

salesforce

Multi-Org Security Summary

Gain insight into Salesforce security settings across your company!

Installation Guide (for v2.7 - August 2020)



Introducing Multi-Org Security Summary



Complete insight into the security health of orgs across your company

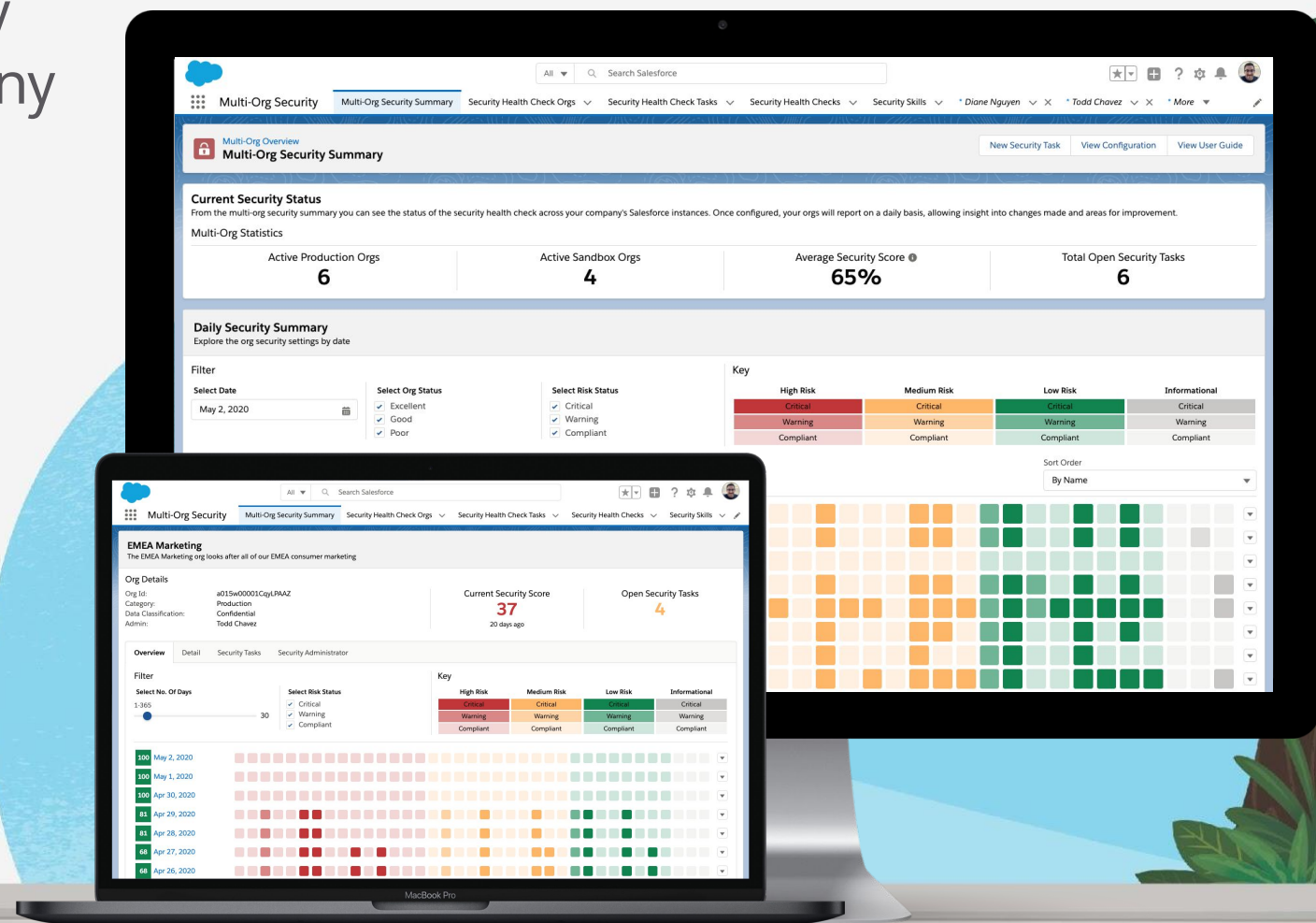
Powered by Lightning Web Components

Easy to install and simple to configure

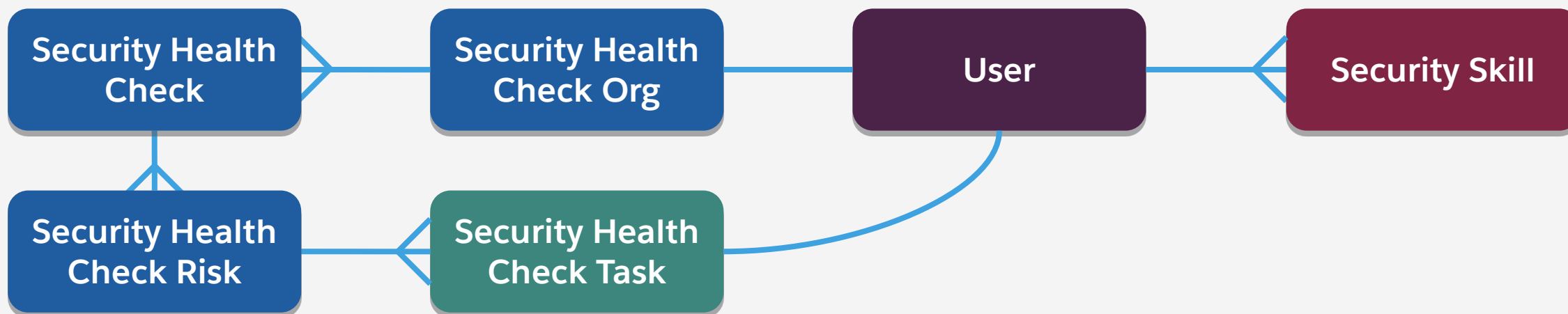
Access to scores, risks and historical trends

Create and assign tasks to improve security

100% natively built on Salesforce



Core Object Model



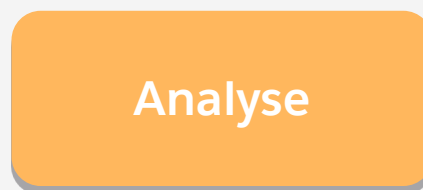
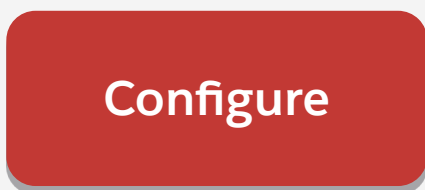
Security Health Check - A daily snapshot of a Salesforce org's security health check and associated risks.

Security Health Check Org - The definition of the org that is connected to a security health check.

Security Health Check Task - A task used to instruct users when security risks need to be mitigated.

Security Skill - A record of your Admin's skills and commitment to learning.

Multi-Org Security Summary



Set up the central org by creating a record for each of your orgs.

Install the package into each child org and enter the required configuration.

Schedule the reporting service, which will report daily data to the central org.

