DATA SHEET

Skyhigh Secure Web Gateway Cloud Administration

Audience
This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with web protection.

Recommended Pre-Work
- Knowledge of Windows and system administration, network technologies
- Basic understanding of computer security, command line syntax, malware/anti-malware, virus/anti-virus, and web technologies

Course Overview

The **Skyhigh Secure Web Gateway on Cloud Administration** course provides in-depth training on Skyhigh Security Cloud and related cloud products. The course covers the configuration and administration of critical Security Service Edge (SSE) functions. It also walks through the components to help participants identify, define, and refine use cases based on specific scenarios. Products and capabilities covered in this course include the Skyhigh Security Cloud platform, Skyhigh Secure Web Gateway (SWG), Cloud Firewall, Data Loss Prevention (DLP), Infrastructure as A Service (IAAS), Software as a Service (SAAS), Remote Browser Isolation (RBI), and Private Access (ZTNA).

Course Agenda

Day 1
Welcome
SSE Principles
Cloud Connector and Integrations
Secure Web Gateway Setup
Web Policy Overview
HTTPS Scanning
Web Filtering

Day 2
Media Type
Shadow IT
Anti Malware
Remote Browser Isolation
Common Rules and End User Notifications
Classifying Data
DLP Web Policy

Day 3
Incidents
Analytics
Cloud Firewall
Private Access
Cloud Administration
Hybrid

Day 4
Dashboards and Reporting
Logging, Backups, and Restore
Troubleshooting
Skyhigh Mobile Client

Course Objectives

Welcome
Review the course agenda and support resources. Log in to the virtual lab environment to confirm readiness for hands-on exercises and activities.

Security Service Edge Principles
Identify core Security Service Edge SSE services and traffic redirection methods. Understand the benefits of a direct-to-cloud architecture for modern security.

Cloud Connector and Integrations
Install the on-premises Cloud Connector. Integrate it with Active Directory for user data, and configure it to receive logs via Syslog for analysis.

Secure Web Gateway Setup
Configure global settings for the Skyhigh Client Proxy SCP. Build and deploy a client policy file to manage traffic redirection and bypass lists.

Web Policy Overview
Understand the core components of the Web Policy engine. Learn to build, position, and publish custom rule sets using the central List Catalog.

HTTPS Scanning
Implement HTTPS scanning to inspect encrypted traffic. Configure certificate verification rules and create bypasses for sensitive sites that use certificate pinning.

Web Filtering
Configure global block and bypass rules. Create a web filtering policy that blocks URL categories and inspects the contents of archive files.

Media Type
Configure global block and bypass rules. Create a web filtering policy that blocks URL categories and inspects the contents of archive files.

Shadow IT
Discover and assess the risk of unsanctioned Shadow IT applications. Implement policies to block high-risk services and enforce tenant access restrictions.

Anti-Malware
Implement a multi-layered anti-malware policy. Configure the Gateway Anti-Malware engine and submit suspicious files to the Trellix IVX sandbox for analysis.

Remote Browser Isolation
Protect endpoints by isolating web sessions in a remote container. Configure both "Risky Web" and "Full Isolation" policies to mitigate browser-based threats.

Common Rules and End User Notifications
Configure specialized common rules for traffic handling. Customize and apply branded end-user notification pages to inform users when web content is blocked.

Classifying Data
Create custom data classifications using keywords, dictionaries, and advanced patterns. Understand use cases for fingerprinting structured and unstructured sensitive data.

DLP Web Policy
Learn to configure, manage, and analyze Data Loss Prevention (DLP) policies, using rules and evidence to prevent data exfiltration and investigate incidents.

Incidents
Navigate incident dashboards to filter, analyze, and manage policy violations. Configure views and generate reports on specific events like Web DLP violations.

Analytics
Use Web Analytics to investigate traffic and identify risky users. Learn to filter data, create custom views, and generate scheduled security reports.

Data Security Posture Management (DSPM)
Understand how DSPM and Security Service Edge (SSE) work together to create a strong security system.

Cloud Firewall
Enable the Cloud Firewall within the client proxy policy. Construct rules to control outbound traffic and monitor all firewall activity using dedicated dashboards.

Private Access
Implement Zero Trust Network Access (ZTNA) by configuring applications, deploying connectors, and creating policies that grant secure access to private corporate resources.

Cloud Administration
Manage administrator access using SAML SSO and Role-Based Access Control (RBAC). Configure Data Jurisdictions to restrict data visibility for specific users.

SWG Web Hybrid
Configure a hybrid deployment by synchronizing on-premises appliances with the cloud. Manage policy routing and identify use cases for a unified security posture.

Dashboards and Reporting
Build custom dashboards by adding and arranging cards from saved views. Generate on-demand reports and schedule them for recurring, automated delivery.

Logging, Backups and Restore
Export logs using the Log Collector and Log Stream. Perform and restore web policy backups, and outline the on-premises to cloud migration process.

SWG Cloud Troubleshooting
Troubleshoot common web proxy errors using the Rule Tracing tool. Diagnose and resolve frequent Skyhigh Client Proxy (SCP) issues involving VPNs and policies.

Skyhigh Mobile Client
Configure and deploy the Skyhigh Mobile Client to extend security policies to iOS and Android devices using MDM and certificate-based authentication.

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

Skyhigh Security is a registered trademark of Musarubra US LLC. Other names and brands are the property of these companies or may be claimed as the property of others. Copyright © 2026.