DATA SHEET

Skyhigh Mobile Client

Unified Mobile Security for Internet Access and Private Access

Android · iOS · MDM-Managed and BYOD

KEY ADVANTAGES

Unified Mobile Security

- Single app for Internet Access and Private Access
- Android and iOS support
- MDM-managed and BYOD deployments
- Least-privileged access enforcement through defined policies

Zero Trust Private Access

- IPSec-based secure tunnel to Skyhigh Cloud
- Certificate-based device authentication
- DNS-based traffic interception for private app routing
- Per-App VPN support for Android and iOS

Identity and Device Awareness

- SAML-based user authentication
- Access decisions based on identity, device state, and policy
- Authentication status maintained in Skyhigh Cloud

Enterprise Deployment Ready

- Compatible with Microsoft Intune and Workspace ONE (Airwatch)
- Certificate provisioning via MDM or Apple Configurator
- Downloadable from Google Play Store and Apple App Store
- Works without MDM for BYOD scenarios

Private App Launchpad

- In-app catalog of configured private applications
- Policy-driven app list updated dynamically
- Single tap access to private applications from mobile
- Consistent experience across Android and iOS

Product Overview

Mobile users connect to business applications from personal devices, public networks, and locations outside the enterprise perimeter. Security must follow the user across every device, ensuring that Internet traffic is inspected and private application access is governed by Zero Trust policy, with no requirement for device management.

Skyhigh Mobile Client extends the Skyhigh Security Service Edge platform to Android and iOS devices. A single app secures both Internet Access through the Skyhigh Secure Web Gateway and Private Access to applications hosted across private and public cloud environments. Access is enforced through defined policies on a least-privileged basis, with identity evaluated at every session.

Skyhigh Mobile Client integrates natively with:

- Skyhigh Secure Web Gateway: Internet and SaaS traffic inspection
- Skyhigh Private Access ZTNA: Zero Trust access to private applications

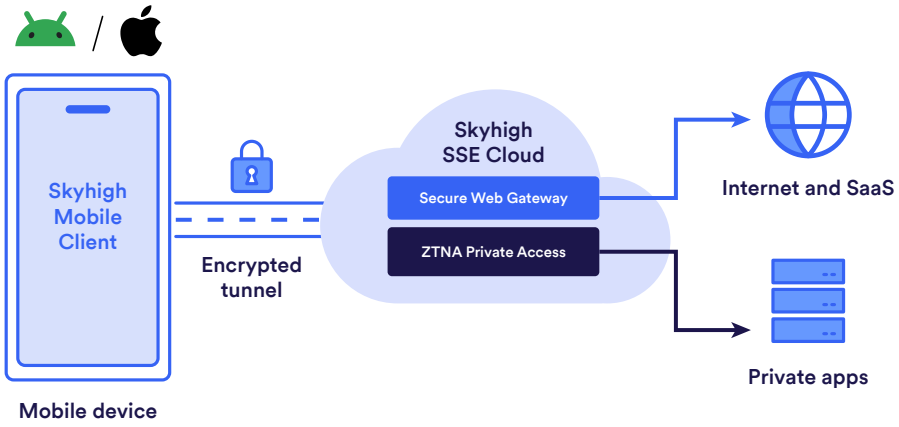

Figure 1. Skyhigh Mobile Client.

What Is Skyhigh Mobile Client?

Skyhigh Mobile Client (SMC) is a lightweight security app for Android and iOS that intercepts device traffic and forwards it to the Skyhigh Security SSE inspection and enforcement. Beginning with version v4.0, the product is known as Skyhigh Mobile Client (SMC). It establishes a secure tunnel between the mobile device and Skyhigh Cloud, routing Internet-bound traffic through the Secure Web Gateway and private application traffic through the Private Access enforcement plane.

A single app instance handles both Internet Access and Private Access. The app supports:

- On-demand and always-on VPN modes
- Full Tunnel and Private Access-Only Tunnel routing configurations
- MDM-managed and unmanaged (BYOD) device deployments

Access policy is centrally defined in Skyhigh Cloud and automatically downloaded to the app. Users authenticate once via SAML and access all configured private applications through the in-app launchpad.

