

---

# Tableau & Mobile Security

# Overview

Regardless of the application or device, security is integral to every decision your company makes. That's why we've designed a mobile solution with security in mind from the start. We've approached this challenge from a holistic perspective, carefully considering the security impact in each of the following areas:

Device Security

How Mobile Devices Connect to Tableau

Data Transmission

User Authentication and Authorization

Data Encryption at Rest

App-Development Best Practices

We've Got You Covered

## Device Security

Device security is the foundation of your organization's success with mobile apps. With company-issued phones and tablets, you can more easily ensure that devices meet your security standards. But in bring-your-own-device (BYOD) scenarios, things become more challenging.

How do you protect company data on employees' devices? Start by giving them guidelines to secure the whole device with a strong password. Go further with mobile-device management (MDM) utilities like MobileIron or VMware AirWatch. These not only let you precisely control how mobile apps are deployed, but also let you define enterprise-wide rules for security policies, device encryption, and more.

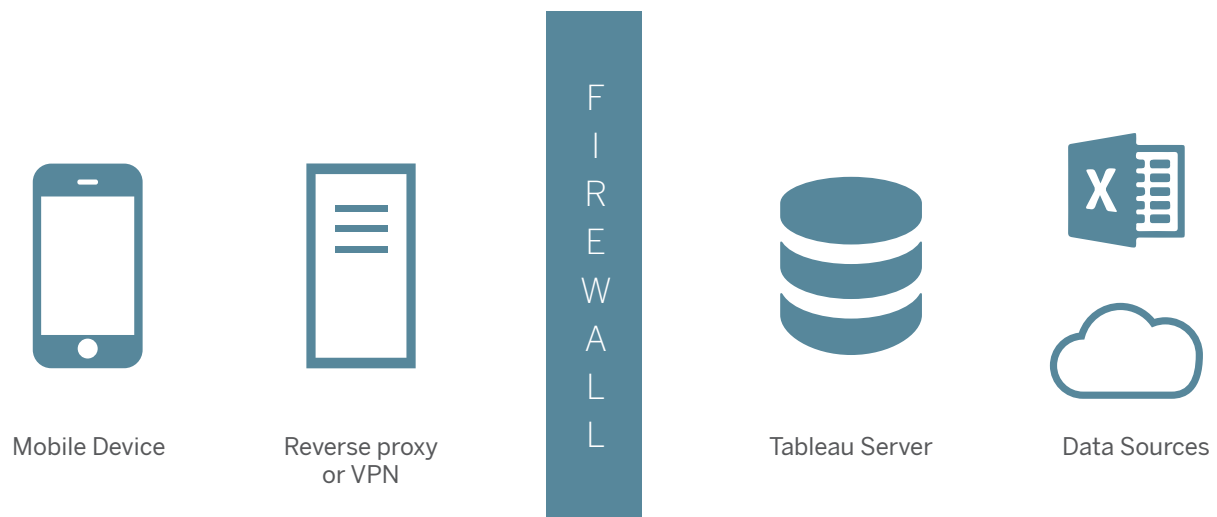
To help you quickly get up and running with MDM tools, Tableau provides detailed guides like [Deploy Tableau Mobile with AirWatch](#). We'll soon offer guides for other popular vendors. Return to this whitepaper online to see the latest content.

# How Mobile Devices Connect to Tableau

Your organization has a variety of mobile needs, so Tableau lets users connect in multiple different ways. For occasional access to Tableau servers or to vizzes embedded in a portal like SharePoint, the mobile browser is a good choice. You can also embed vizzes into custom apps you develop in-house.

For the fastest, most delightful way to stay on top of Tableau data with a phone or tablet, use Tableau Mobile. The app provides a mobile-optimized experience for sign-in and content browsing, and it even lets you work offline. Check out our [product page](#) for details.

When users authenticate via browser or Tableau Mobile, our recommended network architecture below ensures secure communication between mobile clients and data on Tableau Server.



*Tip: If you use Tableau Online, we secure the communication detailed in this whitepaper for you. For details, see [Security in the Cloud](#) in Tableau Online Help.*

## Data Transmission

The Tableau Mobile app supports encrypted data transmission in all forms, from the initial handshake of user credentials to ongoing exchanges of confidential business information. As a first step, configure Tableau Server to use Secure Sockets Layer (SSL) and an SSL certificate that your mobile devices trust. For details, see [Configure External SSL](#) in the Tableau Server help.

Certificates issued by major third-party authorities like VeriSign and GlobalSign are secure and trusted by mobile devices. But you can also use a certificate issued by your organization's internal certificate authority.

