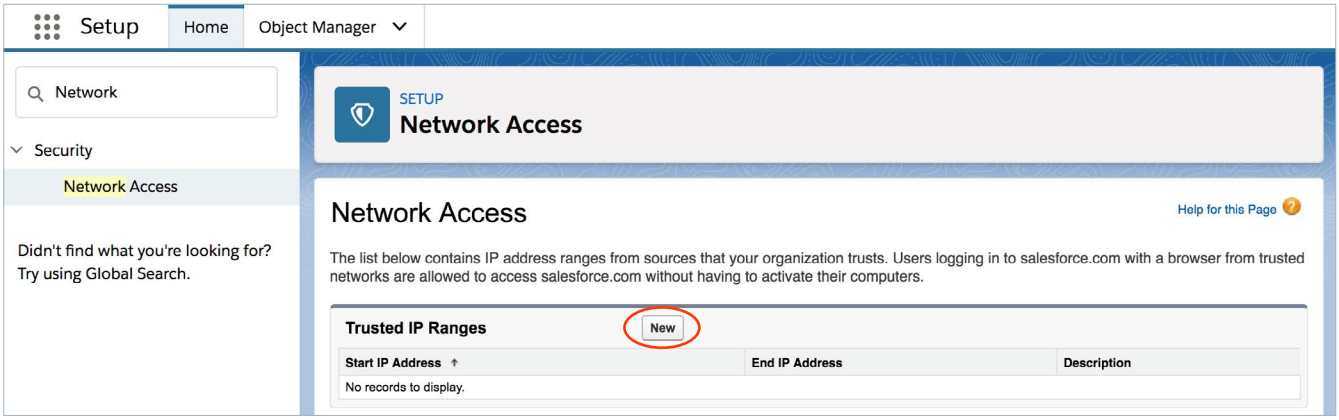
Pro Tip: Use the Salesforce Authenticator App for two-factor authentication



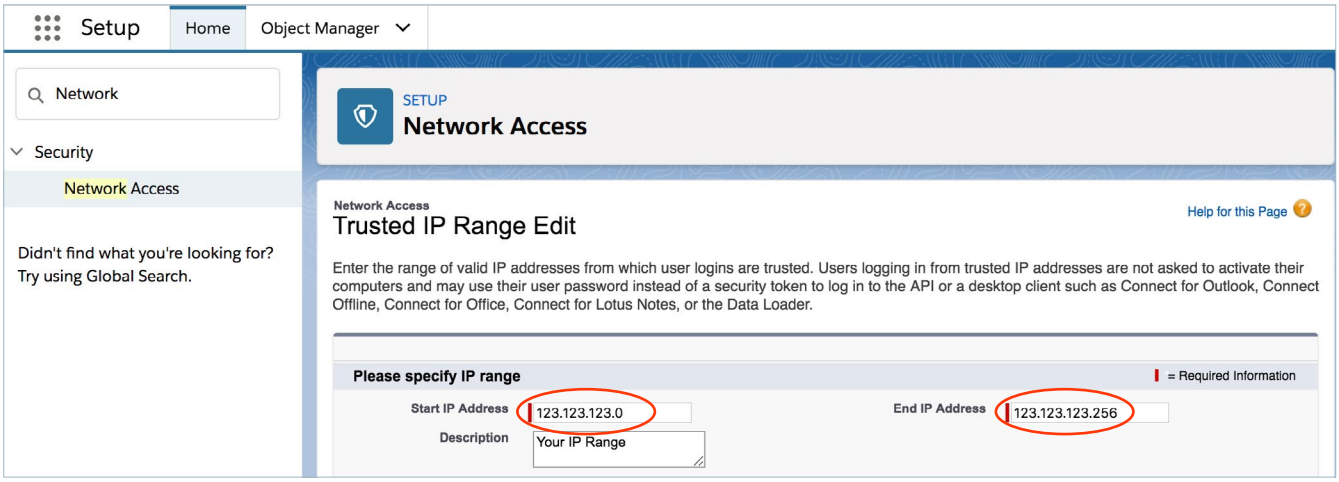
Set up a trusted IP range so users that login outside of that range need to verify their identity to access Salesforce.

How to Set up Org-Wide Configuration

Step 1: In Setup search for Network Access and click “New” to create a new trusted IP Range.



Step 2: Specify the Start IP and the End IP for the trusted range.



Pro Tip: If you plan to have multiple trusted ranges, add informative descriptions to specify which range applies to which use case.

Wrap Up

In the next chapter we discuss how to track login history and enable App Allowlisting. If you want to learn more about how to educate your users, protect your Salesforce org, and encourage a culture of security, we recommend this Security Basics module from Trailhead: bit.ly/securitybasicstrail.

CHAPTER 2

How to Make Logins More Secure: Part II

In this chapter we'll cover:

