DATA SHEET

Skyhigh Client

Unified Endpoint Traffic Steering and Visibility for the Modern Enterprise

KEY ADVANTAGES

Unified Endpoint Traffic Steering

- Single client across all Skyhigh SSE services
- Web and non-web traffic interception
- Policy-driven routing across cloud and on-prem destinations

Advanced Policy Control

- Granular policies based on user and group context
- Powered by the Mowgli policy engine used across Skyhigh SSE
- Policy cloning and migration from legacy Client Proxy
- Routing decisions based on port, process, domain, and IP

High Availability with Multi-Gateway Support

- Define more than two gateways per policy
- Automatic rerouting during gateway failure
- Improved resilience for remote and mobile users

Profile-Based Client Configuration

- Unlimited Client Profiles per tenant
- One profile per client policy
- Profile-level controls for connectivity, device posture, and tamper protection
- Strong isolation between user groups such as HR, Finance, and Engineering

Deep Visibility and Faster Troubleshooting

- Modern Skyhigh branded client UI
- Real-time service connectivity status
- Built-in diagnostics and log capture
- Controlled temporary client disablement for troubleshooting

Product Overview

Modern enterprises operate across on-prem, cloud, and hybrid environments while supporting distributed users and applications. Endpoint traffic must be routed precisely, policies must remain consistent, and troubleshooting must be fast and deterministic.

Skyhigh Next Gen Client 5.0 represents the evolution of Skyhigh Proxy Client 4.9, delivering enhanced policy intelligence, expanded platform support, and deeper SSE integration. It is a unified, lightweight endpoint client that intercepts and steers both web and non-web traffic from endpoint devices to Skyhigh Security SSE services or on-prem enforcement points.

Skyhigh Client integrates natively with Skyhigh SSE:

- Skyhigh Secure Web Gateway
- Skyhigh Private Access ZTNA
- Skyhigh Cloud Firewall
- Skyhigh CASB (inline and API)
- Skyhigh Remote Browser Isolation (RBI)

This enables a single endpoint client to support secure access, inspection, and enforcement across all enterprise traffic paths.

What is Skyhigh Client?

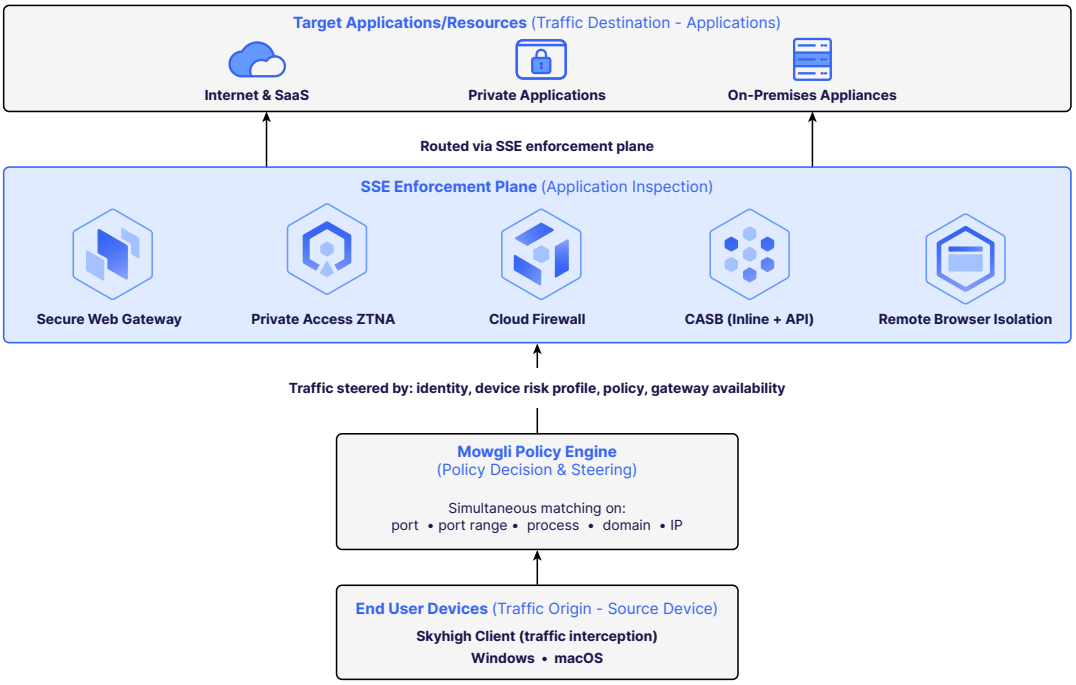
Skyhigh Client is a unified endpoint traffic steering client that dynamically routes traffic based on user identity, device risk profile, policy conditions, and service availability. It supports:

- On-prem environments
- Cloud-only environments
- Hybrid deployments

A single client instance works across all Skyhigh SSE services and routes traffic automatically based on user entitlements and configured policies.

Architecture Overview

Skyhigh Client intercepts all endpoint traffic and forwards it to the appropriate Skyhigh SSE enforcement point based on policy, licensed services, and gateway availability.



