Security + Access manager

For Salesforce®

Best Practices for Managing Salesforce Security & Permissions

ApplicationPerfection

BURGESS
Cloud Consulting
For Salesforce®

Contents

Contents

Executive summary

With more focus than ever on what data we keep in our CRM and who has access to that data, we have produced this document to outline some of the best practices in making sure your Salesforce.com instance is secure and how to manage and maintain the permissions of your users. With many different types of users from sales to finance accessing the valuable data in your CRM, permissions can become complex. We have all heard numerous costly horror stories of internal and external data breaches. This is a critical area due to all the new data legislation such as GDPR, PIPEDA etc. By implementing the best practices outlined in this doc you can minimize your risk exposure.

Changes included in this edition

Based on feedback from the readers of previous editions we are now including an overview of security and permissions changes on our blog page.

Foreword & note on the Security + Access Manager App

"Through our experience working with our customers, we have produced this document to outline some of the best practices for managing security and permissions in Salesforce. When conducting a security and permissions review, we recommend using our App Security + Access Manager. Throughout this document we have incorporated top tips for how Security & Access Manager can save you time, money and effort in reviewing your Salesforce permissions. However, this whitepaper is meant to give guidance and add value to all Salesforce Admins, not just those using our App. We hope you get value from this White Paper. If there is anything additional you would like to see covered, please drop us a line at marketing@applicationperfection.co.uk and we will try to include in future versions. Hope you enjoy the read!"

James Burgess – Founder & CEO, Application Perfection LTD.

Understanding Salesforce permissions

With so many ways to grant access to Salesforce, it's worth doing some preparation to understand and update your knowledge and ensure you have designed the best security model for your business. Fortunately, with the Trailblazer Community there are some great trailheads available for you to use to upskill.

Trailheads available to you:

- **Security Specialist**: Flex your security muscles by locking down permissions and tracking changes.
- **Data Security**: Explains how to control access to your org, objects, fields, records, defining role hierarchies & sharing rules.
- **Protect Your Data in Salesforce**: Secure your Salesforce org by controlling login and data access for users.
- **User Management**: Set up users and control how they can view or edit your business data.
- **Sales Territories and Forecasting**: Set up Enterprise Territory Management and assign accounts, rules and users.
- **Sharing CRM Data with your Partners**: Learn how to use Salesforce settings to share CRM data securely with partners.
- **Cybersecurity Threat Prevention and Response**: Learn coding best practices to safeguard your Salesforce data.
- **Session-Based Permission Sets and Security**: Use session-based permission sets to limit access to data in your org.
- **Salesforce Mobile Application Security**: Secure the Salesforce mobile app and control access to Salesforce from mobile devices.
- **Shield Platform Encryption**: Encrypts your data in the cloud and manage the life cycle of your encryption keys.
- **Salesforce Optimizer:** Learn how to use Salesforce Optimizer to get insights into the health of your org.
- **Identity for Customers**: Use Salesforce Identity to engage your customers and attract new ones.
- **Security Basics**: Educate your users, protect your Salesforce org and encourage a culture of security.

Understanding the importance of permissions reviews and the risks of neglecting them

A Salesforce.com instance naturally evolves through new business requirements and onboarding new types of users. As your functionality evolves to meet new business requirements, permissions need to evolve as well.

Reasons why a permissions review may be necessary, if not an already a regularly scheduled activity:

1. Internal security breach may have occurred with data leaving the organization, perhaps through disgruntled staff.
2. External security breach.
3. Initial security model created for go live is out of date.
4. Onboarding of new business units requiring different access.
5. System Admin staff churn, the initial reasons why a security model has been setup may no longer be known.
6. Lack of a documented security model.
7. Compliance to HIPPTD, GDPR or other data legislation.
8. Increased support tickets from users querying data access.
9. Audit, risk or compliance teams may be requesting info.
10. Lack of user adoption as users are frustrated with not accessing the data they need or having too much access.
11. Less efficient search capabilities. With open orgs trying to navigate to the record a user needs can be a challenge.

Common pitfalls in security models

When external org-wide defaults are public, users can access all object data, a security risk. Removing fields from page layouts doesn't secure them in reports; field-level security is key. Despite disabling Excel export, users can still query data. API-enabled users can export data, necessitating careful API access control. APEX classes or triggers in system mode can override permissions, highlighting the importance of robust permission management.

Salesforce system level security best practices

Salesforce provides a variety of security settings, but effectively utilizing them falls to each customer. Our recommendations below highlight key best practices for maintaining the security of your Salesforce.com instance.

The focus is on achieving a balance: these practices are designed to enhance security while minimizing disruption to the user experience.