Use the Multi Org Security app to view the summary of this data.

Each day will contain the security score and associated risk information.

Review the risks, paying particular attention to those marked Critical.

Identify orgs or risks that need to be reviewed and improved.

Assign tasks to the relevant admin, with an appropriate deadline and priority.

See the result of changes as your org scores improve.



Setup Guide

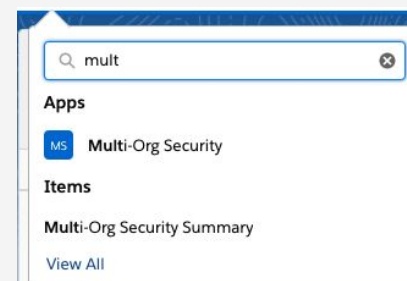


Configuration Instructions



Start by installing the package in the **central** org. This org will be the one that collates data across all of your orgs. Once installed you will need to perform the following actions

- 1 Open the *Multi-Org Security* app via the app launcher
- 2 Open the *Security Health Check Orgs* tab and click *New* to create the org record for the Central org. This is needed so that details about the central org can appear in the summary pages. [See the next page for details of what to provide]



Setting up the Central Org



Security Health Check Org

The security health check org record is used to categorize and store security health checks against the relevant org.

Name: The name of the central Org

Organization Id: The Id of the central Org. This can be found in the *Company Information* section in *Setup*.