After encrypting communication with SSL, you'll need to let mobile users access Tableau Server behind your corporate firewall. We recommend one of these approaches:

- A virtual private network (VPN), either as a standalone solution or integrated into an MDM utility like AirWatch. An MDM utility lets you create multiple VPN profiles with unique traffic rules you can apply to different device types and even individual apps. Per-app VPN provides maximum security.
- A reverse proxy server that manages all traffic coming from the internet to Tableau Server. In conjunction with SSL, a reverse proxy authenticates traffic while concealing the IP address of the server from clients. For more information, see [Configure Tableau Server to Work with a Reverse Proxy Server](#) in Tableau Server: Everybody's Install Guide. To secure communication with Tableau Server, you'll also need to configure the proxy server to [forward the X-Forwarded Proto HTTP header](#).

## User Authentication and Authorization

After you secure mobile devices and their network connections, ensure that the right users have access to content and permission to perform essential tasks. Tableau Server provides a robust system for both authentication and authorization, with a consistent experience regardless of where you're connecting from or what device you're using.

The Tableau Mobile app supports local authentication by Tableau Server, or external authentication via Active Directory, SAML, or Kerberos. For details, see [Authentication](#) in the Tableau Server Help. In single sign-on environments, you'll need to use SAML or Kerberos. If you've configured Tableau Server to use SAML, single sign-on works automatically in Tableau Mobile. If you use Kerberos, [follow this configuration guide for iOS devices](#) in the Tableau Knowledge Base.

If your users commonly connect to Tableau Server via mobile web browsers or targeted apps you've developed in-house, you can also authenticate using trusted tickets. This approach can be helpful when you need to provide broad mobile access to a narrow set of views and dashboards embedded in HTML.

For authorization, Tableau Server lets you logically organize content into separate sites and projects, each of which can have unique permissions. User and group settings let you specify which actions people can perform, and what content they can access—down to the level of individual workbooks and sheets. Tableau even respects permissions from external data sources, so users see only the data they're allowed to see. For configuration steps, see [Manage Permissions](#) in the Tableau Server Help.

For more details, see the related whitepaper, [Tableau Server Security](#).

## Data Encryption at Rest (iOS)

When mobile users interact with content on Tableau Server or Tableau Online, the server processes your underlying business data, and the Tableau Mobile app renders it for display. To display content more quickly, the iOS version of Tableau Mobile securely caches the following content. (The Android app doesn't cache this content, but we recommend encrypting the entire device.)

- Snapshot images of favorite workbooks and sheets. (You can [disable snapshots for specific sites](#).)
- Metadata about favorite workbooks and sheets, such as name, owner, and last-modified date.

This content is securely stored using iOS best practices. Snapshots and metadata are encrypted when devices are locked, and excluded from device backup processes.

For further protection, snapshots and metadata are completely deleted whenever:

- A user signs out of the server or uninstalls the Tableau Mobile app.
- You remove a user account from Tableau Server, and the user tries to sign in with Tableau Mobile.

For maximum control, we recommend managing devices with an MDM utility like AirWatch or MobileIron, which lets you remote-wipe the Tableau Mobile app along with all of its offline content.

## App-Development Best Practices

All of these security efforts start with our development of the Tableau Mobile app itself. We continuously educate our teams on current best practices, validating our approach with regular code reviews and third-party security tests of authentication methods, data exposure, and other factors. Tableau has a well-defined process for communicating and responding to security vulnerabilities.

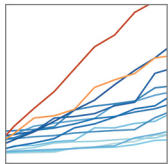
For a complete picture of our approach, go to [tableau.com/security](https://tableau.com/security).

## We've Got You Covered

Tableau provides a comprehensive, secure mobile solution for the modern enterprise and both major mobile platforms. Download the free app from the Apple [App Store](#) or [Google Play](#) today, and start exploring data wherever you go, right when you need it.

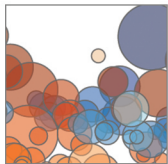
# About Tableau

Tableau Software helps people see and understand data. Offering a revolutionary new approach to business intelligence, Tableau allows you to quickly connect, visualize, and share data with a seamless experience from the PC to the iPad. Create and publish dashboards and share them with colleagues, partners, or customers—no programming skills required. See how Tableau can help your organization by starting your free trial at [tableau.com/trial](http://tableau.com/trial).



## Additional Resources

[Download Free Trial](#)



## Explore Other Resources

- [Product Demo](#)
- [Training & Tutorials](#)
- [Community & Support](#)
- [Customer Stories](#)
- [Solutions](#)