Security best practices:

1. **Critical updates review**: Regularly review Salesforce's critical updates for enhanced security, and conduct impact analysis.
2. **Password policies**: Implement stringent policies, including history, length, and complexity requirements (uppercase, lowercase, numbers, symbols, minimum 8 characters), and enforce password expiry.
3. **Login attempts**: Limit multifactor authentication login attempts to 3-5.
4. **Session lengths**: Set short session timeouts, with user warnings for re-login.
5. **IP restrictions**: Apply restrictions for certain user groups, focusing on office-based profiles.
6. **Org-wide defaults**: Start with a private model for internal and external users and adjust sharing settings as needed.
7. **Device management**: Ensure devices accessing Salesforce have updated browsers, anti-malware, and operating systems, in coordination with IT.
8. **APEX usage**: Limit APEX running in system mode to maintain security integrity.
9. **Single sign-on**: Implement for streamlined access and reduced support issues.
10. **Two-factor authentication**: Use tools like Salesforce Authenticator to increase security.

AECOM Group Security & Access Manager review:

“Amazing”

Security + Access manager
For Salesforce

“Useful on the first day of install - We have a very large org. Around 400 permission sets, 30+ profiles, 500+ objects, 50k+ users. It was extremely painful to figure out who changed what permission when, and which profiles had what access to objects and fields. It would usually take us hours to update object permissions on various profiles and permission sets by clicking though setup. Once we installed this application, it became super simple! We were able to use it immediately to remove deleted permissions from several permission sets at once. I love the simplicity of the UI. The data dictionary is a nice add too. James is always SUPER responsive and helpful if there’s an issue. Wish I could rate this more than 5 stars!”

Salesforce user level permissions best practices

Here are some of the best practices we recommend implementing at a user/profile level. It's important to ensure your users have the access they need without overly exposing data they don't need. Sys Admins regularly get asked for more access to data. However, our CRM's contain massive amounts of data over exposure to too much data can make the system less usable. Too much data requires more effort searching for the right record. Equally there is a security risk of data breaches.

Ask the difficult questions, does a sales person really need access to all opportunities in Salesforce? Take the time to focus on security & permissions, put that nagging worry of a data breach away. Sometimes it's hard to focus on this area when you have multiple stakeholders to please, but security is never a big deal until something goes wrong and then it is a big deal! Make your stakeholders aware of the impact of not doing a review and they will prioritize it.

Permissions best practices:

1. **Profile and permission sets** – Be aware of the API Enabled, Report Builder, Export Reports, View All Data, Modify All data and View Encrypted Data permissions. These profile permissions will override any further sharing settings you have created. A user with the View Encrypted Data permission can see the non-encrypted version of each Encrypted Text field you have.
2. **Object level security** – Try to avoid using view all or modify unless necessary. This will override any sharing settings you have defined.
3. **Field level Security** – Many organizations store more information on their customers than their employees need to see to complete their job. Be aware of what specific data points each employee can see. This can reduce the damage a breach causes and help identify the leak source.
4. **Page layouts** – Remove any unnecessary fields from page layouts. This makes the user experience more efficient, however remember to lock them down in field level security as well. If a user has access to the fields, they can still report on them, even if they aren't in the page layout.
5. **Record Sharing Settings** – Use this to reduce the damage caused by a data leak. An employee can only export records they have access to. Establish your standard security model and allow users to share additional records with one another where necessary in their jobs.
6. **Role Hierarchy & territory management** - Ask some tough questions: Do Managers really need access to all data across the organization, or just their team's data? Does everyone in your sales team really need access to all leads, or can they be split up by territory, area, industry?
7. **APEX sharing** – As soon as you start using APEX sharing it becomes more difficult to audit and review and takes a developer to make changes. Stick to standard methods if possible.

8. **Reports & Dashboards** – A user with Export Reports, Report Builder and "View All Data" permissions can quickly and easily build a report of all your data or use a data export tool to query it. Then they can export that data. Ensure users can only access reports that they need. Watch out for reports and dashboards with a specific point in a hierarchy saved. A user may see a hierarchy view saved in a dashboard but when they drill down not see all the underlying data. Ensure they are not public and that only appropriate users have access to them. Inspect your reports and dashboards to make sure there are appropriate filters on each report (such as only selecting My Records instead of All Records). With report builder so easy to use, it’s worth scheduling regular reporting reviews to remove unnecessary or draft reports
9. **Exporting Salesforce Data** – It’s possible to remove the exporting data permissions from your organization, however this does not completely block users from exporting data. For this you need to remove their access to the records. The best approach is to add friction to employees attempting to export data by disabling, Printable view, Report export permission, however this means as a Sys Admin you must upskill your users in how to build reports in report builder. Or provide the exact reports they need in Salesforce, many users will be used to working in Excel and will be frustrated if they can’t get the reports they need.
10. **API Enabled users** – Users with this permission can use data export tools to pull all records they have access to out of Salesforce. Use this for interfaces only where possible.

