Skyhigh Proxy Installation

To install and run Skyhigh On-Premise Proxy, you will need to download and install a pre-configured virtual appliance and deploy it. Follow the instructions below.

https://success.myshn.net/Setup\_and\_Configuration/Firewall\_and\_Proxy\_Integration/01\_About\_Firewall\_and\_Proxy\_Integrations

Pre-requisites for installing on-premise proxy:

vCenter 5.x for installing On-Premise Proxy virtual appliance.

Minimum 1 public IP for proxy management. If you want to actively monitor the services, then the recommendation is to have 2 IPs . One for proxy management purpose and another one for data traffic.

ICAP server for monitoring the services (must be existing).

The following ports will be used by On-Premise proxy and your firewall should be configured to allow this.

* Outgoing ports : 443. This will be used by proxy to contact dashboard, receive configuration and send events.
* Incoming Ports : 2222 (For SSH purpose). In addition to that proxy will be listening in port 80, 443 for receiving http(s) requests and port 1344 for receiving ICAP purpose

Follow the instructions below to install the proxy

1. Add the proxy in the dashboard

Login to Dashboard and click "Control -> Proxy Management". Click "Add another Proxy". Enter the name, Management IP, Passphrase and Virtual IP. If you have 1 Public IP, then enter the same IP in Management and Virtual IP field. Once proxy is added, all your existing managed services will be managed using this proxy.

2. Download and Deploy Proxy Appliance

Click the "Download Skyhigh Proxy" button to download the proxy appliance. This will be a zip file. Unzip the file in a directory.

Login to the vCenter using VMWare vSphere Client. Click File -> Deploy OVF Template. Go to the location where the zip file was extracted and select the OVF file (.ovf extension). Continue the workflow by providing inputs. At the end of workflow select "Power on after deployment" check box and then click Finish.

Deployment of the appliance time takes some time. You can monitor the progress of the deployment by opening the console and wait for the provisioning to complete. The appliance will be rebooted once the configurations are completed.

Once the appliance is fully UP, you can see the status of the proxy in Dashboard (Proxy Management) and proxy will manage the services.

3. Configuring existing ICAP server to forward the requests to proxy

The existing ICAP server should forward the requests to Proxy only in Response Modification Mode. The ICAP server in the On-Premise will be listening on port 1344 on the management IP. For example if your management IP is 216.156.214.14, then the requests should be forwarded to icap://216.156.214.14:1344/request

The detailed information and instructions for all these 3 steps are available in user guide.

If you have any questions or issues, please contact us.

ICAP Proxy Configuration

Configure your ICAP proxy’s network configuration on this page to integrate with your forward proxy and enable DLP inspection of data flowing out to SaaS applications such as Evernote and Slack.

Step 1 :

Provide the ICAP Details

ICAP Proxy : Enabled Disabled

Port : 

SSL : Enabled Disabled

ICAP Server Host Name :

.cigna.shnpoc.net

IP Address :



Step 2 :

Create a Skyhigh Certificate or A Certificate Signing Request (CSR)



Since you’ve chosen to disable SSL, you don’t need to complete this step.Email:



SSL : Create a Skyhigh Certificate





|  |
| --- |
| Test Failed. |
| Please verify the information above is correct and try again. |

Create a Customer CSR

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | Service that can be monitored (via ICAP) |  | |
|  |
| |  | | --- | | 4shared | | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | |  |  | | Monitor only | | |  | | Bitcasa | | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | |  |  | | Monitor only | | |  | | Dropsend | | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | |  |  | | Monitor only | | |  | | StrongSpace | | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | |  |  | | Monitor only | | |  | | Yousendit | | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | |  |  | | Monitor only | | |  | | Carbonite | | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | |  |  | | Monitor only | | |  | | Egnyte | | |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | |  |  | | Monitor only | | |

Create a New Fingerprint

Table of contents

1. [Create an Structured Data Fingerprint](https://success.myshn.net/Policy_Management/Fingerprints/02_Create_a_New_Fingerprint#Create_an_Structured_Data_Fingerprint)
2. [Create an Unstructured Data Fingerprint](https://success.myshn.net/Policy_Management/Fingerprints/02_Create_a_New_Fingerprint#Create_an_Unstructured_Data_Fingerprint)