1. How to track Login History
2. How to enable App Allowlisting

Tracking Login History

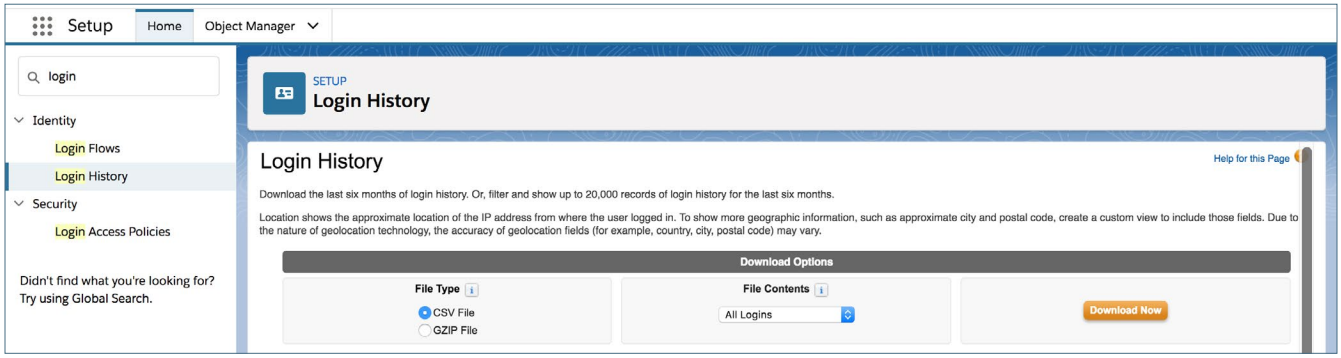
Tracking Login History is another easy way to increase the security of your instance. Salesforce even provides a standard report called "New Login Location Report".

Why Track Logins?

For example, if a salesperson is using an application like WorkBench, Browser, Data Loader, etc. to export leads, this could signal that employee is preparing to leave the organization. And they might be trying to take leads and other confidential information with them.

How to Track Logins

Search for Login History under the Setup menu.



Review for unusual behavior, you can also download this report to better query it for specific users/activities as required.

Allowlisting

With the rise of OAuth, it's easier than ever before for employees to install an App in Salesforce. This is problematic because not all employees understand (nor should they be expected to) all the factors that are taken into consideration when vetting if a 3rd party application should have access to Salesforce. To prevent an employee from accidentally giving a solution access to Salesforce, App Allowlisting should be enabled in the Org. This will block end users from giving solutions access to Salesforce.

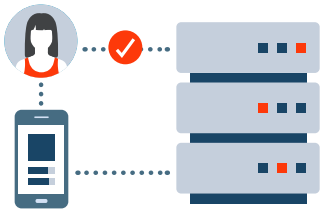
Here's an example of why enabling App Allowlisting in your Org is so important. Let's say a well-meaning employee gives an instant messaging platform access to Salesforce so they can receive notifications about Opportunities. While that employee may have only good intentions, they might not realize that giving that platform access to Salesforce violates their organization's HIPAA or GDPR compliance. The employee in question isn't aware they're doing anything wrong and it could take days to months to discover this change has been made and correct it.

In the age of compliance, organizations have to invest in properly configuring Salesforce. Enabling App Allowlisting in Salesforce allows the Admin(s) to specify which Apps users can grant access to. This can be managed at the org-wide level (all users), or for specific users. It's a scalable solution because it applies the same limitations to new users, and provides a centralized location to manage user authorization.

How to Enable App Allowlisting

Step 1: App Allowlisting must be set up by Salesforce for your Org. The Admin(s) of your instance need to submit a case or call Salesforce to ask that this feature be enabled.

After Salesforce has enabled App Allowlisting in your Org, you can assign certain Profiles and Permission Sets access to specific Apps. In the following example, we use Data Loader because it's a commonly used and very powerful App. However, not every user should have access to it.

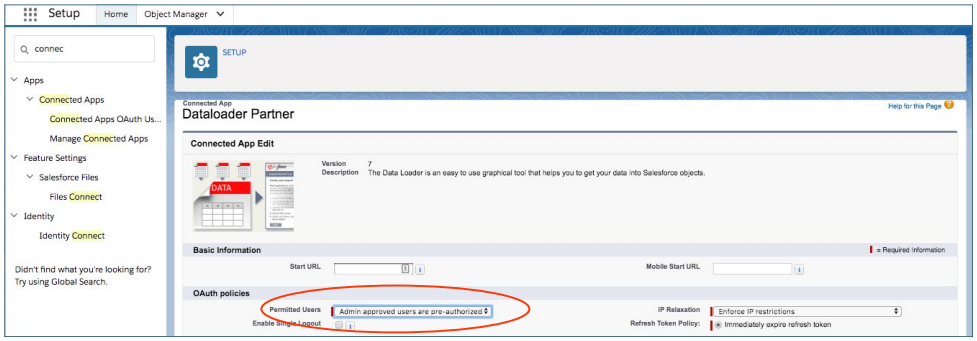


What is OAuth?

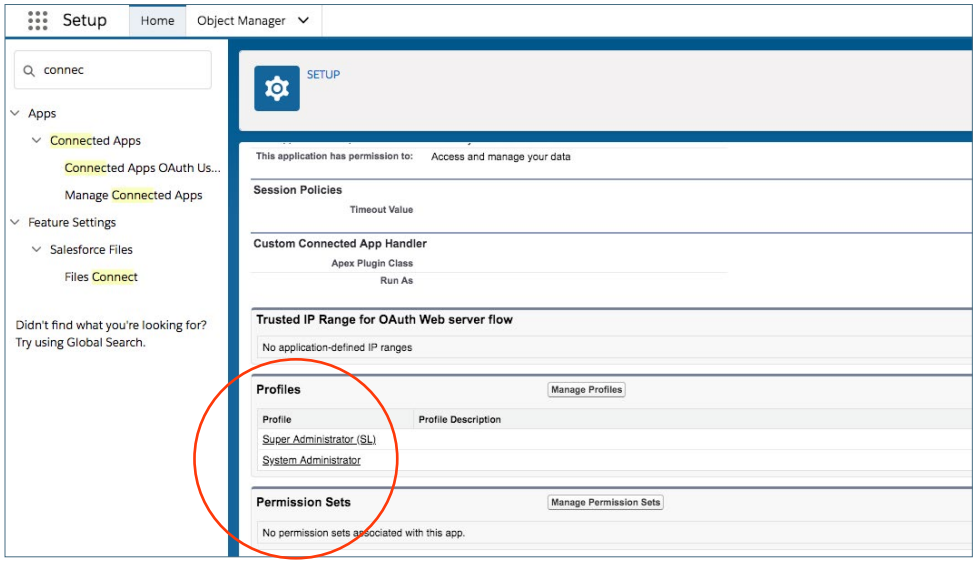
OAuth is an authentication protocol that allows you to approve one application interacting with another on your behalf without giving away your password.
bit.ly/OAuth101

Step 2: Under “Managed Connected Apps”, click “Edit” next to Dataloader Partner.

