

Workday Mobile Security FAQ

Workday Mobile Security FAQ

Contents

The Workday Approach	2
Authentication	3
Session	
Mobile Device Management (MDM)	(
Workday Applications	4
Web	4
Transport Security	5
Privacy	5
Security Domains	5
Logging and Monitoring	6
Security Testing	6
Glossarv	-

The Workday Approach to Mobile Security

What is Workday's philosophy around mobile security?

Workday takes a device-agnostic approach to security. Whether you sign in from a desktop, smartphone app, or Workday Mobile Web, your user profile determines your authentication and authorization settings. This approach allows us to institute the same underlying security architecture across all clients and apply enhancements and fixes uniformly across all devices.

Why can't the mobile application be configured to behave differently than the desktop application?

As the line between mobile solutions and traditional desktop/laptop solutions continues to blur, we believe that providing mobile-specific configurations from within the tenant has two main disadvantages. First, it creates much more complexity for our customers and their implementations. Fewer configurations and more simplicity in security mean quicker, easier implementations. Second, it places security constraints on the wrong "dimensions" of the system. For example, we often find that the desired behavior is to lock down functionality by network (i.e. in firewall, out-of-firewall), by location (proximity to office/site), or by assumed role (admin as admin, admin as self-service user).

Authentication

How does Single sign-on (SSO) work for the native mobile applications? What is passed to the mobile device for authentication, and how is that stored on the device?

The Workday tenant is configured with a mobile-specific SSO login page. Mobile clients redirect to this URL for authentication via an embedded WebView within native mobile apps. Upon successful authentication, the Workday mobile app reads the session ID returned by Workday and uses it for the duration of the session.

Is there re-authentication for certain functions to ensure the user is still the authenticated and authorized user?

Not currently. However, Workday is actively working on the requirements and design details to support this feature.

Can the mobile application take advantage of a client certificate for verification or authentication?

Not natively, but SSO solutions that utilize client certificates can be used with the Workday Mobile Web solution for authentication.

Session

Does a session ID stay the same for the duration of a user's connectivity?

Currently, a session ID stays the same for the duration of the session. A nonce is added for sensitive tasks. However, a nonce is securely transmitted for any update tasks.

Does Workday allow for session or password storage on mobile devices?

No. Users must authenticate at the beginning of each new session.

How long does a session last before it times out?

This is configurable from within the Workday tenant based on customer preference. A default session lasts 20 minutes before requiring re-authentication.

Can a user have concurrent sessions?

Yes.

How can we control what data is transmitted over the internal/corporate network vs. an external network? Is there a method to determine if a device is connected to an internal or external network?

For all Workday clients, IP restrictions can be configured by security group membership. However, distinct detection of device type is not supported nor recommended as a security feature.

Are there different user configurations and privileges available on mobile devices based on role, user, or group?

No, we take a consolidated approach. There are no mobile-specific user access configurations. If it's available to a user on the desktop version, it's available on mobile.

Mobile Device Management (MDM)

Does Workday support third-party MDM solutions?

For information on MDM and Workday, reference the MDM Overview and Guidelines. The path is: Community > Product Dashboards > Mobile > Mobile Security Overview.

Workday Applications

What data persists on mobile devices when using Workday's native mobile applications?

Workday follows the guidelines set forth by Apple and W3C to prevent data being stored on any device, both through the native applications and the browser. Only simple values that facilitate reconnecting to the correct destination persist across sessions:

- Tenant
- Connection URL
- Username
- Proxy On/Off

Note that there are three exceptions to this rule that apply to optional features:

- PDF viewing features (payslips, talent card) require that the PDF is cached while in view and deleted once closed. PDFs are encrypted with the Data Protection API on iOS and by the OS on Android.
- If the Workday tenant is configured to use Mobile PIN Login and a user has opted in for the feature, a random temporary app token is stored to facilitate authentication via PIN
- 3. If doc sharing is enabled on iOS, users can share attachments from the Workday app to other apps on the device.

How are these connection settings protected?

The connection settings listed above are stored in the standard settings files for Workday native apps.

Is any business data stored locally on mobile devices?

Your data is secure in the cloud and that is where it should reside. We avoid all local data storage except for the three instances listed above to ensure a secure environment.

Can administrators disallow certain data to be saved or downloaded onto a mobile device?

Any activity relating to downloadable business data (i.e. emailing annotated reports, viewing payslip PDFs, document sharing) can be disabled at the tenant setting level.

Which versions of iOS and Android OS do you support?

Reference our <u>Mobile Documentation</u> for device requirements. The path is: Community > Documentation > Mobile Solutions > Mobile Devices and Features > Device Requirements.

What data protection guidelines do you follow?

Android: We follow the guidelines set forth in Google's developer documentation.

iOS: We follow Apple's guidance on securing information by using the Data Protection APIs.

Web

Do clients running Workday mobile use web services? If so, what are used, are they exposed via WSDL query, and what tcp/udp ports are utilized from the mobile client?

No. Mobile clients do not utilize web services. Mobile clients communicate using a distinct protocol separate from any exposed Web Services. NOTE: 443/TCP is used for our SOAP web services (SOAP/web service WSDLs are exposed).

