MVISION Cloud Secure Policy Configuration

MVISION Cloud configuration entails using the Policy Editor to configure the Policy template for email message objects and fields. During the configuration, the system administrator needs to return to Salesforce and perform verification and editing tasks, and follow the confirmation instructions on the email account.

Salesforce Configuration

On-Demand Email-to-Case configuration in Salesforce should be performed as directed by Salesforce. The system administrator configures the Salesforce.com platform, MVISION Cloud Secure, and provides an example of system email case submission and forwarding definition. For more detailed instruction, contact Salesforce support.

Salesforce Reports and Views

In order for the Salesforce application to support Reports and Views for custom fields when working through MVISION Cloud Secure, the user’s SFDC credentials must be entered into the Admin Console. The credentials need to be entered in the Salesforce Credentials tab under Setup.

NOTE: You must perform a Deploy Now after setting up the credentials for the support to become active.

Salesforce for Outlook

Salesforce for Outlook, a Microsoft Outlook integration application that you install, automatically syncs contacts, events, and tasks between Outlook and Salesforce. You can also manually add Outlook emails to these Salesforce records:

* Contacts
* Accounts
* Opportunities
* Leads

When working with Salesforce through MVISION Cloud Secure, the ability to encrypt email, contacts, events, and tasks is added. The system administrator configures Salesforce and the user configures Salesforce for Outlook.

To work through MVISION Cloud Secure, the system administrator configures Outlook in Salesforce and the policy template in MVISION Cloud. Step-by-step instruction can be found in the knowledgebase.

Salesforce/Outlook Configuration

Outlook configuration in Salesforce should be performed as directed by Salesforce. The only consideration that should be taken is that under Email Setting, only Add Email should be selected.

The MVISION Cloud Secure configuration is performed in the Policy Editor. The system administrator configures the objects Email Messages and Attachments with the proper encryption type according to the company policy. The only consideration that should be taken is that when encrypting the From: Email Address object, the end user needs to re-enter the My Email to Salesforce page in Salesforce and click Save, ensuring emails go through MVISION Cloud Secure first for encryption.

User Configuration

Once the system administrator configures Salesforce and MVISION Cloud Secure, the user can install (if not yet done) and configure the Salesforce for Outlook application. The considerations that should be taken are:

* The application should be configured with the MVISION Cloud Secure domain login URL.
* The Email to Salesforce address in the My Email to Salesforce page should not be used to send emails as it will send clear text and not encrypted.

Chatter

* When working with Salesforce Chatter (browser) through MVISION Cloud Secure, the following functionality is supported:
* Encryption of chatter feeds, posts and comments
* Search & Favorite
* @mention, #topic and links into content
* Email reply and links-in-email
* File attachments
* Post links

About Ionic DRM

Table of contents

1. [Use Cases](https://success.myshn.net/Settings/Ionic_DRM/About_Ionic_DRM#Use_Cases)
2. [Supported Services](https://success.myshn.net/Settings/Ionic_DRM/About_Ionic_DRM#Supported_Services)

By integrating with Ionic’s DRM system, MVISION Cloud Secure can apply DRM policies to files generated inside your proxy-integrated cloud services, providing protection to the files leaving your cloud services in concert with MVISION Cloud Secure’s protection for files entering your cloud services.

Use Cases

MVISION Cloud/Ionic DRM Integration covers two key use cases:

1. Files downloaded from your MVISION Cloud Sanctioned cloud services can be detected and protected by Ionic DRM
2. Files uploaded to the your MVISION Cloud Sanctioned cloud services can have Ionic protection applied as part DLP policy

Supported Services

Ionic DRM integration is currently supported for the following products for proxy-based integrations:

* MVISION Cloud for Salesforce
* MVISION Cloud for Microsoft O365 and OneDrive

Protect Uploaded Files with Ionic DRM

Table of contents

1. [Define Rules in Ionic DRM Dashboard](https://success.myshn.net/Settings/Ionic_DRM/Protect_Uploaded_Files_with_Ionic_DRM#Define_Rules_in_Ionic_DRM_Dashboard)
2. [Define Rules in Skyhigh](https://success.myshn.net/Settings/Ionic_DRM/Protect_Uploaded_Files_with_Ionic_DRM#Define_Rules_in_Skyhigh)

You can apply Ionic DRM to files uploaded to supported cloud services through the use of DLP rules. Once encrypted, the files can only be viewed by authorized users through the Ionic plugin.

Define Rules in Ionic DRM Dashboard

In order to protect uploaded files with Ionic DRM, first create a policy in the Ionic DRM dashboard. Set the rule to encrypt files uploaded to your target cloud service.

Please consult Ionic’s help documents for instructions on building rules in their dashboard.

Define Rules in Skyhigh

Once configuration is complete in the Ionic Dashboard, you must create a rule in the MVISION Cloud to pass the uploaded file to Ionic for encryption before uploading it to the cloud service. Follow these steps to define the appropriate rule:

1. Navigate to Policy > DLP Policies and click Create Policy.
2. Set type Proxy.
3. Select the Service to be Managed (i.e. Salesforce).
4. Choose Data Identifier as SSN.
5. If you want all uploaded files to be protected by Ionic DRM, set the Rule for Collaboration: Upload.
	1. If you want other conditional rules to determine encryption (for example, to only encrypt documents that contain Social Security numbers), add the rules in addition to the Collaboration rule. For example, to protect documents with Social Security Numbers, add the rule Data Identifier: SSN.
6. Because Ionic DRM’s plug-in cannot decrypt .xlsx files, set the exception rule for File Type: Microsoft Excel.
7. Set the response Apply DRM.

Any file uploaded to the selected service (that matches any other rules) will be encrypted by Ionic DRM. Authorized users can view plain-text versions of the files through the Ionic Plugin.