Step 3: Under OAuth policies, Permitted Users select “Admin approved users are pre-authorized”.



Step 4: Under “Manager Connected Apps” if you click the Data Loader label to bring up the Connected App Detail, you may assign Profiles and Permission Sets to have access to the App.



Wrap Up

If you’re looking to learn more about security features like two-factor authentication, custom domains, and single sign-on, Trailhead is an incredible free resource. We recommend starting with the User Authentication module in Trailhead: bit.ly/userauthtrail.

CHAPTER 3

How to Make Integrations More Secure

More and more businesses are taking advantage of integrating AppExchange Apps and other paid tools with their Salesforce instance. What does this mean for Salesforce Admins? It means most Admins today are managing a Salesforce ecosystem instead of just a Salesforce instance.

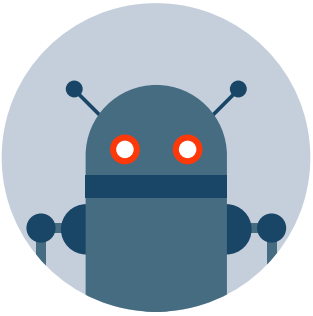
In the last two chapters, we've covered how to make logins more secure. Now we're going to discuss how to make sure integrations are stable, auditable, and secure.

How do you ensure all your integrations are stable, auditable, and secure?

An easy way to address this challenge is to invest in a Dedicated Salesforce Integration User. Not only will this help manage integrations more seamlessly; but most importantly, it will also increase the security of your instance.

What is an Integration User?

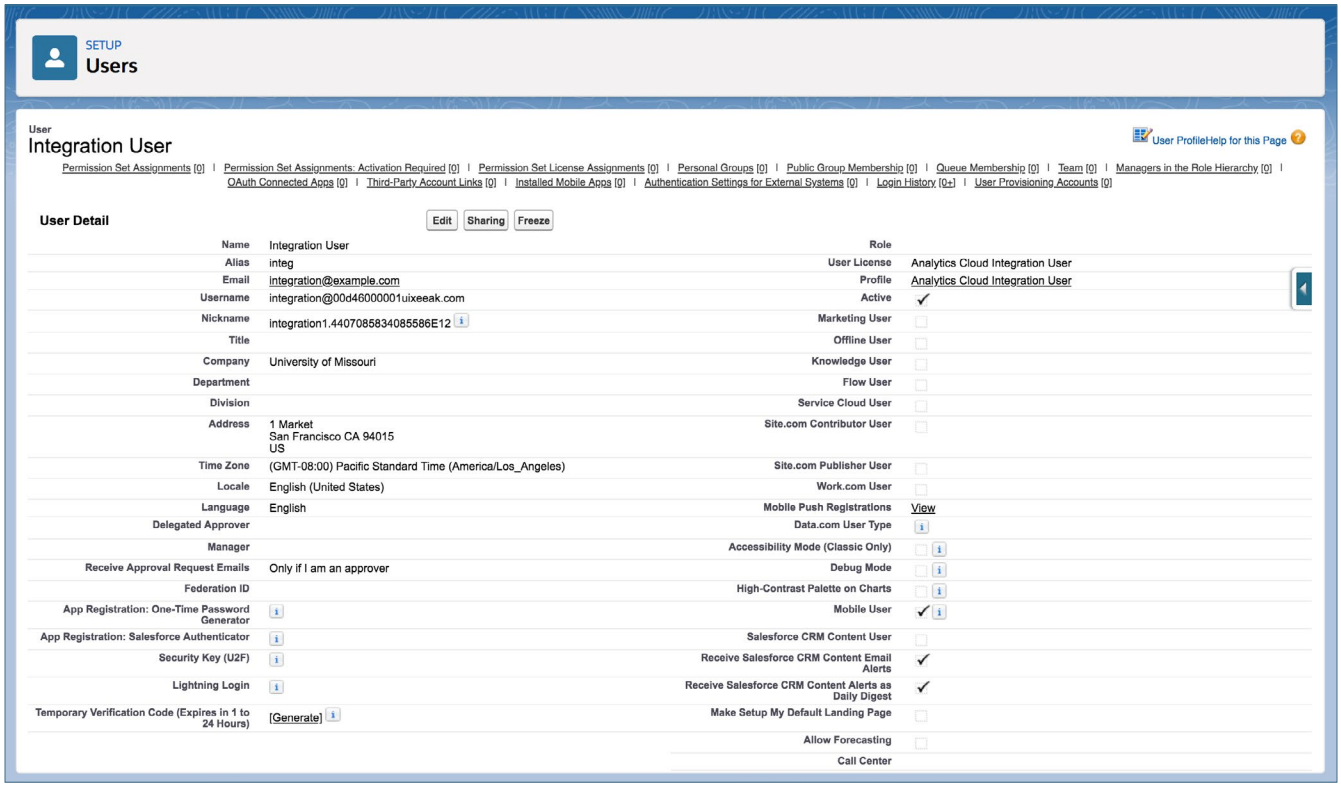
An Integration User can be an Admin's best friend. It's a dedicated (not used by any human) full Salesforce license that has a custom Profile, Permission Set, and is used for any 3rd party integrations, like: marketing automation, CTIs, data enrichment tools, and even your own custom API work. Integration Users are particularly important for these kinds of tools because they tend to update thousands (or tens of thousands) of records per day.



