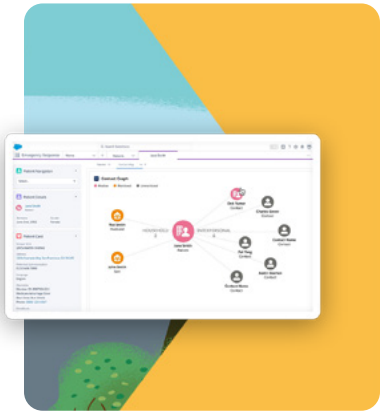
WORK.COM

Security and Compliance Best Practices and FAQ



The Work.com Workplace Command Center and Contact Tracing are built on the Salesforce Platform, which has robust security controls in place. **Shift Management** is also built on the Salesforce Platform, with the optimization functionality leveraging ClickSoftware (more details below). Trust and compliance documentation for all Salesforce products can be found here.

Work.com Security Best Practices

Salesforce believes in a defense in depth approach, which means that there are multiple security countermeasures to protect all information assets. This includes the code that runs Salesforce, the infrastructure that supports the application, the multiple factors of authorization, and the authorization required for logical access. Salesforce works to incorporate privacy and data protection concepts from the inception of each new service or feature it offers.

Some key aspects to remember about the inherent Salesforce defense in depth approach when purchasing Work.com:

- Salesforce agrees by contract that its personnel may access personal data only in accordance with our customers' documented instructions for specific purposes, including processing under the contract, processing initiated by the customer in using the services, and processing to comply with other instructions provided by the customer.
- Salesforce application and website are monitored on a 24/7 basis for reliability and performance by the site reliability team.
- We have one of the best computer security incident response teams (CSIRT), which runs in parallel with site operations to provide 24/7 monitoring and incident response. CSIRT receives and reviews threat alerts from a variety of sources, leveraging heuristic detection as well as other third-party vulnerability intelligence feeds.
- We have third-party security firms provide periodic vulnerability scanning and continuous perimeter monitoring to detect changes in IP addresses or ports opened, service versions, and certificate expirations.
- See this white paper on Salesforce's approach to security for more information.

FAQ

Given the sensitivity of the data collected, are there recommendations on how to configure the Workplace Command Center org securely?

Work.com is required to be installed in a new org to ensure that employee data is protected with proper application access controls. A common data access control anti-pattern is the excessive provision of System Administrator profiles. It is *critical* for a Work.com implementation to follow best practices around least privilege, or limiting access rights for users to the bare minimum they need to perform their work. If this principle is not followed, sensitive or private personal data (or personal health data) about employees may be exposed to others. To secure its workplace command center, Salesforce administrators can implement the following:

- Require multifactor authentication, which provides an effective layer of protection against one of the greatest threats to your org: credential abuse ("loaned," guessed, or stolen passwords). The Salesforce Authenticator is included with all Salesforce orgs, and is easy to implement and use.
- Use single sign-on to validate users against your own corporate user database.
- Use profiles and permission sets to define access to objects and fields.
- Use organizationwide sharing defaults to set the baseline level of access to your records.
- Use role hierarchy, sharing rules, or Apex sharing to open up record access beyond the organizationwide defaults.
- Restrict where and when users can log in to Salesforce.
- Set complex password policies.
- Use session security to limit exposure to your network when a user leaves the computer unattended while still logged in.
- Check out this data security Trailhead module and this Salesforce security guide to learn how to use these features.
- Develop a plan for monitoring your org's security settings. Security Health Check is a good (free) tool within your org for identifying and fixing potential vulnerabilities.
- Natively encrypt PII, PHI, sensitive, confidential, or proprietary data at rest (see below for additional information).

What can I do if I see something suspicious related to my Salesforce implementation? Report it to security@salesforce.com, in addition to your own IT or security team. Trust starts with transparency. That's why Salesforce displays real-time information on system performance and security at trust.salesforce.com. For security-specific information, go to trust.salesforce.com/security. This site provides live data on system performance, alerts for current and recent phishing and malware attempts, and tips on security best practices for your organization.

How can I monitor and audit activity within the Workplace Command Center? How can I see who is accessing records? Leverage the Setup Audit Trail feature to monitor activity performed by your administrators, including the creation, disablement, and changes to permissions of user accounts (along with other configuration/metadata changes). Setup Audit Trail records are retained for 180 days. To retain them longer, extract them via API, the data loader tool, or event monitoring.

- **Login History:** You can review a list of successful and failed login attempts to your organization for the past six months. Login history older than 180 days can be downloaded. You can review which login activity is suspicious to prevent identity fraud in Salesforce. The history provides you key user access data, including the average number of logins per user per a specified time period, who logged in more than the average number of times, who logged in during nonbusiness hours, and who logged in using suspicious IP ranges.
- **Event Monitoring**: You can review granular event logs that cover most activities occurring in a Salesforce org. Event Monitoring enables you to identify which users viewed or exported which records. It is also valuable for monitoring security, troubleshooting performance of your custom code, and assessing adoption and usage patterns (including auditing privileged-access users). With Event Monitoring, you'll also get access to Threat Detection, which uses statistical and machine learning methods to detect threats to your Salesforce org.
- Record Modification Fields: All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.
- Setup Audit Trail: Administrators can also view a Setup Audit Trail, which logs when modifications are made to your organization's configuration. See Monitor Setup Changes with Setup Audit Trail.
- Field History Tracking: You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing. See Field History Tracking (note: this functionality is not yet available for the Employee Object, Internal Organization Unit Object, Employee Crisis Assessment Object, or Crisis Object).
- Field Audit Trail: Retain field history data for more than 18 months and up to 10 years with Field Audit Trail (note: this functionality is not yet available for the Employee Object, Internal Organization Unit Object, Employee Crisis Assessment Object, or Crisis Object).

