

Skyhigh for Office 365

# Integration Pre-requisites

This document lists the pre-requisites necessary for the deployment of Skyhigh for Office 365 solution. It has been organized as per the use cases of the customer for this product and the pre-requisites necessary to implement the related feature.

If a test/sandbox/lower environment is in scope for a specific use case, the same pre-requisites are applicable, and separate for the lower environment as well, unless specifically mentioned otherwise.

***Please check the check box (**) against each item to indicate readiness of the specific pre-requisite.***

1. Connect Office 365 tenant to Skyhigh Tenant

The following is mandatory for Skyhigh for Office 365 API solution:

**A Service account in your Office 365 tenant with the following permissions**

Service account should be a global admin with the following permissions

* + 1. *Read user profiles*
    2. *Have full control of all site collections*
    3. *Read and write items and lists in all site collections*
    4. *Read all users’ full profiles*
    5. *Read directory data*
    6. *Read DLP policy events including detected sensitive data (Office 365 Management APIs)*
    7. *Read activity data for your organization (Office 365 Management APIs)*
    8. *Read and write mail in all mailboxes*

Service account should have Sharepoint Online and OneDrive (and Exchange Online, if applicable) licenses assigned.

Service account should be an admin for root Sharepoint Online site i.e. https://<customdomain>.sharepoint.com

Service account should have the attribute "work email" configured in its user profile.

|  |  |
| --- | --- |
| Environment | Service account Username |
| Sandbox |  |
| Production |  |

1. Exchange Online Mailbox Auditing

If Exchange Online Auditing is an use case, the following are the prerequisites

Exchange Mailbox auditing should be enabled for the Office 365 tenant. Details can be found in Microsoft’s KB article: <https://technet.microsoft.com/en-us/library/dn879651.aspx>

The Service Account in Use Case I above should have its mailbox configured.

1. Data Loss Prevention – Enterprise DLP Integration

Enterprise DLP integrates Skyhigh with any on premise DLP that supports the ICAP protocol. This enables Skyhigh to integrate with solutions such as Symantec Vontu, McAfee, RSA, or any other vendor's DLP that supports ICAP protocol.

Enterprise DLP Appliance

1. That supports ICAP protocol
2. Appropriate license that allows the DLP appliance to listen for and scan files coming over ICAP protocol (e.g. *Network Prevent for Web* license for Symantec Vontu DLP appliance).

VM to run Skyhigh Enterprise DLP Integrator

The Skyhigh DLP Integrator Service acts as a 3-way bridge between Skyhigh, the CSP and Customer’s DLP appliance. It is a Linux/Windows Service and would need to be installed in the Customer’s environment. It is a memory and network intensive process and appropriate sizing is necessary. Typically, we recommend the following:

|  |  |  |
| --- | --- | --- |
|  | Sandbox | Production |
| # of processing cores | 4 | 8 |
| RAM | 8 GB | 16 GB |
| HDD | 100 GB | 100 GB |
| Operating System | Windows 8 and above (64-bit), Windows Server 2008 and above, RedHat/CentOS 6 and above, 64-bit. | |

Please contact Skyhigh Team with approximate data upload traffic into the CSP for the sizing details.

Firewall rules for Skyhigh Enterprise DLP Integrator

Appropriate firewall rules would need to be setup in the Customer’s environment to enable the Skyhigh DLP Integrator service to connect to Skyhigh, the CSP and the Enterprise DLP appliance.

1. Outgoing 443/tcp to myshn.net (shnpoc.net, in case of sandbox)
2. Outgoing 443/tcp to Microsoft Office 365
3. Outgoing 1344/tcp to Enterprise DLP Appliance
4. Data Loss Prevention – Fingerprinting

Skyhigh Fingerprints allow you to monitor your organization's data, build indices of rolling hashes of that data on premise, and prevent sensitive or confidential information from leaving the organization by creating compliance policies around it.