A Dedicated Integration User has a full Salesforce license that is not used by any human.

An Integration User is a more secure, auditable way to move data into and out of your instance without relying on an existing user's license.

Dedicated Integration User Profile



ROI of an Integration User: Security

Now, let's talk about how a Dedicated Integration User increases the security of your Org. As we covered earlier, most organizations are integrating external tools with their Salesforce instance. The AppExchange thoroughly vets all vendors, so you can trust that while expanding the value your organization gets from Salesforce, you aren't compromising the security of your instance. However, not all external tools come from the AppExchange and undergo the same rigorous vetting process.

The status quo in many organizations is Salesforce integrations are given access via the Salesforce System Administrator's own license. While it's easy to understand why this is the status quo, you should consider the access you are giving that tool.

When an integration has System Admin access to Salesforce, that tool is able to:

Create or delete your users

Delete records

Reset users' passwords

Log in as any user

Create new permission sets and assign them

A 3rd party application should **never** be able to do these things.

Mitigating Risk

When an employee, whose Salesforce license is being used for an integration, leaves the company or changes their password, it can create problems.

A change in an Admin's password will break any integration attached to that license and, it may take days, weeks, or even months before someone realizes the integration is broken. Perhaps more concerning, Admins (those with the most power in Salesforce) may forgo updating their passwords because of the level of work involved in updating the login criteria with every integration tied to their user. Additionally, consider what happens if that Admin is leaving the organization—a freeze or deactivation on their user will break every sync tied to them.

A Compelling Case

The upfront costs of an extra license and the work to set up a Dedicated Integration User can seem daunting to organizations and their Salesforce Admins. However, it's a small cost relative to the clean up costs of a data breach. Learn how to set up a Dedicated Salesforce Integration User in the next chapter.

CHAPTER 4

How to Setup a Dedicated Integration User

This chapter provides a step by step guide on how to create a Dedicated Salesforce Integration User.

Step 1: Create a Profile

Your integration user(s) have unique needs and need a unique Profile in Salesforce. Follow these steps:

1. Start by cloning your “Standard User” **NOT** the System Administrator Profile
2. Then make sure the following are setup:
    - No access to Setup area of Salesforce
    - Modify All on all records that your integration(s) need to update, in particular, keep in mind custom record types that are deployed by integrations’ own packages
    - Broad access to reports/dashboards
    - Be able to post to Chatter

Step 2: What Permissions to Enable

Administrative Permissions

Next, you'll be prompted to select what administrative permissions should be enabled for this Integration User. These aren't hard and fast rules, but making the assumption you are using marketing automation, data enrichment and other popular tools, you'll want to set up the permissions as follows:

Should be Enabled

- API REST Services and API Enabled should be checked
- Create, Customize and Schedule Reports and Dashboards and folders
- Edit HTML templates
- Password Never Expires—doing this prevents the password from expiring while someone is out of the office with no one available to update it across integrations

  TIP: Put a recurring meeting in your calendar to change the password and list every integration tied to it. Include at least two people on the invite (you and someone else) in case someone is on vacation or has left.
- Transfer Records
- Update Records with Inactive owners
- View All Data, Modify All Data, View All Users
- View Roles and Role Hierarchy

Should NOT be Enabled

- Assign permission sets
- Bulk API hard delete
- Create and upload change sets
- Deploy change sets
- Manage Auth providers
- Manage IP Addresses
- Manage Package Licenses
- Manage Profiles and Permission sets
- Manage Roles
- Manage Users
- Manage login access and password policies
- Reset user passwords and unlock users
- Weekly Exports
- Lightning experience user ⇨ on the Profile level

General User Permissions

Next, you'll be prompted to select what general User Permissions should be enabled for this Integration User.

Should be Enabled ✓

- Convert Leads
- Edit Events and Tasks
- Import Leads and Cases
- Manage Leads
- Run Reports
- Transfer Cases and Leads
- *API Only User
  (this is optional, please see explanation below)

Should NOT be Enabled ✗

- Manage two-factor authentication in API or User Interface
- Require two-factor authentication for API logins and User Interface logins
- View encrypted data

*The API Only User

The "API Only User" setting is primarily used for Integration users. If you choose to enable this security feature, there are pros and cons to consider:

Pros:

- Disallows anyone who may have access to this users credentials to log in through the User Interface and gain access to information they should not otherwise see. In short, it is more secure.

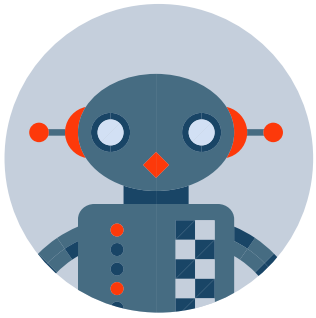
Cons:

- The only way to reset the password for an API Only User is for an Admin to click "Reset Password" on the user page and go through the email process to change the password.
- A small number of integrations may require access to page layouts in order to work properly. If API Only User is active, they will fail (so this should be tested before you deploy).

