Splunk Connected Experiences

The Power of Splunk Wherever You Are

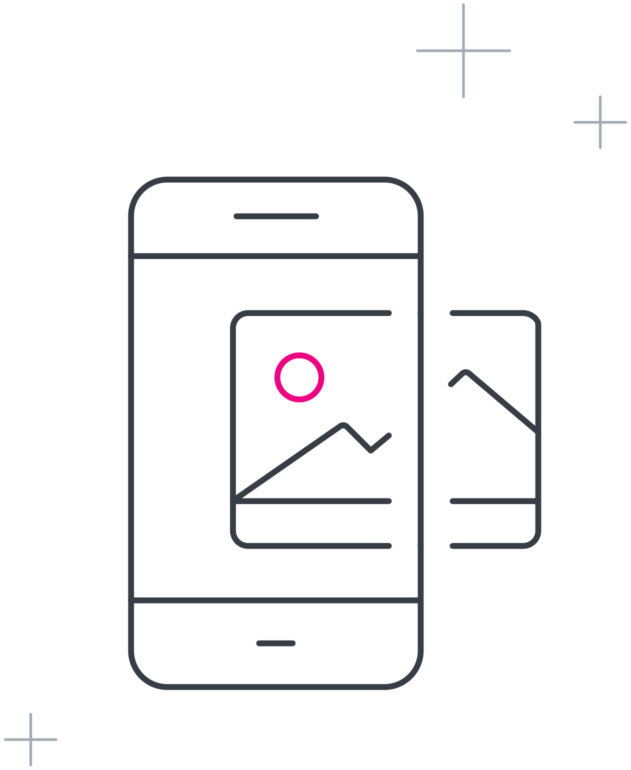
splunk>®
turn data into doing™

Table of Contents

Introduction to Splunk Connected Experiences

Splunk already provides great value in the office at your desk with beautiful visualizations and dashboards. What if you can take that experience on the road? Splunk Connected Experiences lets users consume, interact and take action on data while on the go.

This whitepaper introduces the Connected Experiences product line, explains the system that works behind the scenes to power the connected applications, and provides a helpful overview for deploying Connected Experiences in your organization.



Welcome to Connected Experiences

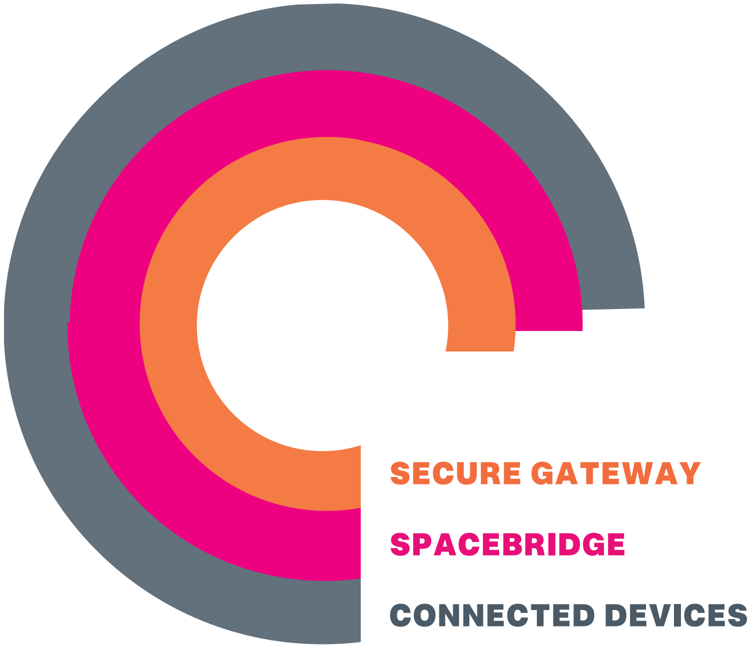
Take the capabilities of Splunk beyond the desktop with the Connected Experiences apps. Everyone in your organization can access data and see insights on the go with Splunk Mobile, Splunk for iPad, Splunk TV, Splunk Augmented Reality (AR), and Splunk Virtual Reality (VR).

Backend Products.

Two products facilitate the secure transfer and management of your Splunk data.