Can I associate my Employee data from other objects in one place?

Employee has a lookup to the Individual object. The Individual object can act as a junction object between Employee and other objects that represent individuals. PersonAccount, for example, is sometimes used to represent employees. Data synchronization is still required, depending on your own data model. The Command Center package ships with triggers that are designed to populate Individuals based on Employees, and associate Individuals to Users based on the Employee Number field. More information can be found here.

Additionally, high-level consent fields exist on the Individual object, if the customer chooses to use them (for example, profiling, tracking, geotracking, processing).

How can I prevent users from running reports with sensitive data or exporting records?

Transaction Security is a feature that is packaged with Event Monitoring and is commonly used for data loss prevention. It provides the means of blocking specific user activities, requiring escalated authentication before specific actions are permitted, or simply notifying an administrator of the user action. Check out this Transaction Security Trailhead module to get started.

Can I encrypt the data at rest?

Yes, a recent update as of August 1, 2020, allows customers to encrypt standard fields within the Employee object using Platform Encryption for an extra layer of security. To enable Platform Encryption for the Employee object, please reach out to your account team.

Please keep in mind that encryption solves for a very specific risk vector, and few regulations require encryption. As mentioned above, Salesforce has strong security measures in place for all data. If you have additional concerns, please reach out to your account team, who can connect you with a Security Architect to discuss further.

Is there a way to mask this sensitive data in my sandbox?
Data Mask allows you to obfuscate, pseudonymize, or delete the data in whichever fields you specify, thereby fully supporting development and QA efforts while adhering to your organization's least privilege data access model. Data Mask is 100% native to the Salesforce Platform, avoiding the need to vet the security and compliance of a separate platform. Obfuscating contact details in lower environments could also avoid accidental communications to data subjects resulting from development and testing activities.

What mobile security features are available for users who access Work.com from their phone?
Application access controls can be applied for Salesforce mobile through flexible connect app policies. Example protections include blocking copy/paste functionality or file sharing, as well as encrypted data storage. Integrated mobile app management (add-on) allows jail break detection, detecting man-in-the-middle attacks, device blacklisting, rogue network access, and logging screenshots and email interactions. See this datasheet for more.

Where does Work.com data reside?
A new org created for Work.com will be provisioned in the same region as your existing org: US, EMEA, UK, APAC, Canada, and Australia.

All data for Contact Tracing and Shift Management is stored on infrastructure managed by Salesforce. Shift Management will use the underlying field service capabilities of optimization, which calls out to an AWS-hosted optimization engine service that Salesforce runs. This engine does not store any data, and is encrypted in transit.

Find where your instance is located here.

If I am a U.S.-based company, but have employees in other countries with data residency regulations, do I need a separate org for each country?
We offer our customers international transfer mechanisms via our data processing addendum that incorporates the following transfer mechanisms: our processor binding corporate rules and the standard contractual clauses as approved by the European Commission. To read more about data transfers, check out this FAQ.

If there is a specific requirement for data to remain within a country, you can request for your new Work.com org to be in the following regions: EMEA, UK, APAC, and AMER.

Is Work.com included in your compliance efforts (for example, ISO certifications or SOC reports)?
work.com is currently not in scope for ISO certifications or SOC reports during the period of November 2019 through May 2020.

I've already purchased Shield licenses. How can I use them with Workplace Command Center?

- **Event Monitoring**: You can review granular event logs that cover most activities occurring in a Salesforce org. Event Monitoring enables you to identify which users viewed or exported which records. It is also valuable for monitoring security, troubleshooting performance of your custom code, and assessing adoption and usage patterns (including auditing privileged-access users). With Event Monitoring, you'll also get access to Threat Detection, which uses statistical and machine learning methods to detect threats to your Salesforce org.
- Transaction Security is a feature that is packaged with Event Monitoring and is commonly used for data loss prevention. It provides the means of blocking specific user activities, requiring escalated authentication before specific actions are permitted, or simply notifying an administrator of the user action. Check out this Transaction Security Trailhead module to get started.

- A recent update as of August 1, 2020, allows customers to encrypt standard fields within the Employee object using Platform Encryption for an extra layer of security. To enable Platform Encryption for the Employee object, please reach out to your account team.
- Field Audit Trail support for the objects that comprise Workplace Command Center is coming soon (safe harbor).

How does the manual Contact Tracing solution work? Does this solution require the collection of sensitive or special categories of personal data?
Refer to our privacy FAQ.

Can I use Shield (Field Audit Trail, Platform Encryption, and Event Monitoring) with Contact Tracing?
Yes.

What is the Employee Wellness Check? Does it require the collection of sensitive or special categories of personal data?
Refer to our privacy FAQ. Employee Wellness Check surveys bundle all symptom and exposure questions into a single yes/no attestation, so customers do not associate employees with specific symptom or exposure data.

Contact Tracing for Employees mandates only one field (Last Name), encouraging customers to keep collection of unnecessary data to an absolute minimum.

Can managers see employees' Wellness Status when using Shift Management?
No. Shift Management only surfaces employees' availability (such as available/not available), so that managers won't see employees' Wellness Status directly in their workflows. This preserves employees' privacy, helps avoid bias, and keeps access to a "need to know" basis. Learn more here.

Is Work.com HIPAA compliant?
Refer to our privacy FAQ.

How did Salesforce build Work.com with privacy and ethics in mind?
Refer to this post to learn more, such as these survey design considerations for maintaining data privacy.

Will work.com be available to be deployed in Government Cloud?
At this time, the Workplace Command Center and Shift Management managed packages are not included in scope for FedRAMP.