Innovation, Science and Economic Development Canada review:

“Excellent way to audit permissions and profiles in org”

“Understanding which profiles and permission sets have particular object and field permissions is not easy to review and audit. When someone can access something that they shouldn't be, understanding where the problem is can be extremely challenging. This app has been amazing in helping us! We can diagnose issues very easily and is super useful to ensure all profiles and permission sets have the correct settings. Also a life saver when we started to move things away from profiles and into permission sets. Highly recommend for every org!”

Conducting a permissions review

In this section we suggest best practices around the steps that you should take when conducting permissions reviews. Please note that not all steps may be relevant to every permission review you conduct. They are suggestions on steps you can take but may vary on the scale of the permissions review.

For example, if you are trying to fix a bug from a support ticket to an end to end compliance review. Equally you may be using a release management tool. Try to think of these steps in the context of your existing processes.

1. Define objectives

There are many reasons to review permissions from a regular review for your IT governance team to rolling out access to a new user group. Before starting it’s always best to set clear objectives that you can track your effectiveness against. Don’t bite off more than you can chew. It may be that you want to conduct an end to end review but due to competing business requirements you may need to plan this entire activity into manageable chunks over several releases.

2. Define ownership & access sign off

As a Sys Admin, while you oversee the CRM system's security, delegate the approval of user access levels to the appropriate stakeholders. Document the data access permissions for each user type and have stakeholders confirm their accuracy. This approach helps prevent future issues. If access queries arise, you can refer to the documented, stakeholder-approved setup. Involving your compliance or audit teams for their advice can also be beneficial.

Typical system access owners and stakeholders:

- IT systems governance
- Business process owners
- CRM systems owners
- Business unit managers
- Information owners and stewards
- Compliance teams

3. Identify risk areas in access to sensitive data

It's worth taking the time to identify where you are storing sensitive data in your CRM. This may take the form of external customer data that you have a duty of care to protect such as contact info, DOB, profiling info etc. or corporate sensitive data such as pipeline info that you might want to restrict by user group, geographic region etc. Once you know exactly where your sensitive data is you can then review access, remove duplication and make sure just the users that need it have access.

4. Data protection & legislation

Understand the data legislation that applies to your org. We are sys admins not legal professionals; however, we should have a good business understanding of the data legislation. This may affect what we allow our users to see in our CRM. Once you have an outline understanding ask your Legal team for advice and perhaps ask them to sign off that the controls you have put in place are enough.

Example of a light Risk Reduction Operational Plan

A Risk Reduction Operational Plan is a strategic document or framework used by organizations to identify, assess, and mitigate risks that could impact their operations. Here are some actions you can take in that area:

1. Profile data use and authorization structure
2.Identify critical data
3.Reduce excess access to data
4.Identify key users and owners
5.Define and implement data governance policies

5. Review where you are today

Before granting access to a new CRM user group, ensure you have clearly identified who is responsible for user access within your organization and located all sensitive data storage. It's vital to evaluate the current access levels to determine if the existing permissions framework can accommodate more users without introducing undue complexity. Ensure your current configuration is formally approved —share an 'as is' document with the pertinent stakeholders that outlines the current setup and the anticipated changes or effects of your implementation. Consider asking the following questions:

1. Struggling to see the forest for the trees? Begin by examining if there are any unused permission sets, profiles, roles, etc., that are redundant or could be consolidated or removed. Cleaning up these elements first will simplify the review process of what remains.
2. Can your existing permissions setup support the new or change to permissions? If so, leverage those avoiding adding more complexity, unless truly necessary.
3. When expanding your current setup to include new users, consider whether this extension impacts the access levels of existing users and whether these changes require formal approval.

6. Document new model

When implementing a change to existing permissions or onboarding a new user group, take the time to document it thoroughly, from both a technical and business standpoint. Documenting the technical side will make management easier moving forward and help educate new sys admins that will be managing the security setup in the future. From a business perspective documenting the access at this point will then allow you to succinctly go to the business owner and ask for sign off on the setup.

6. Create new model

Think about all the options available. Remember its always harder to lock down permissions than open them up. So, think about going with a more restrictive model to start with. You can always open it up later. Following your own release management process create the new permissions settings. Potentially in a sandbox. It is always important to create a test version of the model before approaching stakeholders for sign off. This avoids them signing of on something you can’t deliver.