How Skyhigh Mobile Client Works

Skyhigh Mobile Client secures device traffic by enforcing Cloud Application Control policies through the Skyhigh Secure Web Gateway Cloud Service. Traffic is forwarded over a secure tunnel on ports 80 and 443 to Skyhigh Cloud, where web traffic is inspected by theSecure Web Gateway and private application traffic is routed to the appropriate Private Access Gateway.

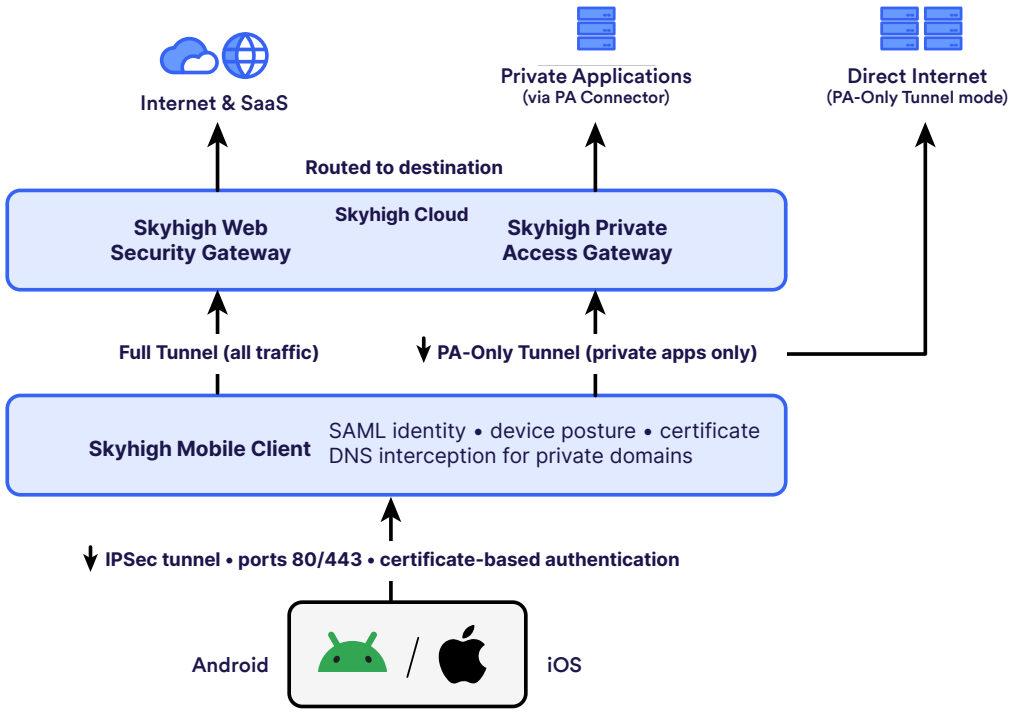

Figure 2. How Skyhigh Mobile Client works.

Secure Tunnel Establishment

When the app starts, it establishes a secure IPSec VPN connection to Skyhigh Cloud. The connection uses certificate-based authentication, with the device certificate provisioned during onboarding through MDM or manual enrollment. Once the tunnel is active, all policy-relevant traffic from the device is forwarded through Skyhigh Cloud for inspection and enforcement.

DNS-Based Private App Traffic Interception

The app intercepts DNS queries for configured private application domains. For each private domain, Skyhigh Cloud returns a mapped CGNAT address (100.64.0.0/10 range). The app's traffic steering engine intercepts all connections to these IPs and tunnels them through Skyhigh Cloud to the Private Access Gateway. Internet traffic not destined for private applications is bypassed from the tunnel.

Traffic Routing Modes

Full Tunnel (mobile.skyhigh.cloud): all traffic from the device, including Internet Access and Private Access, is routed through the Skyhigh Secure Web Gateway for full inspection and enforcement.

PA-Only Tunnel (pa-mobile.skyhigh.cloud): only Private Access traffic is routed through the Gateway. Internet Access traffic goes directly from the device to the internet. This mode is suited for organizations that want Zero Trust access without routing all mobile internet traffic through Skyhigh Cloud.

Skyhigh Mobile Client IPsec VPN connection flow (Android and iOS)

Step 1: Generate the Root CA certificate
Create or obtain a Root CA certificate. This certificate validates all client certificates issued under it and establishes the trust anchor for the IPsec server.