Create an Structured Data Fingerprint

1. Choose Policy Management > DLP Policies > Fingerprints.
2. Click Create New Fingerprint > Structured Data Fingerprint.
3. Fingerprint Name. Enter a name for the Fingerprint.
4. Source File. Enter the path to the source file that holds the data you want to fingerprint.
5. Folder Path to Locally Generated Hashed Files. Enter the path to the folder where your locally generated hashed files will be stored. Space allocated for this should be about 10-20% of the size of data to be fingerprinted.
6. Column Separator. Select the delimiter that separates the columns of your source file: either Comma, Tab, or Pipe.
7. First row of file contains column names. Activate this check box if the first row of your source file contains column names.
8. Column. If the field names aren't automatically detected, enter the first Field Name for your source file. Then select the Field Type from the menu. Selections include:
   * Alphabetic. Alphabetic characters.
   * Number. Numbers supported with decimals.
   * Alphanumeric. Alphanumeric characters.
   * Zip Code. ##### or #####-####
   * Email. LOCAL\_SUBPART ('.' LOCAL\_SUBPART)\* '@' DOMAIN\_SUBPART ('.' DOMAIN\_SUBPART)\*;
   * Date. ##/##/#### or ##-##-####
   * Phone. (###)###-#### or ###-###-####
   * Credit Card Number. CCNs formatted with decimals, spaces, or underscores, separated by pipes or semicolons.
   * Social Security Number. ###-##-####, or ### ## ####, or ###.##.###, separated by pipes or semicolons.
   * Identifier. Letters and numbers with hyphens and decimals.
9. Click + to add as many Columns as required.
10. Click Save.

The new Structured Data Fingerprint is created and appears on the Fingerprint page. Next, [generate an index](https://success.myshn.net/Policy_Management/Fingerprints/03_Generate_an_Index).

Create an Unstructured Data Fingerprint

1. Choose Policy Management > DLP Policies > Fingerprints.
2. Click Create New Fingerprint > Unstructured Data Fingerprint.
3. Fingerprint Name. Enter a name for the Fingerprint.
4. Machine Path. Enter the path to the machine that holds the files you want to fingerprint. Click + to add an additional paths, if necessary.
5. Folder Path to Locally Generated Hashed Files. Enter the path to the folder where your locally generated hashed files will be stored. Space allocated for this should be about 10-20% of the size of input paths/folders.
6. File Type Exclusions. Enter any file types to be excluded. (Archive files such as ZIP files are automatically excluded.)
7. Click Save.

The new Unstructured Data Fingerprint is created and appears on the Fingerprint page. Next, [generate an index](https://success.myshn.net/Policy_Management/Fingerprints/03_Generate_an_Index).

Generate an Index

Table of contents *No headers*

After you have created your fingerprint for the first time, generate the index. Or generate a new index when new files have been added to the host machine.

1. Choose Policy Management > DLP Policies > Fingerprints.
2. Find the Fingerprint for which you want to generate an index.
3. In the Actions column, click Generate Index.

This triggers index generation by the on-prem DLP Integrator, but you can cancel the generation anytime.

Indices are present until the [fingerprint is deleted](https://success.myshn.net/Policy_Management/Fingerprints/Delete_a_Fingerprint).

1. [Back to top](https://success.myshn.net/Policy_Management/Fingerprints/03_Generate_an_Index#title)
   * [Create a New Fingerprint](https://success.myshn.net/Policy_Management/Fingerprints/02_Create_a_New_Fingerprint)
   * [Add a Fingerprint to a DLP Policy](https://success.myshn.net/Policy_Management/Fingerprints/Add_a_Fingerprint_to_a_DLP_Policy)

* Was this article helpful?
* Yes
* No
* Leave feedback

Recommended articles

1. There are no recommended articles.
2. [DLP Policy Rules and Rule Groups](https://success.myshn.net/Policy_Management/Data_Loss_Prevention_Policies/DLP_Policy_Rules_and_Rule_Groups)
3. [Fingerprints](https://success.myshn.net/Policy_Management/Fingerprints)
4. [Create a New Fingerprint](https://success.myshn.net/Policy_Management/Fingerprints/02_Create_a_New_Fingerprint)
5. [Edit a Fingerprint](https://success.myshn.net/Policy_Management/Fingerprints/Edit_a_Fingerprint)