Transport Security

Does all data that transfers between mobile devices and Workday travel via Secure Sockets Layer (SSL)?

Yes, all data that transfers between a mobile device and Workday travels via SSL. 128-bit SSL is the minimum required by Workday's servers, but if the client uses a stronger algorithm (i.e. 256-bit SSL), Workday's servers will respect that.

How do you defend against "man-in-the-middle" attacks?

Workday's Dynamic Certificate Pinning feature helps prevent man-in-the-middle attacks that utilize malicious DNS servers to harvest credentials, etc. The primary use case for Dynamic Cert Pinning is mobile access from untrusted networks (i.e. ESS/MSS mobile access from a Starbucks).

Privacy

How do Workday's mobile solutions handle data masking?

Any data masking that's configured in the desktop application is reflected on mobile. There are no configuration options specific to mobile.

Do Workday's mobile solutions use location tracking features?

GPS is used in our mobile apps to help make selections from a list on the device, but the user's geocode is never sent back to Workday servers. All other location-based workflows use location data previously entered into Workday (i.e. address information from Workday Contact Information). No location data captured by the device is stored or submitted to Workday.

How can we prevent users from taking screenshots while using Workday mobile?

There are no built-in defenses against screenshots within the apps or Mobile Web solution. Screen shots can sometimes be prevented using Mobile Device Management and Provisioning capabilities (see Section 4). This would depend on which third-party MDM solution is in place.

Mobile-Specific Security Domains

What are the "mobile usage" security domains mentioned in the user documentation? How do they work? How are they configured?

Workday administrators can use the mobile usage security domains to decide which mobile solutions are available to which users in their tenant. We have mobile-specific domains to enable our Mobile Web, Workday for iPad, Workday for iPhone, and Workday for Android. All additional domains mentioned in our user documentation are simply the domains needed to enable a given feature across all solutions. Visit our documentation for more information. The path is: Community > Documentation > Mobile Solutions.

Logging and Monitoring

What information is logged by Workday when using the mobile application?

None—we don't log any intra-app actions on any of our solutions.

Can we review logs? How detailed are the logs?

Within Workday is a delivered report called "Mobile User Tracking," which is secured to the domain Workday Insight. The report shows the mobile logins per user for a specific date range. There is one column for each type of mobile solution (iPad, iPhone, Android, Mobile Web) that was used by the user in that date range. All other logging capabilities have the same behavior as the browser application.

How do I know what tasks are available on mobile? How do I find out about new features in a release?

Refer to our <u>List Tasks Available on Mobile</u> document on Community. The path is: Community > Product Dashboards > Mobile Product Information.

Security Testing

Have you had a third party perform a web services penetration test, code review, and/or security architecture review?

Yes. The following third-party tests and reviews have been performed:

- Application security testing by iSEC Partners and others
- Source code analysis by Veracode
- System and network security testing by Cigital

What security testing has been performed on both the mobile client and the web services/servers that are used? Who performed this testing?

Extensive testing is carried out both by Workday's internal Application Security team as well as by third-party security firms like iSEC Partners.

iSEC's security testing targets specific threat scenarios, identifies vulnerabilities, and enumerates exploitation possibilities. While the testing methodology is flexible, each assessment includes the following processes:

- · Documentation review
- Active testing and Code Review
- Manual and automated penetration testing
- Review fixes to previously identified issues

The penetration testing leverages information from developer interviews and framework analysis. The attack classes tested during the penetration test included, but were not limited to:

- Cross Site Scripting
- XPath/SQL Injection
- HTTP Redirects (Hostile Link attacks)
- Response Splitting
- Directory Traversal
- CSRF / Forced Browsing
- SSL Cipher Strength Analysis
- Cookie Security
- · Information Leakage
- Malicious File Execution (Remote File Inclusion)

Did it test the OWASP Top Ten?

Yes, we tested the OWASP Top Ten where applicable to mobile.

Where can I find a copy of the results, or at least summary and follow-up actions?

Customers can download a copy of the most recent penetration testing reports from the Workday Customer Portal.

Glossary

Native mobile applications: Workday's mobile solutions built specifically for the Android, iPhone, and iPad. Downloadable through Google Play and the Apple App Store.

Workday Mobile Web: Workday's mobile solution that's accessible on any smartphone or tablet through mobile web browsers (e.g. Safari, Chrome, etc.). Includes all the same features as the native apps and is compatible with third-party MDM solutions.

Session: The period of time during which a user logs in to and interfaces with Workday. The session ends when a user times out after a configurable period of time or signs out of Workday.

WebView: A web page embedded within a native mobile app.

User Profile: The security group, usually determined by department and role, that dictates what configurations and privileges a user has in Workday.

Client: Networked devices used to access Workday, including desktop computers, smartphones, and tablets.

Authentication: The process of ensuring and confirming a user's identity.

Client certificate: A security feature used to identify a client or a user, authenticating the client to the server and establishing precisely who they are.

Nonce: A unique, randomly generated marker (usually a number) used, in this case, for session authentication.

Data Masking: The process of hiding original, sensitive data with random characters or data.