Step 2: Generate a client certificate (PKCS#12 / P12)
Create a client certificate signed by the Root CA. Export the certificate along with its private key as a .p12 file.

Step 3: Upload the Root CA certificate to the Skyhigh tenant
Upload the Root CA to the customer's Skyhigh tenant. The IPsec server will trust any client certificate issued by this Root CA.

Step 4: Provision the client certificate to the mobile device
Distribute the .p12 certificate to devices using one of the following methods:

Intermediary Step
MDM configuration profile (Android and iOS): Push the certificate to devices through a Mobile Device Management solution. This is the recommended method for enterprise deployments.

Android (manual): Import the .p12 certificate directly into the Skyhigh client.

iOS (manual): Package the .p12 using Apple Configurator and install it on the device.

Step 5: Establish the IPsec tunnel
The device uses the provisioned client certificate to initiate an IKEv2/IPsec connection to the IPsec server. On successful authentication, the IKEv2 handshake completes and the encrypted IPsec tunnel is established.

Policy Enforcement

Access policy is defined in the Skyhigh Security management console and downloaded to the app as a policy file. Routing decisions, application allow/deny controls, and data transfer rules are all governed by the downloaded policy. Policy updates are applied automatically on the next app sync cycle without requiring manual intervention.

Private App Launchpad

On successful authentication, the app displays a catalog of all private applications configured for the user. The launchpad is automatically updated when policy changes are applied. Users tap an application to open it directly, with traffic routed through the secure Private Access tunnel. No separate VPN client or browser extension is required.

Authentication

SAML-Based User Authentication

User identity is verified through SAML authentication, integrated with the organization's identity provider. Authentication is performed once through the app and the token is maintained in Skyhigh Cloud. The authentication status is evaluated at every access request; users do not need to authenticate per application or per session restart.

When an access request arrives at the Secure Web Gateway, the gateway validates the user's SAML token against the stored authentication state. If authentication tokens are expired or unavailable, access is denied and the user is prompted to re-authenticate through the app.

Certificate-Based Device Authentication

Each device is authenticated using a client certificate provisioned during onboarding. On MDM-managed devices, certificates are distributed and renewed automatically through the MDM profile. On unmanaged devices, certificates can be provisioned manually via Apple Configurator (iOS) or through the app onboarding workflow (Android). The certificate identifies the device to Skyhigh Cloud independently of the user authentication flow.

Zero Trust Access Model

Every access request is evaluated against two signals simultaneously: verified user identity via SAML and authenticated device via certificate. Access is granted only when all three conditions satisfy the configured policy. No implicit trust is extended based on network location, device ownership, or prior authentication history.

Platform Capabilities

Android

The Android implementation uses a local VPN service that intercepts both Wi-Fi and cellular traffic. A local VPN connection running on the device reads TCP connections and routes them through the Skyhigh Cloud tunnel.

- Local VPN server approach: works without MDM
- Intercepts Wi-Fi and cellular traffic
- Per-App VPN support via Android VPN Service SDK
- Certificate-based onboarding through app workflow
- SAML authentication with enterprise identity provider
- Device signals including OS version and management status
- On-demand and always-on VPN connection modes
- Available from Google Play Store

Android Deployment

- Google Play Store: direct install for managed and BYOD
- Microsoft Intune: enterprise-scale MDM deployment
- Workspace ONE UEM: enterprise MDM deployment
- Manual onboarding available for BYOD without MDM

iOS

The iOS implementation uses an IPSec VPN profile that works on both MDM-managed and unmanaged devices. The VPN profile is visible in iOS Settings under VPN. When the tunnel is active, an IPSec connection is established to Skyhigh Cloud. DNS traffic is tunneled through the IPSec connection to the Skyhigh DNS server, which resolves private application domains to CGNAT (100.64.0.0/10) address range for traffic steering.

- IPSec-based tunnel to Skyhigh Cloud
- Works on MDM-managed and unmanaged devices
- Certificate-based authentication via MDM or Apple Configurator
- DNS interception for private application routing
- Per-App VPN support for iOS managed devices
- SAML authentication with enterprise identity provider
- Device signals including OS version and management status
- Available from Apple App Store

iOS Deployment

- Apple App Store: direct install for managed and BYOD
- Microsoft Intune: enterprise-scale MDM deployment with policy push
- Workspace ONE UEM: enterprise MDM deployment
- Apple Configurator: certificate provisioning for unmanaged devices

Common Use Cases

Mobile BYOD Access to Private Applications

Employees using personal Android or iOS devices access internal applications such as CRM, ERP, ticketing systems, and intranet through the Skyhigh Private Access tunnel. No VPN client or corporate device enrollment is required. Access is governed by Zero Trust policy with identity evaluated at every session.