Creating Page Layouts When “API Only User” is Not Enabled

If you choose not to enable “API Only User”, the Admin(s) will have to create Page Layouts for that user. Sometimes (depending on how it is built/syncing with Salesforce) an integration can only “see” fields if they have access to a Page Layout the fields are visible on. For that reason, you need to create custom Page Layouts that include every field on an object that your integrations may need to read or write to.

Often, cloning your Admin Page Layouts is a good place to start with this process. As the integration user isn’t human, you don’t have to worry about the Page Layouts being clean and how their flow works. Simply ensure the fields are visible to the Profile.



Give your Integration User a “robot” or similar image.

Step 3: Create Your User

Now that the Profile, Permission Sets, and Page Layouts have been created it’s time to create your User. When you set up your Dedicated Integration User you clone a “standard user” profile instead of using the System Admin’s profile. When creating an Integration User give them a “robot” or similar image and make sure their Chatter profile explains the purpose of the license.

Wrap Up

Once you have the Integration User(s) created, it’s best practice to migrate one integration at a time. Start with the lowest risk integrations first and work your way up. Ensure Permission Sets applied to the original Admin for each integration are also applied to this user. Watch for failed logins and check your Audit Trail.

CHAPTER 5

How to Add Friction to Employees Exporting Data

Restrict Employees From Exporting Salesforce Data

Another important part of securing your Salesforce instance is making sure your Sales Cloud data is protected. To achieve that, users (who are not supposed to) shouldn't be able to export data from your organization.

A common example is a sales rep trying to export leads before they leave an organization. Unfortunately, there is no way to completely block users from exporting data from Salesforce without blocking their access to that data. The best approach is to add friction to employees attempting to export data. The more onerous the process, the more you minimize the chances an end user will steal data.

You can add friction to stop users from exporting data by:

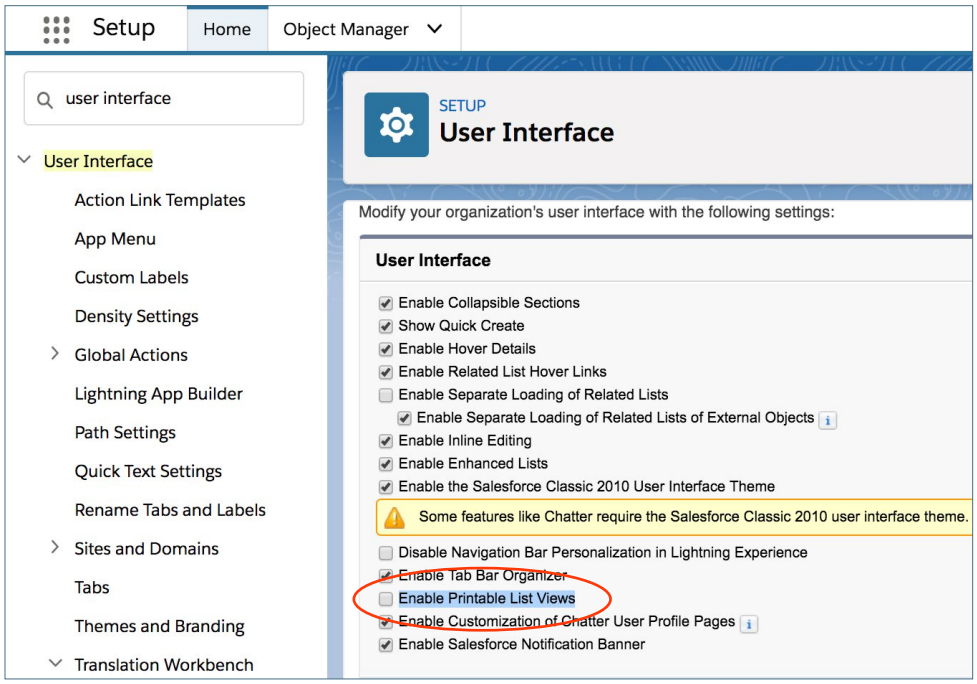
DISABLING	ENABLING
☐ Printable View ☐ Report Export Permission	☑ App Allowlisting

Print Screen

If “Print Screen” is enabled, users can print a List View of a 1,000 records at a time. This is a quick way to export data from Salesforce. Also, there is no record of this type of activity in the Audit Trail, so an Admin can’t flag that a user has done this.

By disabling “Print Screen”, users will be forced to screenshot each individual screen one at a time if trying to export data. It’s not a perfect solution, but it does add a considerable amount of effort on the user’s end.

How To Disable Print Screen: Under User Interface in Setup, uncheck “Enable Printable list views”.



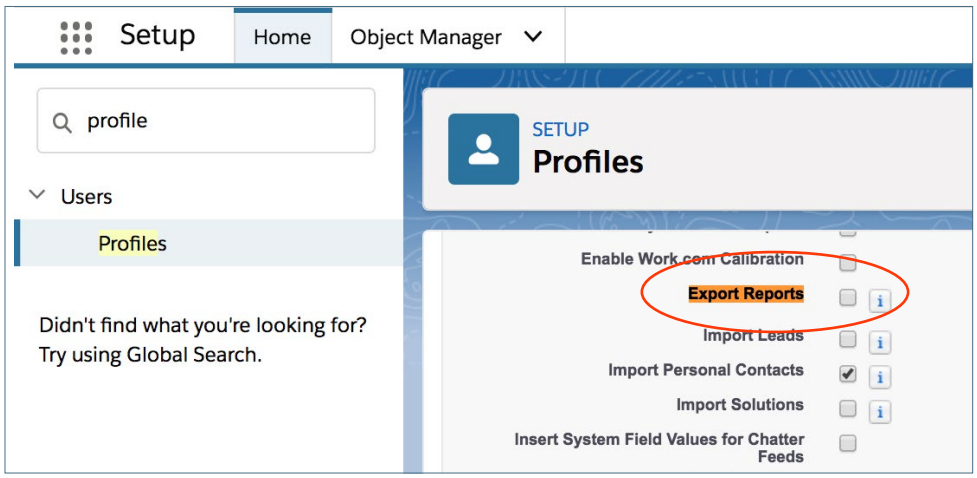
By disabling “Print Screen”, users will be forced to screenshot each individual screen.