Splunk Secure Gateway

Splunk Secure Gateway, or SSG, is a Splunk app that lets you administer and manage your fleet of mobile devices at scale. It's also where authorized users can register their mobile devices.



Spacebridge

Spacebridge is a cloud-hosted service that securely routes data between Splunk platform instances and connected devices. As of February 2021, Spacebridge has been certified to meet SOC2, Type 2, and ISO27001 standards and is HIPAA and PCI-DSS compliant.

Welcome to Connected Experiences

Now that you're familiar with the products that enable the Connected Experiences apps, get to know the apps that empower your organization to do more with data:

Splunk Mobile

View mobile-friendly dashboards, receive and take action on alerts, and stay up to speed with your business wherever you are from your mobile device.

Splunk AR

Experience your data in augmented reality. Splunk AR users can scan an asset, spatially interact with live data, and take action with guided workflows to troubleshoot real machines and more.

2:35
Dashb
CMC - Cloud
Favorite
Cloud M
Overview
12 visualizations
Indexing Performance
5 visualizations · nobody · Viewed:
Indexes and Storage
5 visualizations · nobody · Viewed: 02:34 PM
Index Detail
6 visualizations · nobody · Viewed: 02:34 PM
Skipped Scheduled Searches
7 visualizations · nobody · Viewed: 02:35 PM
Search Performance Analysis
2 visualizations · nobody · Viewed: Friday
User Activity
7 visualizations · nobody · Viewed: Friday
User Detail
10 visualizations · nobody · Viewed: Friday
Alerts
Dashboards
2:33
Overview
12 visualizations
Search Count (Yesterday)
Last updated just now
16,770
↑ 2,558
Searches by Type (Last 24h)
Last updated 15s ago
6:30 PM
ad hoc 193
scheduled 14
summarization 4
other 0
500
400
300
200
100
0
1:20 AM
9:40 AM
6:00 PM
Throughput by Index (Last 24h)
Last updated 15s ago

Splunk for iPad

View dashboards optimized for the larger iPad real estate, all while taking advantage of its portable and interactive nature with unique dashboard annotation and note features.

Splunk TV

Imagine a whole NOC or SOC full of TVs with easy-to-navigate, beautiful Splunk dashboards. Swipe through dashboard slideshows, organize your data, and focus on charts with Splunk TV.

Splunk VR

Explore your data and collaborate with others on an infinite canvas in virtual reality.

Backend Breakdown

Where does my data go?

We know that data is your most valuable asset. Here's how Connected Experiences keeps your data safe.

Secure Message Patterns

Every Connected Experience product delivers the right data to the right user's authorized device.

To do this, all devices must be registered under local or Security Assertion Markup Language (SAML) Splunk accounts. Behind the scenes, device registration is a means to exchange public keys between the mobile device and the Splunk instance. Once keys are exchanged, Spacebridge allows messages to flow from the mobile device to the Splunk platform instance and back.

Messages are encrypted with the public key of the receiver, which means that data can only be seen by the Connected Experience device and the Splunk platform instance. Since this data is encrypted as it passes through Spacebridge, not even Spacebridge can decrypt the data. The only data that Spacebridge stores are key pairs and encryption keys so it can correctly route data.

Encryption

All data sent via Spacebridge is encrypted in transit and at rest.

Encryption in Transit: Libsodium encryption library and TLS 1.2 encryption protocol encrypts data end-to-end at multiple layers of the process.

Encryption at Rest: AES-256 encryption encrypts all registration and asset data.

User and Device Management

User Management

Connected Experiences is built right on top of Splunk's core authentication system and uses Splunk's role-based access controls (RBAC) rules, meaning users accessing data on mobile devices have the same access as they would on the web. Connected Experiences supports both local and SAML account types, and a variety of SAML Identity Providers (IdP).