Description: Provide an overview of the purpose of the org

Data Classification: The level of security applied to the org

The screenshot shows the 'New Security Health Check Org' form in Salesforce. The form is divided into several sections: Information, Classification, Status, and Point of Contact. The 'Information' section includes fields for 'Security Health Check Org Name' (Global IT Hub), 'Organization Id' (00D5w000003TfjYEAS), 'Owner' (Stephan Garcia), and 'Latest Score' (0). The 'Description' field contains the text: 'This org is used to manage global IT operations and is used as our security hub org.' The 'Classification' section has 'Data Classification' set to 'Internal' and 'Org Type' set to 'Production'. The 'Status' section shows 'Active' and 'Current Org' both checked. The 'Point of Contact' section has 'Point of Contact' set to 'Stephan Garcia' and 'External Contact Email' is empty. At the bottom right, there are buttons for 'Cancel', 'Save & New', and 'Save'.

New Security Health Check Org	
Information	
* Security Health Check Org Name Global IT Hub	Owner Stephan Garcia
Organization Id 00D5w000003TfjYEAS	Latest Score 0
Description This org is used to manage global IT operations and is used as our security hub org.	
Classification	
Data Classification Internal	Org Type Production
Status	
Active ☒	Current Org ☒
Point of Contact	
Point of Contact Stephan Garcia	External Contact Email
Cancel Save & New Save	

Setting up the Central Org



Security Health Check Org cont.

Org Type: Production or Sandbox

Active: True if the org is currently being reported on. Use this toggle to add/remove the org from the summary screens.

Current Org: Set this to true

Point of Contact: The main point of contact for the org

External Contact Email: The email of the point of contact if they are not a user in this Salesforce org

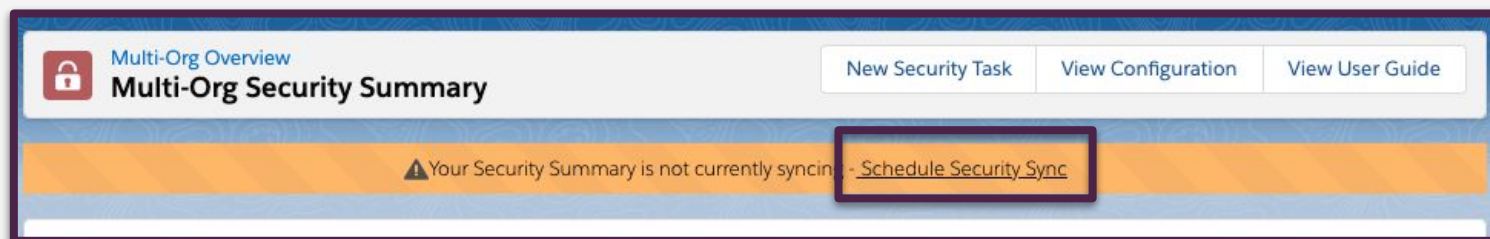
The screenshot shows the 'New Security Health Check Org' form in Salesforce. The form is divided into several sections: Information, Classification, Status, and Point of Contact. The 'Information' section includes fields for 'Security Health Check Org Name' (Global IT Hub), 'Organization Id' (00D5w000003TfjYEAS), 'Owner' (Stephan Garcia), and 'Latest Score' (0). The 'Description' field contains the text: 'This org is used to manage global IT operations and is used as our security hub org.' The 'Classification' section has 'Data Classification' set to 'Internal' and 'Org Type' set to 'Production'. The 'Status' section shows 'Active' and 'Current Org' both checked. The 'Point of Contact' section shows 'Point of Contact' as 'Stephan Garcia' and 'External Contact Email' as an empty field. At the bottom right, there are buttons for 'Cancel', 'Save & New', and 'Save'.

New Security Health Check Org	
Information	
* Security Health Check Org Name Global IT Hub	Owner Stephan Garcia
Organization Id ⓘ 00D5w000003TfjYEAS	Latest Score 0
Description This org is used to manage global IT operations and is used as our security hub org.	
Classification	
Data Classification Internal	Org Type Production
Status	
Active ⓘ ☒	Current Org ☒
Point of Contact	
Point of Contact Stephan Garcia	External Contact Email ⓘ
Cancel Save & New Save	