How Skyhigh Client Works

Traffic is routed to	Routing decisions are based on
• Secure Web Gateway: web and SaaS traffic • Private Access: Zero Trust access to private applications • Cloud Firewall: network-level controls for all ports and protocols • CASB: inline and API-based cloud application controls • Remote Browser Isolation: risky web sessions • Secure browser controls: For safer AI adoption • On-prem appliances: where required by policy	• Policy conditions and licensed services • User identity and group membership • Device risk profile (native + CrowdStrike) • Gateway availability and health status • Traffic matching criteria (port, port range,protocol, process, domain, IP)

This model provides consistent enforcement while maintaining high availability and predictable user experience.

Key Benefits and Capabilities

Unified Endpoint Traffic Steering

- Single client for all Skyhigh SSE services
- Web and non web traffic interception through a unified endpoint agent
- Policy driven traffic routing across cloud and on premises destinations
- Flexible traffic steering to one or more gateways based on business and security requirements

Unified and Granular Policy Control

- Powered by the Mowgli policy engine used across Skyhigh SSE, including SWG, Cloud Firewall, DLP, ZTNA, CASB, and RBI
- Consistent policy behavior between endpoint traffic steering and SSE enforcement
- Granular policy creation based on user, group, application, network, and device context
- Simultaneous matching on port, port range, process, domain, and IP address for precise policy enforcement
- Policy cloning and migration capabilities for existing Skyhigh Proxy Client deployments

Multi Gateway High Availability

- Support for multiple gateways within a single policy
- Automatic gateway failover and traffic rerouting during outages
- Improved service availability and user experience for remote and mobile users
- Scalable traffic distribution across cloud and on premises environments

Device Aware Zero Trust Enforcement

- Native device risk profiles integrated into policy decisions
- CrowdStrike integration with real time Zero Trust Assessment (ZTA) scores
- Dynamic access decisions based on live device posture and risk level
- Stronger security controls beyond traditional device enrollment checks

Role Based Policy Segmentation

- Unlimited client profiles per tenant
- Dedicated profiles and policies for different user groups such as HR, Finance, Engineering, contractors, and third parties
- Strong policy isolation between user populations
- Profile specific controls for connectivity, device posture, tamper protection, and user experience

Enhanced Visibility and Troubleshooting

- Modern Skyhigh branded client interface
- Real time visibility into service connectivity and client status
- Built in diagnostics, log collection, and troubleshooting tools
- Controlled temporary client disablement for support and operational workflows
- Faster issue identification and resolution for administrators and help desk teams

Simplified Operations

- Single client architecture reduces endpoint complexity
- Consistent policy management across endpoint and SSE services
- Easier deployment, administration, and lifecycle management
- Reduced operational overhead through centralized control and policy reuse across the Skyhigh platform

Policy Engine Capabilities

Skyhigh Machine Client uses the Mowgli-based policy engine, aligned with Skyhigh SSE web and access policies.

Policy Configuration

- Define more than two gateways per policy
- Combine multiple conditions using logical operators
- Simultaneous evaluation across all traffic matching criteria
- Create distinct policies per user group
- Map multiple user profiles to individual policies
- Clone and migrate legacy Client Proxy policies

Traffic Matching Criteria

- Port (specific port number)
- Port range (e.g. 8080–8090)
- TCP, UDP, and configurable protocol lists
- Process (application initiating the connection)
- Domain (FQDN, wildcard, subdomain)
- IP address (single or CIDR range)

All criteria are evaluated simultaneously for precise routing and enforcement.

Visibility and Troubleshooting

Skyhigh Client includes a redesigned UI for Windows and macOS that provides real-time insight into client health, connectivity, and traffic redirection across all configured SSE services.

Section	What It Shows
Home Dashboard	Consolidated status for SWG, Private Access, Cloud Firewall, CASB, and RBI. Status states: Secure, Warning, Error, Disabled.
Client Overview	Client version, applied policy name, policy revision number, and last policy update time.
Connectivity	Service-level connectivity insights including gateway health, PA dashboard access, and Cloud Firewall enforcement status.
Log Capture	On-demand diagnostics including error, informational, and debug logs for faster issue resolution.
Disable Client	Temporary disablement for a defined duration using an admin-issued release code. Prevents unauthorised bypass.

Supported Operating Systems

Platform	SC Version	Supported Versions
Windows	5.0.0	Windows 10 LTSC 2021 (21H2)
		Windows 11 GA (23H2, 24H2)
		Windows 11 LTSC (24H2)
Windows Server	5.0.0	Windows Server 2022, Windows Server 2025
macOS	5.0.0	macOS 14 (Sonoma), macOS 15 (Sequoia), macOS 26 (Tahoe)

SC Version	Supported Chipsets (macOS)
5.0.0	Intel (64-bit), Apple M1, M2, M3, M4

Deployment Options

Standalone Installation

- Lightweight installer
- Windows and macOS
- Supports on-prem, cloud, and hybrid environments
- Available from Skyhigh Success and Content Security Portal

Managed Deployment via MDM

Recommended for enterprise scale.