7. Sign off new permissions

Once you have documented the new model, approach the relevant permissions owner to sign off your understanding of the access required.

8. Test. Deploy. Test.

After implementing the new permissions functionality, conduct thorough testing by simulating the login process for several users. Consider drafting a test script for a Business Analyst to carry out. It's essential to evaluate the effects of the new permission settings on the existing configurations to prevent any issues or inquiries from users regarding changes in their access. For instance, modifying a sharing setting for a specific role could inadvertently alter the access levels for other roles within the hierarchy. Once you've conducted these tests and are confident that everything operates as anticipated, proceed with deploying the changes to your production environment. Following deployment, it's advisable to perform additional tests in the production setting, as it may differ from your test environments, to ensure everything functions correctly.

9. Communicate

Always communicate the change, the impact, the timing and the reason for it to effected users.

Regular permissions maintenance reviews

Great, you have conducted an end to end security & permissions review. You can put that worry out of your mind and get on with delivering the fun new stakeholder requirements. Yep, well for a short time at least until the worry starts nagging again.

Once you have conducted an end to end permissions review, don’t let it get out of control. Schedule regular reviews into your release management process, or book in a time for your next review. These things can easily become outdated and it is best to document any changes as you go along, following the steps above for any changes to permissions.

Stay up to date with Salesforce releases. With every new release there are more permissions and security functionality added.

Mitigating the impact of a Salesforce data breach

What is a data breach?

A data breach is essentially an incident where data is taken or stolen from a system without authorization of the owner. It's important to differentiate this from other cybersecurity attacks.

Security basics

There is a great Security Basics Trailhead module to give you a high-level understanding of how to educate your users, protect your Salesforce org, choose the right Salesforce security settings and encourage a culture of security.

Perform an audit of your existing access model and agree access moving forward

Please relate to the previous section describing how to conduct a security review.

Organize an expert response team

If the unthinkable happens and you experience a data breach. Its best to be prepared in advance with a response team including legal, IT, HR, operations, communications, investor relations staff, and management experts. This team will oversee dealing with the aftermath of a breach in all aspects of your business.

What is the impact of a data breach?

Data breaches have a range of negative consequences including legal fines such as we saw with BA receiving a multimillion-pound GDPR fine, to broken customer trust, impact on company reputation, loss of existing or new business, and lawsuits that result in hefty fines.

Create a communications plan

Now is the time for transparency and communications both internally and externally. Companies that try to bury the extent of their breach, like Uber, often experience much worse consequences in customer backlash. Consider all stakeholders in the plan, including business partners, investors, employees, and customers. Deliver a clear statement that is open and thorough without divulging information that could add risk.

Data access risk scenarios

Internal Risk:

- Data Breaches: If users are granted access to sensitive data that they don't need, it increases the risk of data breaches. This can result in the loss of confidential information, which can be costly for the company.
- Data Manipulation: Granting users with inappropriate access can lead to unauthorized modifications of data. This can result in inaccurate data, which can negatively impact decision-making and customer relations.
- Legal Violations: Allowing users to access data that they shouldn't have access to, can violate legal regulations, such as GDPR. This can result in hefty fines and damage to the company's reputation.
- System Integrity: Granting users with the wrong level of access can also negatively impact the system's overall security and integrity.

Why secure internal user access to data?

It is important to ensure that users have access to only the data that they need to perform their job duties.

Controlling employee access to CRM data is important to protect sensitive information and maintain data security.

Best practices to consider:

- Role-Based Access Control: Implement role-based access control (RBAC) to limit user access to CRM data based on their job responsibilities. This ensures that employees only have access to the data they need to perform their duties.
- Need-to-Know Access: Limit access to sensitive information and data to only those employees who require access to complete their work.
- Regular Access Reviews: Conduct regular access reviews to ensure that employees only have access to necessary data and revoke access for those who no longer require it.
- Access control: Ensure that only authorized personnel have access to the CRM database. Limit access to only those who require it to perform their job functions.
- Authentication: Implement strong authentication protocols such as multi-factor authentication (MFA) to prevent unauthorized access to CRM data.
- Training: Provide regular training to employees on data security and the importance of protecting sensitive data.