Schedule your Health Check Sync



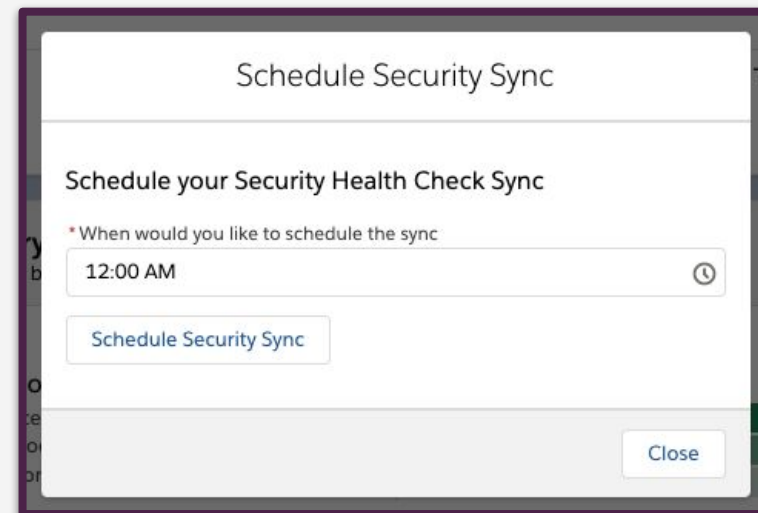
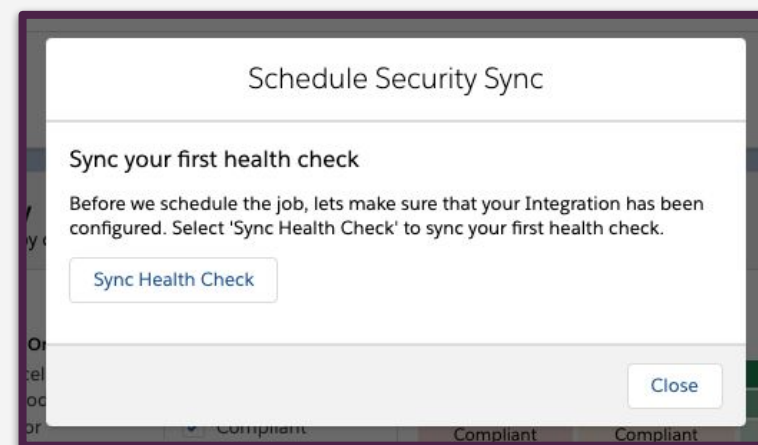
- 3 Navigate back to the Multi-Org Security Summary tab and you will see the following banner displayed on the page.



- 4 Select *Schedule Security Sync* and follow the instructions. This will generate your first set of data for this org.

At the next prompt, select the time of day to schedule the daily data generation and click *Schedule Security Sync*. [Ideally this should be set up to be around the same time for this central org and all other child orgs].

- 5 After the job has been scheduled, close the prompt and refresh the page. You should now see the daily security summary with your central org listed and data populated.



Create the Reporting Endpoint



Create Remote Site Settings



Create A Remote Site Settings in the Central Org

Navigate to *Setup > Remote Site Settings*

6

Create Remote Site Setting: <https://this-org-mydomain--c.visualforce.com>

This link for the central org will allow us to get the Health Check from the Tooling API

Remote Site Name	
Remote Site URL	
Disable Protocol Security	☐ 
Description	
Active	☒

Choose your Integration Method



The security health checks are sent to this central org via a HTTP POST request. There are two options around how to configure the endpoint that receives the data :-

OPTION 1

Salesforce Rest Api & Connected App

Create a connected app and authorize each of your child orgs to communicate with Salesforce.

Then use an Authorization provider and named credential in the child org to send the security health check data to the central org.

OPTION 2

Public Salesforce Site Endpoint

Create a public salesforce site and add the supplied Apex Rest service to the site.

Once added, you may add the url of the endpoint to the child org and post the security health check data.

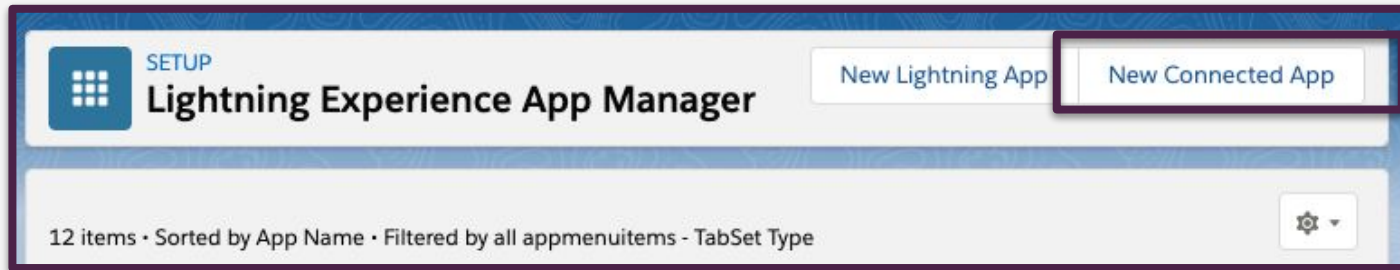
Choose ONE of these methods. The approach with the least amount of administration is OPTION 2.