Supported MDM platforms:

- Trellix ePO
- Microsoft Intune
- Jamf (macOS)

Backward Compatibility

Skyhigh Client supports legacy Client Proxy policies. Full routing flexibility, advanced conditions, and profile isolation are available when using the Mowgli-based Client Policy Engine.

Skyhigh Client Modules

Skyhigh Client routes endpoint traffic to the following Skyhigh SSE services, each independently licensed and enforced through the shared Mowgli policy engine.

Skyhigh Client Modules	
Skyhigh Secure Web Gateway (SWG)	Inspects and enforces policy on web and SaaS traffic, including threat protection and content filtering, as endpoint traffic is steered to the gateway by Skyhigh Client.
Skyhigh Private Access (ZTNA)	Provides Zero Trust access to private applications without exposing the underlying network, using identity and device context evaluated at every session.
Skyhigh Cloud Firewall	Extends enforcement to all ports and protocols beyond standard web traffic, giving network-level control over non-HTTP/S connections originating from the endpoint.
Skyhigh CASB	Applies inline and API-based controls to sanctioned and unsanctioned cloud applications, governing data movement and access within SaaS environments.
Skyhigh Remote Browser Isolation (RBI)	Isolates risky or uncategorised web sessions in a remote container, protecting the endpoint from web-based threats without blocking access outright.
Skyhigh Data Loss Prevention (DLP)	Enforces inline data protection policy through SWG, CASB, and RBI sessions, with classification and policy behaviour kept consistent between endpoint traffic steering and cloud enforcement.

Skyhigh Client Features and Details

Skyhigh Client Features and Details	
Broad operating system support	• Windows 10 LTSC 2021 (21H2); Windows 11 GA (23H2, 24H2); Windows 11 LTSC (24H2) • Windows Server 2022, Windows Server 2025 • macOS 14 (Sonoma), macOS 15 (Sequoia), macOS 26 (Tahoe)
Native Support for Modern Processor Architectures	Optimized for Intel 64 bit and Apple Silicon platforms, including M1, M2, M3, and M4 processors.
Policy engine	Mowgli-based policy engine shared across SWG, Cloud Firewall, DLP, ZTNA, CASB, and RBI for consistent enforcement behaviour between endpoint traffic steering and SSE policy.
Traffic matching criteria	• Port (specific port number) and port range (e.g. 8080–8090) • TCP, UDP, and configurable protocol lists for precise traffic classification • Process (application initiating the connection) • Domain (FQDN, wildcard, subdomain) • IP address (single or CIDR range) • All criteria evaluated simultaneously, without sequential rule fallthrough
Supported Protocols and Services	HTTP/HTTPS traffic interception via configurable TCP ports DNS (UDP 53) NTP (UDP 123) DHCP (UDP 67) IKE/IPsec (UDP 500, ESP Protocol 50) LDAP (TCP/UDP 389, 636, 3268, 3269) SMB (TCP/UDP 445) ICMP GRE (Protocol 47) HTTP Proxy support SOCKS Proxy support Secure gateway communications over TCP 443 and 8081 Configurable local proxy support (TCP 8080 by default)

Skyhigh Client Features and Details	
Gateway support	• Multiple gateways per policy • Cloud and on premises gateway support • Priority based gateway failover • Automatic switch over to available gateways • Fastest response time based gateway selection • Gateway health monitoring • Hostname and IPv4 based gateway definitions • CSV import and export for gateway configurations • Gateway cloning for rapid deployment and consistency • Automatic Cloud Firewall gateway selection • Configurable polling intervals for gateway availability checks • Ordered gateway preference lists with intelligent fallback • Support for scalable and resilient traffic routing across distributed environments
Client Profiles	Profile-level controls for connectivity, device posture, and tamper protection, with strong isolation between user groups. Unlimited Client Profiles per tenant; ONE client profile per client policy.
Device risk and posture	Native device risk profiles evaluated at every policy decision. CrowdStrike integration provides real-time Zero Trust for dynamic access decisions based on live device health. • Device OS Score • Sensor Score • Overall Score
Deployment and lifecycle options	• Standalone lightweight installer via Skyhigh Success and Content Security Portal • Managed deployment via Trellix ePO, Microsoft Intune, and Jamf (macOS)
Backward compatibility	Supports legacy Client Proxy (SCP) policies. Policies can be cloned or migrated into the Mowgli-based Client Policy Engine using the policy migration UI.
Visibility and troubleshooting	• Home Dashboard: consolidated status across SWG, Private Access, Cloud Firewall, CASB, and RBI (Secure, Warning, Error, Disabled) • Client Overview: client version, applied policy name, policy revision, last update time • Connectivity: service-level connectivity insights per configured service • Log Capture: on-demand error, informational, and debug diagnostics
Anti-tampering	• Windows access and uninstall protection, combined with macOS root-level file protection, help prevent unauthorized client disablement or removal.

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

June 2026. DS-EN-000050-01