VM to run Skyhigh Enterprise DLP Integrator

Machine Path: Input of the unstructured data

Folder Path: Location for generated Hashed Files is the output for all the fingerprints created.

1. Active Directory attribute based DLP User Groups

Skyhigh provides the capability to create User Groups based on the AD attributes of a user and allows DLP policies to be selectively applied/excluded for those User Groups.

This would require Customer to install the Skyhigh Enterprise Connector and connect with Customer’s Active Directory over LDAP.

VM to run Skyhigh Enterprise Connector

The hardware specifications for the Skyhigh Enterprise Connector are described in Appendix I. The following are the other pre-requisites to implement this integration.

Service user account on the Customer’s Active Directory Global Catalog with Read Only privileges.

LDAP Connectivity details to Customer’s Active Directory

List of AD attributes

Firewall rules for Skyhigh Enterprise DLP Integrator

Appropriate firewall rules would need to be setup in the Customer’s environment to enable the Skyhigh Enterprise Connector service to connect to Skyhigh and the Customer’s LDAP service.

1. Outgoing 443/tcp to myshn.net (pstat.shnpoc.net, in case of sandbox)
2. Outgoing 389/tcp to LDAP Service
3. SIEM Integration

Skyhigh is capable of sending anomalies and DLP Policy violation events to Customer’s SIEM appliance in LEAF or Syslog format.

This would require Customer to install the Skyhigh Enterprise Connector and connect with Customer’s SIEM appliance.

VM to run Skyhigh Enterprise Connector

The hardware specifications for the Skyhigh Enterprise Connector are described in Appendix I.

Connectivity details of the SIEM Appliance

Configure SIEM Appliance to accept logs from Skyhigh Enterprise Connector

Firewall rules for Skyhigh Enterprise DLP Integrator

Appropriate firewall rules would need to be setup in the Customer’s environment to enable the Skyhigh Enterprise Connector service to connect to Skyhigh and the SIEM appliance.

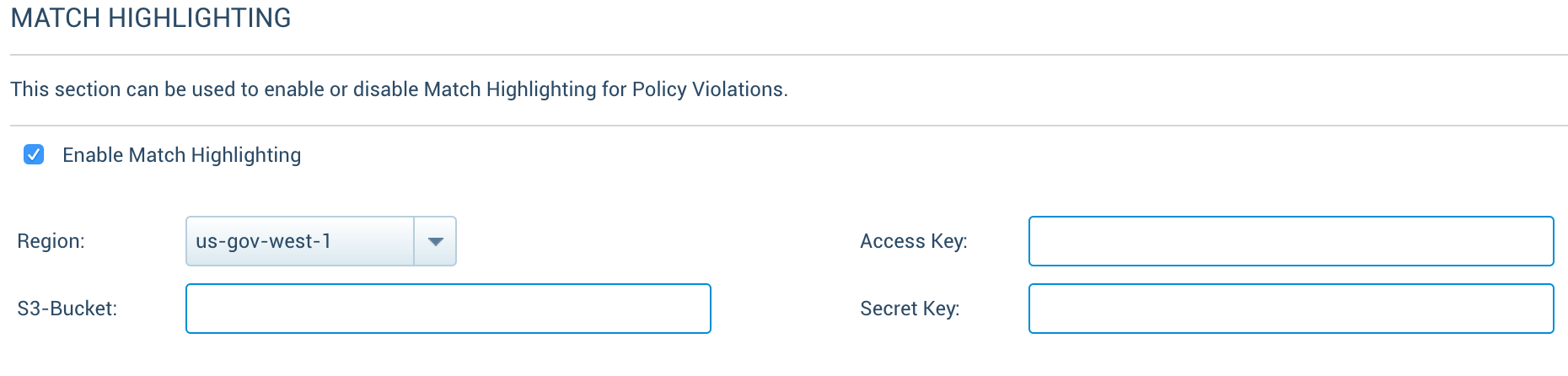
1. Outgoing 443/tcp to myshn.net (pstat.shnpoc.net, in case of sandbox)
2. Outgoing on selected port to SIEM Appliance
3. Match Highlighting

Skyhigh provides the capability to provide a view of the snippets of text that caused a specific DLP Policy violation right from the Skyhigh Dashboard. This feature requires storing those snippets in encrypted format in a Customer owned Amazon S3 bucket.