Option 1 - Connected App Method

Option 1- Connected App Method (1/3)



7 Navigate to Setup > App Manager and Select 'New Connected App'



8 Complete the basic information section of the app.

Make sure you give it a name that is recognizable to yourself and other administrators.

Basic Information

Connected App Name | MultiOrgSecuritySummary

API Name | MultiOrgSecuritySummary

Contact Email | first.last@mycompany.com

Contact Phone

Logo Image URL [Upload logo image](#) or [Choose one of our sample logos](#)

Icon URL [Choose one of our sample logos](#)

Info URL

Description This is used to sync orgs to the central security org

| = Required Information

Option 1- Connected App Method (2/3)



- 9 Enable **OAuth Settings** and Supply a Temporary Callback URL [*the actual URL will be updated later after we have configured the child org*].

The application then requires you to Select the **refresh_token** and api **OAuth Scopes**

- 10 Save your connected App

The screenshot shows the 'API (Enable OAuth Settings)' configuration page in Salesforce. The page has a light blue header with the title 'API (Enable OAuth Settings)'. Below the header, there are several settings:

- Enable OAuth Settings:** A checkbox that is checked.
- Enable for Device Flow:** A checkbox that is unchecked.
- Callback URL:** A text input field containing 'https://www.salesforce.com'.
- Use digital signatures:** A checkbox that is unchecked.
- Selected OAuth Scopes:** A section with two columns. The left column is titled 'Available OAuth Scopes' and lists several scopes: 'Access and manage your Chatter data (chatter_api)', 'Access and manage your Eclair data (eclair_api)', 'Access and manage your Wave data (wave_api)', 'Access custom permissions (custom_permissions)', 'Access your basic information (id, profile, email, address, phone)', 'Allow access to your unique identifier (openid)', 'Full access (full)', 'Provide access to custom applications (visualforce)', and 'Provide access to your data via the Web (web)'. The right column is titled 'Selected OAuth Scopes' and contains two selected scopes: 'Access and manage your data (api)' and 'Perform requests on your behalf at any time (refresh_token, offline_access)'. Between the two columns are 'Add' and 'Remove' buttons.
- Require Secret for Web Server Flow:** A checkbox that is checked.

Option 1- Connected App Method (3/3)



- 11 Navigate to *Setup > Profiles* and locate the profile of the user you will be using with the connected app

Select the Profile and then navigate to *Assigned Connected Apps*. Click 'Edit' and give them access to the connected App you just created. This is required so that the Named Credentials in the child org are able to connect. **If you do not do this you will receive an OAUTH_APP_ACCESS_DENIED error when authenticating later.**

- 12 Save the Profile

Option 2 - Public API Method

Expose an anonymous endpoint via Sites

Option 2 - Salesforce Sites Method



- 13 Navigate to Setup > Sites and Select 'New'

Site Label ↑	Site URL	Site Description	Active	Site Type	Last Modified By
No records to display.					

- 14 Select 'Guest User Licence' , Complete the basic information section and complete the security section in line with your company security policies. Remember to tick ACTIVE to make the site live.

Site Label: Multi-Org Security Endp

Site Name: Multi_Org_Security_Endp

Site Description: This site is used to integrate child orgs into the multi-org security summary.

Site Contact: Stephan Garcia

Default Record Owner: Stephan Garcia

Default Web Address: http://multi-org-security-demo.force.com/

Active: ☒

Active Site Home Page: Unauthorized

Once the site has been created - Select Public Access Settings > Assigned Users > Public Site User Full Name

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Other All									
Action	Full Name ↑	Alias	Username	Last Login	Role	Active	Profile	Manage	
Edit	Site Guest User, Multi-Org Security Endpoint	guest	multi_org_security_endpoint@multi-org-security-demo.force.com			☒	Multi-Org Security Endpoint Profile		

Option 2: Salesforce Sites Method (cont.)