To take advantage of SAML with Connected Experiences, administrators must complete these steps:

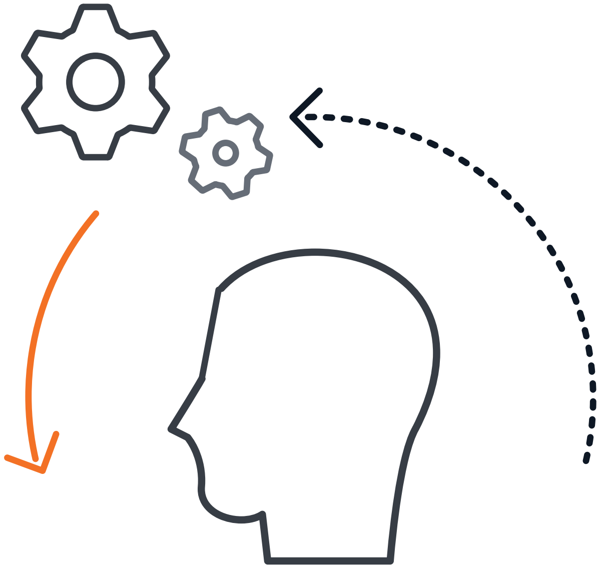
1. Connect your Splunk platform to a supported SAML IdP using scripted authentication or Attribute Query Request (AQR)
2. Enable tokens

Consult the Splunk Secure Gateway documentation to learn how to complete these steps so that SAML Splunk users will be able to register their devices.

Regardless of your account type, the registered device is valid as long as the credentials used at the time of the registration are still valid. If the credentials become invalid, the application automatically logs out the user at the next application load, cutting off access to the Splunk platform instance.

Mobile Device Management (MDM)

Connected Experiences supports many MDM providers such as Microsoft Intune and providers that are part of the App-Config community. With MDM support, administrators can deploy specific security configurations for Splunk Mobile to keep data secure for users accessing information on their personal or corporate devices.



Compliance and Region

Compliance

Spacebridge and Splunk Secure Gateway have been certified to meet SOC2, Type 2 and ISO27001 standards. If you are using Spacebridge with a managed Splunk Cloud Platform deployment and have specifically purchased an applicable regulated environment, then you may transmit the applicable regulated data, including PHI and PCI data, as Spacebridge is HIPAA and PCI-DSS compliant.

Spacebridge does not leverage the FIPS 140-2 validated Splunk Cryptographic Module and may not be used in environments that require this standard. Spacebridge is not available for GovCloud or FedRAMP environments.

Finally, these products undergo regular compliance audits to ensure these standards continue to be met.

Regional Availability

Spacebridge is based in the US East region. Splunk platform versions after .conf21 (Splunk Cloud Platform first, then Splunk Enterprise to follow) let administrators select from a list of Spacebridge locations when initially setting up their Connected Experiences deployments. For more information about this feature, see the Splunk Secure Gateway documentation at the time of release.

Optionally, administrators can opt for a private Spacebridge which lets them host the Spacebridge deployment on-premise in their own environment. Interested customers can follow up with the Connected Experiences team to learn about our initiatives to support private installments of Spacebridge.

When considering the Spacebridge's location, remember that no private information is stored in Spacebridge. It's simply a channel for encrypted information that users with authorized and registered credentials can then access through Splunk web or mobile devices.

Get Started with Connected Experiences

Administrator Steps

To begin using Connected Experiences, start by ensuring that you're using one of the following Splunk platform versions:

- Splunk Cloud 8.1.2103 or higher
- Splunk Enterprise 8.1 or higher

The Secure Gateway Splunk app is already included in these Splunk platform versions. Simply enable it and complete the in-app onboarding steps. Through this process, Splunk Secure Gateway automatically configures Spacebridge on the administrators behalf and no manual port management is needed.

After completing SSG onboarding, all Splunk users can register their own devices using their credentials. If interested, administrators can also customize their Connected Experiences deployment with a series of features available in Splunk Secure Gateway, such as selecting which apps and dashboards are accessible from each app.

Connected App User Steps

To log into a Splunk platform instance from a mobile device, users need to download the Connected Experiences app from the applicable app store on their device.

Then, there are a variety of login methods available. Splunk users should consult their connected app, Splunk Secure Gateway, or administrator to find out which method suits them best.

Refer to the Splunk Secure Gateway documentation for a list of login methods available for your app version.

Conclusion

The Splunk Connected Experiences product line showcases how Splunk is taking many steps to create value wherever data lives. Interacting with data doesn't have to stay at the desktop. Empower your organization and gain more insights by engaging with data in real-world situations and on the go using the Splunk Connected Experiences apps.

Use the Splunk Secure Gateway App to get started on your Connected Experiences journey.

splunk>®
turn data into doing™