Disable Export Report

A very powerful Salesforce feature is the ability to export reports as a CSV. While this feature can be tremendously valuable, it can also be dangerous if the wrong Users have access to it.

For a more secure instance, you should configure who can export data as a Permission Set, not on the Profile level. As an Admin, it is important you know exactly which Users have this Permission available to them so you can quickly remove it, if necessary.

How to Disable Export Reports: Under General User Permissions uncheck "Export Reports". This cannot be changed on the Standard User Profile. You have to clone the Standard User and edit that custom profile.



Allowlisting Apps

In chapter two we talked about enabling App Allowlisting to minimize the effect of unintentional employees mistakes. However, it's also important to enable App Allowlisting to block malicious end users from installing a package like Data Loader to quickly export Salesforce data.

Enabling App Allowlisting in Salesforce helps ensure Admin(s) control which Apps can be installed in Salesforce. For a step by step guide on how to enable App Allowlisting in your Org please see page 8 in chapter two.

If you're looking to learn more about how to control access to data using point-and-click security tools, we recommend this Data Security module from Trailhead: bit.ly/datasecuritytrail.

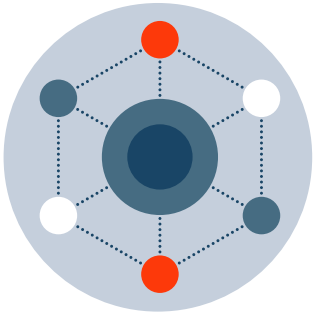
CHAPTER 6

Top Five Things to Monitor in Salesforce

So far in this eBook, we've talked about how B2B SaaS companies can better configure Salesforce to decrease exposure to security issues caused by external threats, employee error, and malicious intent. Now, let's talk about how you monitor the security of your Salesforce instance.

Monitoring Salesforce is key to ensuring the overall security of your instance doesn't degrade over time. Often well-meaning employees make mistakes or inadvertently take actions that create a vulnerability. Here are five items that should be constantly monitored in Salesforce to keep your Sales Cloud data stable and protected.

1. Connected Apps

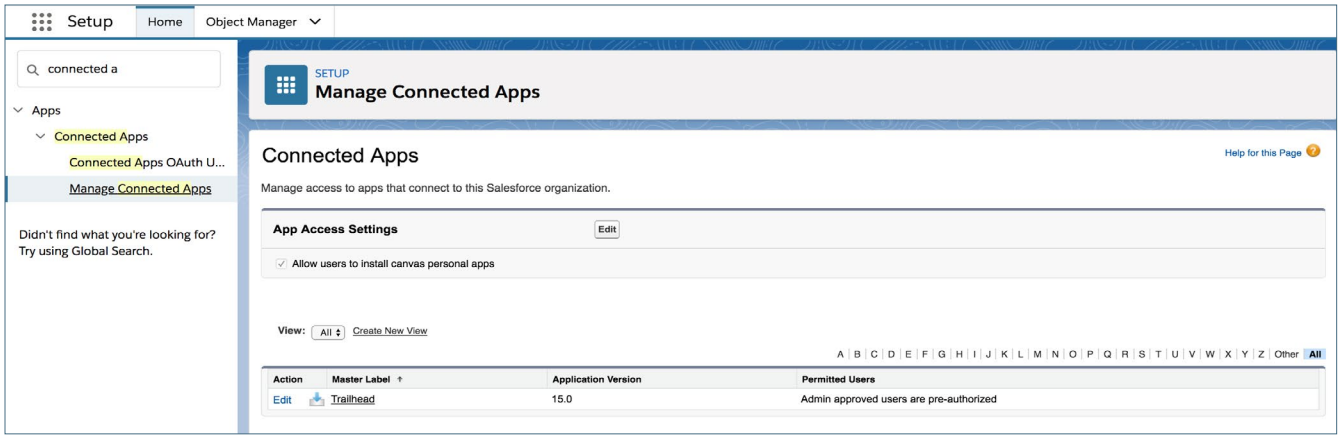


It's important to keep stock of what Apps are connected to Salesforce and remove any that have not been vetted, are no longer in use, or violate your organization's policies. Applications are often granted Admin level access to Salesforce data; which means they have access to create or delete your users, delete records, reset user's passwords and more. In chapter three, we talk about how no integration should ever be given Admin level access to Salesforce. However, for many organization's this is still the status quo.