Internet Security for Mobile Workforce

All internet traffic from mobile devices is routed through the Skyhigh Secure Web Gateway in Full Tunnel mode. Threat protection, URL filtering, and data loss prevention policies are enforced consistently whether the device is on a corporate network, a home network, or a public Wi-Fi connection.

Contractor and Third-Party Access

Contractors using unmanaged devices access only the specific private applications they are authorized for, with no access to other network resources. The Private App Launchpad surfaces only policy-permitted applications. Session data is not retained on the device beyond the active connection.

MDM-Managed Fleet with Unified Policy

Organizations with Microsoft Intune or Workspace ONE UEM deployments push the Skyhigh Mobile Client app and its associated certificate profiles to all managed Android and iOS devices silently. Policy updates from the Skyhigh management console are automatically applied to all enrolled devices without user intervention.

Regulated Industry Mobile Access

Healthcare, financial services, and government organizations extend data protection policies to mobile endpoints. DLP controls enforced through the Secure Web Gateway apply to mobile traffic. Audit logs capture all mobile session activity for compliance reporting.

Zero Trust VPN Replacement on Mobile

Organizations replacing legacy mobile VPN with Zero Trust access deploy PA-Only Tunnel mode. Mobile users access private applications with granular application-level control rather than full network access. VPN clients are removed from enrolled devices and replaced by the single Skyhigh Mobile Client app.

Platform and Supported App Versions and Operating Systems

Android

4.0.x: Android 14, 15

4.1.x: Android 14, 15, 16

iOS

4.0.x: iOS 15+

4.1.x: iOS 15+, including iOS 26

Skyhigh Mobile Client Features and Details

Capabilities	Description
Traffic routing modes	• Full Tunnel (mobile.skyhigh.cloud): all traffic, including Internet Access and Private Access, routed through the Skyhigh Web Security Gateway • PA-Only Tunnel (pa-mobile.skyhigh.cloud): only Private Access traffic routed through the Gateway; Internet Access traffic goes direct to internet
Tunnel Connectivity	IPSec tunnel on ports 80 and 443 to Skyhigh Cloud, with certificate-based authentication for the device tunnel.
Private app traffic interception	DNS-based interception: private application domains resolve to CGNAT (100.64.0.0/10) address range, and connections to those addresses are tunneled to the Private Access Gateway.
Authentication	• SAML 2.0 user authentication with the organization's identity provider, evaluated at every access request • Certificate-based device authentication, provisioned during onboarding and independent of the user authentication flow
Zero Trust access model	Every access request is evaluated against two simultaneous signals: verified identity (SAML) and authenticated device (certificate). No implicit trust based on network location or device ownership.
Connectivity methods	On-demand and always-on VPN modes; Per-App VPN support for Android and iOS.
Deployment and Device Management options	• Direct install via Google Play Store (Android) and Apple App Store (iOS) • Managed deployment via Microsoft Intune and Workspace ONE UEM
Certificate provisioning	• MDM-managed: automatic distribution and renewal via MDM profile • iOS unmanaged: Apple Configurator or manual install • Android unmanaged: in-app onboarding workflow
BYOD support	Works with and without MDM. PA-Only Tunnel mode recommended for BYOD to avoid routing personal traffic through corporate infrastructure.
Private App Launchpad	In-app catalog of policy-permitted private applications, updated dynamically on policy change. Single-tap access without a separate VPN client or browser extension.
Supported Products	**Skyhigh Secure Web Gateway (Internet Access)** Inspects and enforces policy on Internet from Android and iOS devices when Full Tunnel mode is active, applying the threat protection and content controls. **Skyhigh Private Access (ZTNA)** Provides Zero Trust access to private applications from mobile devices using DNS-based traffic interception and an IPSec tunnel to the Private Access Gateway, without exposing the underlying corporate network

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

July 2026. DS-EN-000061-01