16

On the user profile, give the user the permission set 'Multi-Org Security Summary Integration User'. This will give them access to the rest endpoint that allows them to POST their security health check securely.

A screenshot of the Salesforce user profile interface for assigning permission sets. The interface is divided into two main sections: "Available Permission Sets" on the left and "Enabled Permission Sets" on the right. In the "Available Permission Sets" section, "Salesforce CMS Integration Admin" is listed. In the "Enabled Permission Sets" section, "Multi-Org Security Summary User" is listed. Between the two sections are "Add" and "Remove" buttons with right and left arrow icons respectively. At the top and bottom of the interface are "Save" and "Cancel" buttons.

Available Permission Sets	Enabled Permission Sets
Salesforce CMS Integration Admin	Multi-Org Security Summary User

Once this is completed - we will come back later when it's time to integrate the child org.



Finalise the Central Org Configuration



The following instructions apply regardless of whether you are using Option 1 or Option 2.



Central Org - Metadata configuration (1/2)



17

Clone the Security Health Check Config

Navigate to *Setup > Custom Metadata Types*

Select *Manage Records* for the Security Health Check Config record and then select *Configuration* in the configs list.

Clone the record.

Label: Give this a label that allows you to identify the record

Security Health Check Config Name: Make sure you change this to reflect the Label above. *[If the Name is left as Configuration, it will be ignored]*

Central Org URL: Leave as the default

[continue on the next page]

Label	Configuration
Security Health Check Config Name	Configuration
Central Org URL	/services/apexrest/multiorg/SecurityHealthCheckReporting
Token	Add Parent Org Token
Named Credentials	Add Named Credentials
Is this the Central org?	☒
Security Superstar Threshold	10
Created By	Stephan Garcia, 5/1/2020, 2:58 PM

Label	Configuration
Security Health Check Config Name	Child_Org
Central Org URL	/services/apexrest/multi
Token	S3AJU53jaM5vB8y8Tq
Named Credentials	Parent_Security_Org_Cr
Is this the Central org?	☐
Security Superstar Threshold	10

Central Org - Metadata configuration (2/2)



Token: This is not needed in the central org, so leave as is

Named Credentials: This is not needed, so leave as is

Is this the central org: True. This setting controls whether you see the multi-org version of the app page, or the single org version.

Security Health Check Config

EditClone

Label	Configuration
Security Health Check Config Name	Configuration
Central Org URL	/services/apexrest/multiorg/SecurityHealthCheckReporting
Token	Add Parent Org Token
Named Credentials	Add Named Credentials
Is this the Central org?	☒
Security Superstar Threshold	10
Created By	Stephan Garcia, 5/1/2020, 2:58 PM

EditClone

Information

Label	Child Org
Security Health Check Config Name	Child_Org
Central Org URL	/services/apexrest/multi
Token	S3AJU53jaM5vB8y8Tq
Named Credentials	Parent_Security_Org_Cr
Is this the Central org?	☐
Security Superstar Threshold	10