Details of the Amazon S3 bucket

The following details are needed to setup the Match highlighting feature:

1. Amazon S3 Region
2. S3 Bucket name
3. Access Key
4. Secret Key



1. Near Real-time Email DLP (*beta*)

Skyhigh Email DLP allows you to apply DLP policies to your Exchange Online deployment using [email journaling](https://technet.microsoft.com/en-us/library/jj898487(v=exchg.150).aspx) in Exchange Online. Journaling gives you the ability to of sending email traffic through Skyhigh via API.

Global Administrator role in your Office 365 account. You'll need to grant Skyhigh permissions to several functions to enable email journaling

A list of all email domains for your organization. It's important to know the full scope of email domains that should be subject to DLP

A pre-configured quarantine email mailbox, ready to receive any forwarded quarantined emails. This email must be in a domain included in the list above

A pre-configured secondary email address where undeliverable journaled messages will be sent if a problem prevents delivery to Skyhigh

A pre-configured group in Office 365 to test with Skyhigh before deploying Email DLP to your entire enterprise

1. Cloud Access Policies

Cloud Access Policies without Device Certificate Check

Cloud Access Policies are an important part of protecting access to cloud data and managing devices. Cloud Access Polices can be set up to block access to all uploads for a service, for example, or to require step-up authentication before downloading a file.

* Cloud Access policies to block downloads – Business use case
* Cloud Access policies to block access based on IP addresses – Customer’s VPN Subnet

Cloud Access Policies with Device Certificate Check

Skyhigh provides functionality which will allow an organization to confirm that a device a user is using to access a sanction corporate solution, like Office 365 or Salesforce, is a managed device by requesting that a corporate deployed certificate exists on the endpoint or application.

Skyhigh reverse proxy for O365

All the devices should have the client certificate pushed

Root Certificate (PEM Format)

Maximum chain depth: Hierarchy of the certificate trust

Cloud Access Policies with Device Certificate Check and Unique Device IDs

Skyhigh can be integrated with MDM Solutions (Airwatch/Mobile Iron) to do a second layer check against the certificate and UDID of the device. If the UDID of the device is in the SAN list on the certificate, then it passes the second layer.

AirWatch/Mobile Iron should be configured with Enterprise CA (known CA, self-signed CA won't work).

Configure Device Profiles for Certificate-based Authentication

All the devices should be enrolled with AirWatch/Mobile Iron.

AirWatch/Mobile Iron should push the device certificate which contains UDID in SubjectAlternativeName

# Appendix I – Skyhigh Enterprise Connector

The Skyhigh Enterprise Connector acts as a broker between the Customer’s environment and Skyhigh and enables multiple use cases to be implemented Specifically for Office 365, it would be used to implement the SIEM integration and Active Directory attribute based DLP User Groups. The same Enterprise Connector service can be used to implement both these use cases and also, if the Customer already has Skyhigh for Shadow IT implemented with Enterprise Connector setup for log processing, the same can be re-used here.

The following are the minimum recommended specifications for the Enterprise Connector Virtual Machine. If Customer has Skyhigh for Shadow IT implemented, the recommended specifications for the Enterprise Connector VM for Skyhigh for Shadow IT will take precedence over the below.

|  |  |  |
| --- | --- | --- |
|  | Sandbox | Production |
| # of processing cores | 2 | 4 |
| RAM | 4 GB | 8 GB |
| HDD | 100 GB | 100 GB |
| Operating System | Windows 8 and above (64-bit), Windows Server 2008 and above, RedHat/CentOS 6 and above, 64-bit. | |