



# Salesforce Government Cloud

## Background

Federal, state, and local government agencies and government contractors trust Salesforce's cloud-computing platform to deliver critical business applications. This is largely because of Salesforce's commitment to security and privacy. Salesforce's vision is to be government's trusted Cloud Service Provider (CSP), based on the values of maintaining the confidentiality, integrity, and availability of customer data. Salesforce's methods to fulfill this vision are built upon an executive commitment to ensure and continuously improve the security of Salesforce's services, and include:

*"Nothing is more important to our company than the privacy of our customers' data."*

— Parker Harris, Co-founder, Salesforce

- **Defense-in-depth:** whenever possible, multiple controls and technologies are applied to limit the possibility of any single point of failure.
- **Investment:** in personnel, tools, and technologies to manage, analyze, and improve security effectiveness.
- **Transparency:** trust cannot be maintained without open communications regarding service performance, reliability, and security, and to that end Salesforce strives to be the industry leader in transparency. See [trust.salesforce.com](https://trust.salesforce.com) for further details.

## Deployment Model

Salesforce's deployment model is a "public" cloud infrastructure, as defined by NIST 800-145. In the Salesforce Cloud, an agency dynamically provisions computing resources over the Internet on our multi-tenant infrastructure. This is a cost effective deployment model for agencies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability.

As a Software as a Service (SaaS) and Platform as a Service (PaaS) leader, data security is of utmost importance for Salesforce. Salesforce serves over 100,000 customers and processes over three billion transactions a day. The organizations that use Salesforce include customers in heavily regulated industries such as financial services, healthcare, insurance, and public sector that require strict adherence with security and privacy requirements. Salesforce raises the bar of security to meet the requirements of our customers, specifically customers in heavily regulated industries such as Public Sector, by maintaining numerous security and privacy certifications.



## Salesforce Government Cloud

As part of our commitment to our Government Customers, Salesforce has made the investment to create a government specific cloud to address the FedRAMP requirements for cloud computing. In May 2014, Salesforce became the first CSP to attain a **FedRAMP Authority to Operate** for both Software as a Service (SaaS) and Platform as a Service (PaaS), consistent with the FedRAMP moderate baseline controls. The Authority to Operate was granted by the US Department of Health and Human Services for the Salesforce Government Cloud (described in more detailed below).



The Salesforce Government Cloud is a partitioned instance of Salesforce's multi-tenant public cloud infrastructure, specifically for use by U.S federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs). The isolated production infrastructure supporting the Salesforce Government Cloud Customer Data ensures that the physical hardware is separate from hardware supporting other customers. While isolated, the underlying infrastructure supporting the Salesforce Government Cloud is the same trusted architecture model that supports Salesforce's multi-tenant public cloud offering and over a billion customer transactions a day.

Access to systems and permissions, which could permit access to Customer Data inside of the Salesforce Government Cloud, is restricted to Qualified U.S. Citizens. Qualified U.S. Citizens are individuals who are United States citizens, and are physically located within the United States when accessing the Salesforce Government Cloud systems; and have completed a background check as a condition of their employment with Salesforce<sup>1</sup>.

---

<sup>1</sup> This excludes telephone calls for support that may initially be responded to by individuals who may not be Qualified U.S. Citizens and who may be located outside the United States. These individuals will then route cases to a team of Qualified U.S. Citizens.

## Government Cloud compared to Public Cloud

 government cloud	
Identical core hardware	
Identical core code base	
Multitenant infrastructure shared w/ <a href="#">government</a> <sup>2</sup> customers	Multitenant infrastructure shared w/ <a href="#">public</a> customers
<a href="#">FIPS 140-2</a> validated 128-bit or 256-bit AES encryption in transit (TLSv1, 1.1, 1.2)	128-bit or 256-bit ( <a href="#">RC4</a> ) encryption in transit (TLSv1.0, 1.1, 1.2)
<a href="#">FIPS 140-2</a> validated 128-bit AES Encrypted Custom Fields	128-bit AES Encrypted Custom Fields
Support provided by U.S. based, <a href="#">U.S. Citizens</a>	Worldwide follow the sun support
ISO 27001, SOC 2, PCI, HIPAA, and <a href="#">FedRAMP</a>	ISO 27001, SOC 2, PCI, HIPAA
Premiere+ Support <a href="#">included</a>	Premiere+ Support not included

## FedRAMP Authority to Operate (ATO)

The Salesforce Government Cloud information system and authorization boundary, is comprised of the Force.com Platform, Salesforce Services (Sales Cloud, Service Cloud, Chatter), and the backend infrastructure (servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS).

In order to maintain compliance with FedRAMP<sup>3</sup>, Salesforce conducts continuous monitoring on the Government Cloud. Continuous monitoring includes ongoing technical vulnerability detection and remediation, remediation of open Compliance related findings, and at least annual independent assessment of a selection of security controls by a third party assessment organization (3PAO).



<sup>2</sup> U.S federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs)

<sup>3</sup> Salesforce's ongoing commitment to compliance with FedRAMP will be focused solely on the Government Cloud environment. Any potential future modifications required to comply with ongoing enhancements to FedRAMP will be addressed in the Government Cloud. All FedRAMP and other Federal Government security related procedures and documentation will be focused on the Government Cloud.

Federal government Agencies can request access to the Salesforce FedRAMP Agency ATO package by submitting a request to the FedRAMP PMO. All other customers can submit a request to Salesforce via the customer's account representative. Each customer will need to review the documentation and assess that organization's compliance requirements. Customers may need to purchase additional Salesforce and/or third party products and services in order to meet their individual requirements.

## Products Available



The Enterprise Edition and Unlimited Edition of some Salesforce products are available for use on the Salesforce Government Cloud. For a list of available products on the Salesforce Government Cloud<sup>4</sup>, see: <http://sfdc.co/GovernmentCloudProductsList>.

---

<sup>4</sup> From time to time, the list of available products on the Salesforce Government Cloud may change at Salesforce's sole discretion and without any advance notice. Prior to a Government Customer placing an order on the Salesforce Government Cloud, please contact your local Salesforce sales or renewal representative for the most current product availability information on the Salesforce Government Cloud.