18

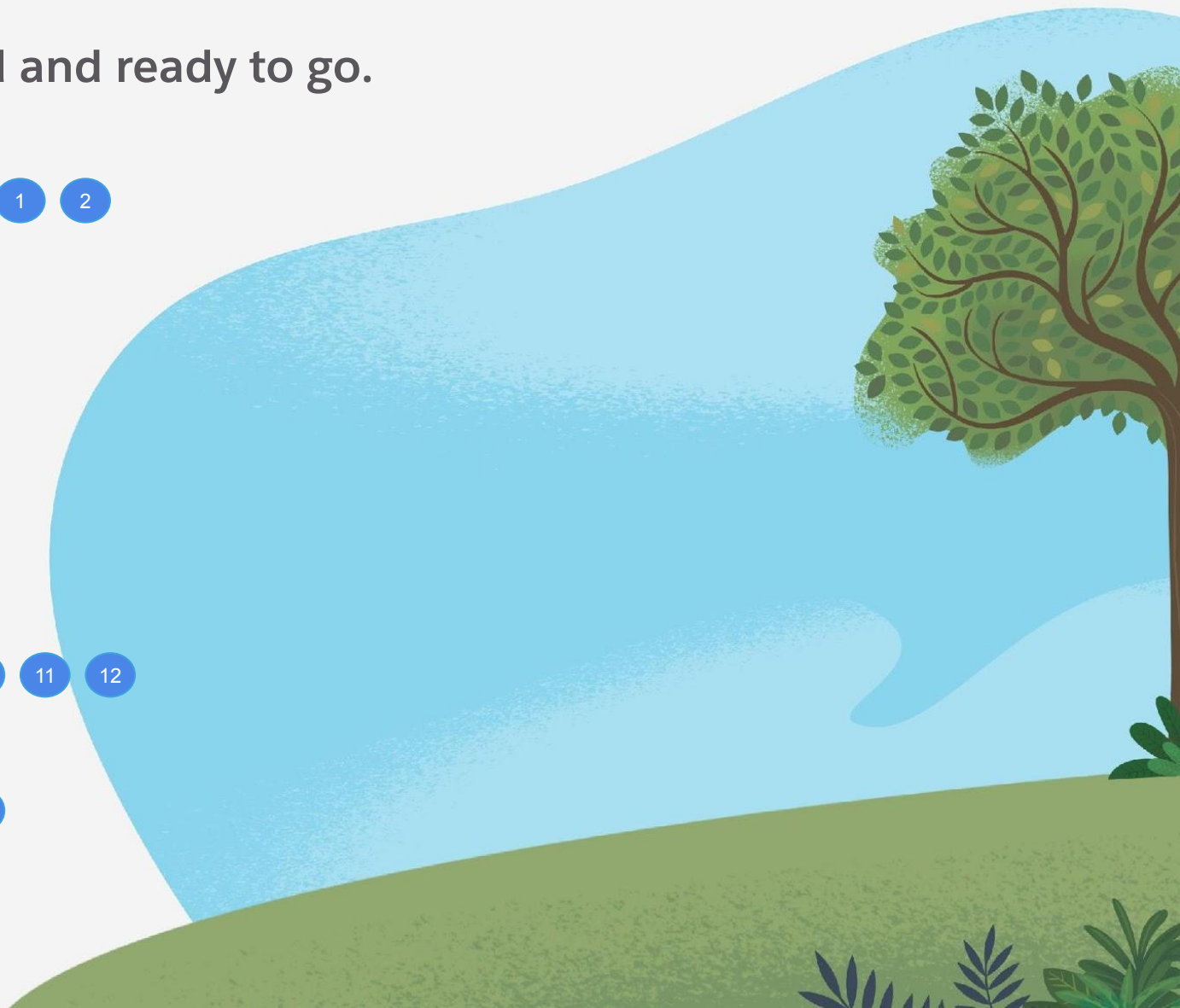
Save the record

Central Org Checklist



That should be the central org configured and ready to go.
Ensure that you have:-

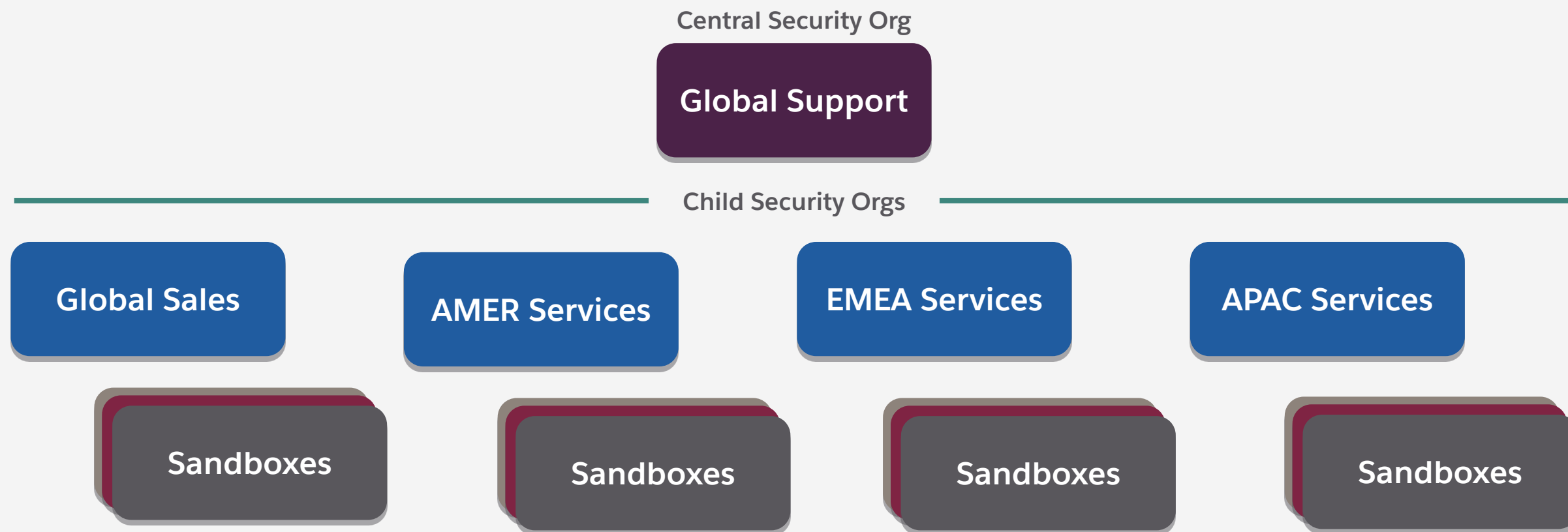
- Created a Security Health Check Org 1 2
- Scheduled the sync job 3 4 5
- Created a Remote Site Setting 6
- Set up the api endpoint
 - Connected App Method 7 8 9 10 11 12
 - OR**
 - Public Site Method 13 14 15 16
- Cloned the metadata type 17 18