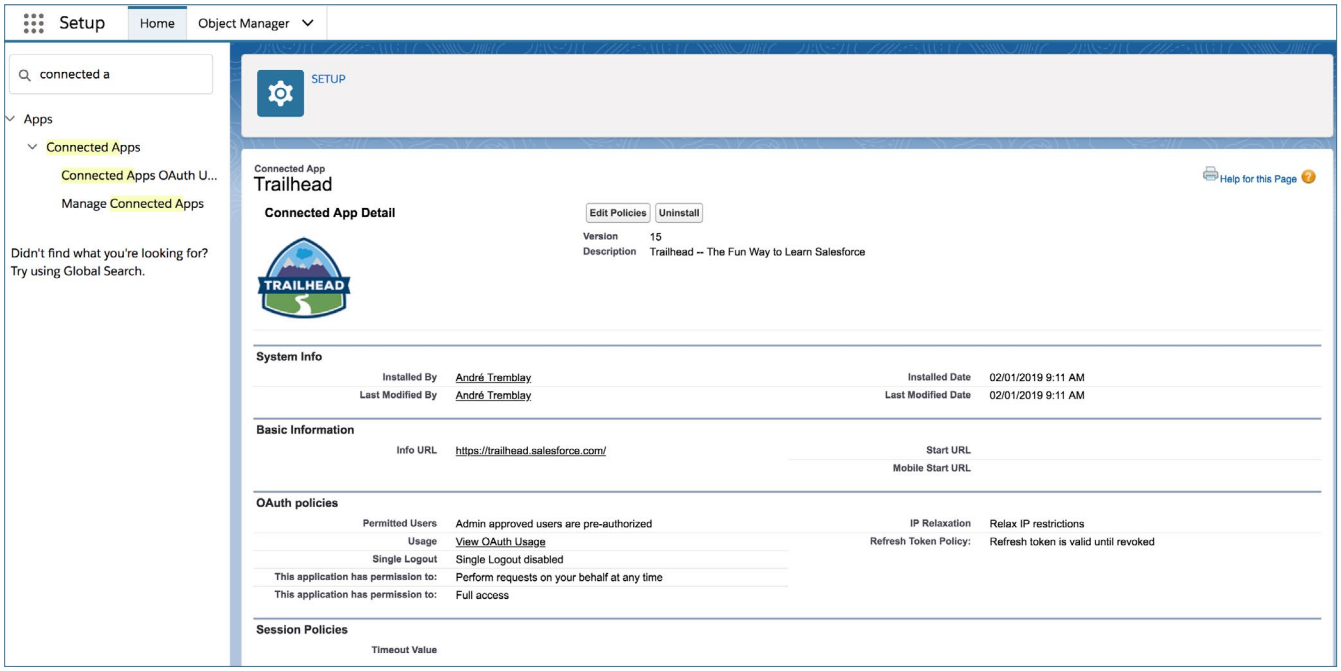
We also talked earlier about enabling the App Allowlisting feature in Salesforce so only Salesforce Admin(s) can install packages or authorize integrations (for more information on App Allowlisting refer to page 8). Even if you do have App Allowlisting enabled, you'll still want to report on what Apps are installed in Salesforce. Human error is always possible, especially if your instance has multiple admins.

How to Report on Apps Connected to Salesforce:

Step 1: Under Setup search for Connected Apps.



Step 2: Each App listed will show details about the App.



2. Deactivation

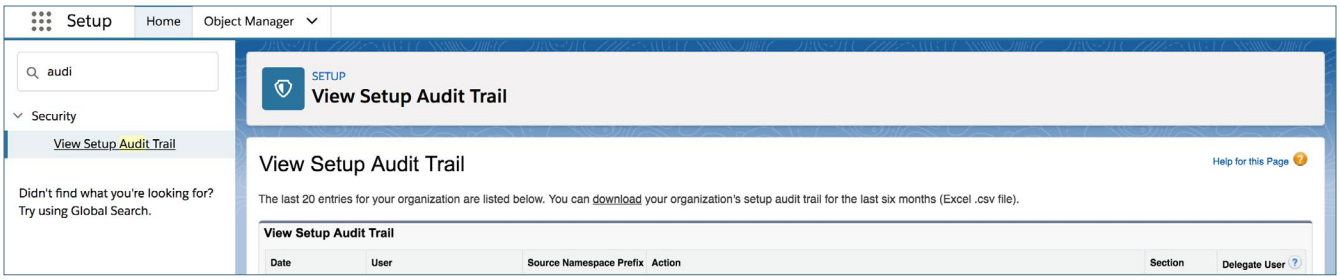
Another area to be aware of is Users or Admins being deactivated because it can be a sign an end user is making malicious changes. Whether it's intentional or not, keeping tabs on how many users and who has been deactivated is smart. User freezes should also be monitored. In order to monitor this, examine the Salesforce Audit Logs and review if a user has been deactivated or frozen and by whom. This is a near impossible event to catch in real time. If someone is acting maliciously it will take them a short amount of time to deactivate users. However, it is good to get in a daily habit of checking the Audit Logs for these events.

3. Metadata changes

Metadata changes are also something that should be monitored daily to ensure no malicious or flawed code has been pushed into production. On a daily basis, Admin(s) should be looking at all new code and examining if anything unexpected has occurred. As an example, if an employee pushed a new piece of code into Salesforce that causes data to pass into another platform, the Salesforce admin would want to catch and reverse that change as soon as possible.

To monitor this daily, an Admin(s) needs to set up an Audit Trail, download the report of the last six months, sort through the CSV. and export daily to see Metadata changes. Then identify if any of those Metadata changes seemed irregular or cause for concern.

Step 1: Search Setup for "View Setup Audit Trail.