External Risk:

- Identity Theft: One of the greatest risks of data breaches is identity theft. Cybercriminals can use stolen personal information such as Social Security numbers, dates of birth, and credit card information to open fraudulent accounts or make purchases. This can cause significant financial and emotional damage to individuals.
- Financial Loss: Data breaches can result in financial loss for individuals and organizations. Cybercriminals may use stolen financial information to make fraudulent purchases or unauthorized transactions.
- Reputation Damage: Data breaches can damage the reputation of individuals and organizations. Customers may lose trust in a company that has experienced a data breach, resulting in reduced sales and potential legal action.
- Legal Consequences: Data breaches can result in legal consequences for individuals and organizations. Lawsuits can be filed for negligence in protecting personal data or for failing to comply with data protection regulations.
- Operational Disruption: Data breaches can disrupt operations for organizations, causing downtime and loss of productivity.

Why secure external access to data?

The risks of data breaches can be significant and potentially devastating for individuals and organizations.

It is important to take appropriate measures to prevent data breaches and protect personal and business data.

General Data Protection Regulation (GDPR) outlines various fines and penalties for organizations that fail to comply with its regulations. Fines can be as high as 4% of an organization's global annual revenue or €20 million, whichever is higher. It's important to take GDPR compliance seriously and ensure that your organization is following the regulations to avoid potential legal or financial repercussions.

Financial Risk:

- Data breaches: If CRM data is not properly secured, it can be vulnerable to data breaches, which can compromise sensitive financial information.
- Compliance violations: CRM data in finance is often subject to strict regulations, so if the data is not properly managed, it can result in compliance violations and legal penalties.
- Data accuracy: CRM data must be accurate in order to be useful, but if the data is not properly maintained, it can become outdated or inaccurate, leading to poor decision-making.
- Privacy risks: CRM data often contains personal information, so if the data is not properly secured, it can result in privacy violations and damage to the reputation of the financial institution.

To mitigate these risks, it is important to have strong data security protocols in place, as well as regular data audits to ensure that the data is accurate and up-to-date.

Security & Access Manager product overview

Product overview

The Security & Access Manager app reduces the time, effort and cost necessary to establish, manage and audit security and access rights. Simple, consolidated tabs enable your administrators to make multiple updates with the click of a button. Clear and concise automated excel and pdf exports of your security setup provide you with a digestible format to make meeting internal audit and compliance requirements far more efficient and user friendly. Query why a user can access a record in seconds rather than having to search through your permissions setup. Track where your sensitive customer or company confidential data is across you Salesforce instance. Mass update help and description text on fields and create profile specific data dictionaries. Reducing support and training time.

Benefits to admins

- Review and update multiple profiles and permission sets from simple screens
- Check and amend which users can access sensitive data in your CRM
- Log the changes you make to permissions and roll back if necessary
- Produce colour coded spreadsheets of your object and field level permissions across profiles and permission sets
- Query an existing security setup or test a new one. Simply select the user and entering an id
- Understand why a user can see a record and what they can do on a record at the touch of a button
- Reduce support tickets by ensuring your users have access to the right records
- Reduce documentation time
- Work with your team to review field descriptions and help text

Security +
Access manager
For Salesforce®

Security & Access Manager Product Overview

Benefits to audit & compliance

- Remove risk of employees accessing and downloading confidential company info they don't need
- Avoid data protection legislation fines by tracking and reporting on where your sensitive data is in Salesforce and make sure access to this data is relevant
- Save time meeting internal audit/compliance/SOX/GDPR requests with export of security setup to Excel and PDF
- Create easily understandable color coded spreadsheets of which objects and fields users can access

Benefits to users

- Improve search by just exposing relevant records and info
- Ensure users can create read and update the records they need
- Improve usability of report builder by only exposing relevant fields to your users
- Produce user specific data dictionaries for users based on their access post training

Useful additional content

There is a wealth of documentation available. It seems with every new Salesforce release more security and permissions capabilities are added. Please see some of the documentation we find useful listed below.

- **Protecting your Salesforce Organization**: Salesforce is built from the ground up to protect your data and applications. You can also implement your own security scheme to reflect the structure and needs of your organization. Protecting your data is a joint responsibility between you and Salesforce. The Salesforce security features enable you to empower your users to do their jobs safely and efficiently.

- **Session Security**: You can change the session connection type, timeout restrictions and IP address ranges to protect against malicious attacks and more. This document explains what each session setting means. After logging in, a user establishes a session with the platform. Use session security to limit exposure to your network when a user leaves the computer unattended while still logged in. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session. Choose from several session settings to control session behavior.

- **Salesforce Shield Overview**: Salesforce Shield is a trio of security tools that Sys Admins and Developers can use to build a new level of trust, transparency, compliance and governance right into business-critical apps.   It includes Platform Encryption, Event Monitoring and Field Audit Trail. Ask your Salesforce administrator if Salesforce Shield is available in your organization.

- **Salesforce Release Notes**: We have included permissions related release notes on our Application Perfection blog to make it easier to keep up with the updates.