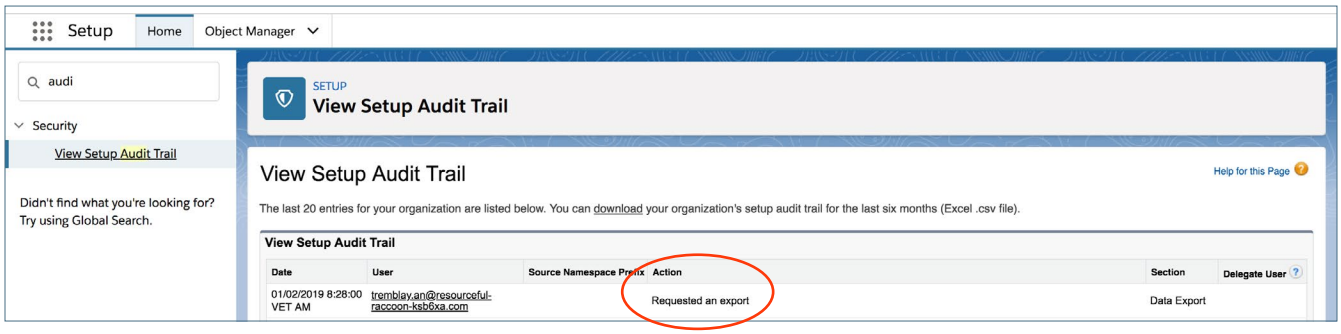


Step 2: Click the download link to get more than the last 20 entries.

4. Mass Data Exports

Another item to watch for is mass data exports. This is relatively straightforward, anytime anyone is mass exporting data in your instance your Admin should know about it. It can often be an indication a sales rep is getting ready to leave the organization and take leads with them. In the absence of a monitoring tool like Salesforce SafeGuard, this is a time consuming process that involves checking Scheduled Jobs and the Audit Trail daily. bit.ly/safeguardforsf

How to Catch Exports through the Data Export tool: Search the Audit Trail for "Requested an Export".

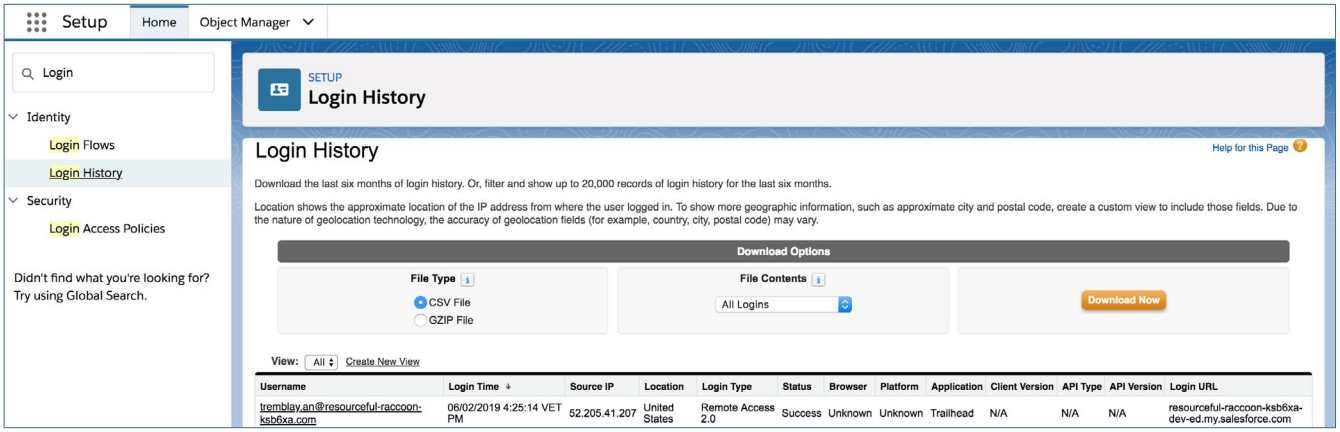


5. Failed Logins

Tracking failed logins can alert your organization to suspicious behavior. If for example, a login fails repeatedly from a country where your company has no offices and then succeeds, that could indicate a threat has gained access to Salesforce.

Once identified, the right course of action might be to freeze that user, change the password quickly or watch for incoming requests. The downside to reporting on this is it cannot be done in real time. If someone malicious gains access to Salesforce, that person has free reign to export data, make changes, etc. until they are caught. Once data has left Salesforce, there's no retrieval process. Ideally failed logins would be tracked in real time with a built-in alert process. However, most organizations don't have a monitoring solution in place (bit.ly/safeguardforsf). Therefore, reporting is the next best option.

How to Export Login History: Under Setup search for “Login History”.
You can export this data for easier reporting.



Wrap Up

Beyond the five items we mention in this chapter, what needs to be monitored in Salesforce is dependent on each organization, how Salesforce is being leveraged, and a number of other factors. Conducting a Salesforce Audit either internally or externally will help determine what items need to be checked and at what cadence (daily, weekly, monthly, quarterly). Once your organization hits a certain size/has a certain number of Users, investing in real-time monitoring solution like SafeGuard is a crucial step to keeping Salesforce secure. bit.ly/safeguardforsf

Conclusion

We hope you found this eBook helpful and are walking away with actionable insights on how to set up and manage a more secure instance of Salesforce.

Have questions about how to monitor your Salesforce instance in real time with SafeGuard? Request a demo today: bit.ly/ckcontactus

You may also like: **How to Eliminate Salesforce Maintenance Headaches**

bit.ly/howtosfheadaches

CloudKettle

Call us at 1-800-878-4756 ext 202
Find us on the web cloudkettle.com
Follow us on Twitter @cloudkettle
Read the Blog cloudkettle.com/blog
Visit us on LinkedIn
www.linkedin.com/company/cloudkettle