Multi-Org Security Reporting



Once a main security org is designated - each of your child orgs can be configured to send their daily security health checks to the central org



Setting up the Child Orgs

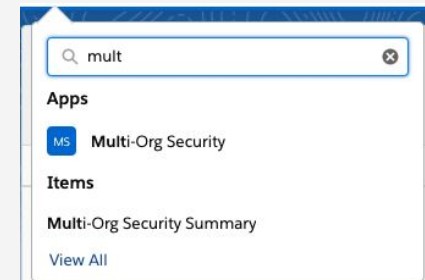
Repeat these steps for each child org.....

Set Up The Central Configuration



Start by creating an entry in the **central** org. This is needed so that the data received can be grouped against the relevant org.

- 1 Open the *Multi-Org Security* app via the app launcher
- 2 Open the *Security Health Check Orgs* tab and click *New* to create the org record for this child org. [See the next page for details of what to provide]



Create Central Security Health Check Record (1/3)



Security Health Check Org

The security health check org record is used to categorize and store security health checks against the relevant org.

Name: The name of the Org

Organization Id: The Id of the Org. This can be found in the *Company Information* section in *Setup*.

Description: Provide an overview of the purpose of the org

Data Classification: The level of security applied to the org

New Security Health Check Org

Information

* Security Health Check Org Name: Global IT Hub

Organization Id: 00D5w000003TfjYEAS

Description: This org is used to manage global IT operations and is used as our security hub org.

Owner: Stephan Garcia

Latest Score: 0

Classification

Data Classification: Internal

Org Type: Production

Status

Active: ☒

Current Org: ☒

Point of Contact

Point of Contact: Stephan Garcia

External Contact Email:

Buttons: Cancel, Save & New, Save

Create Central Security Health Check Record (2/3)



Security Health Check Org cont.

Org Type: Production or Sandbox

Active: True if the org is currently being reported on. Use this toggle to add/remove the org from the summary screens.

Current Org: Set this to **false**.

Point of Contact: The main point of contact for the org

External Contact Email: The email of the point of contact if they are not a user in this Salesforce org

[continued on next page]

The screenshot shows the 'New Security Health Check Org' form in Salesforce. The form is divided into several sections: Information, Classification, Status, Point of Contact, and Integration. The 'Information' section includes fields for 'Security Health Check Org Name' (with a hint icon), 'Owner' (Andrew Paterson), 'Organization Id' (00D4K00000160Gj), 'Latest Score', and a 'Description' text area. The 'Classification' section has dropdowns for 'Data Classification' (Internal) and 'Org Type' (Production). The 'Status' section has checkboxes for 'Active' (checked) and 'Current Org' (unchecked). The 'Point of Contact' section has a 'Point of Contact' dropdown (Pot Anderson) and an 'External Contact Email' field. The 'Integration' section has a 'Token' field and a 'Sync Status' dropdown (Inactive). At the bottom right, there are three buttons: 'Cancel', 'Save & New', and 'Save'.

New Security Health Check Org	
Information	
* Security Health Check Org Name My Child Org Name	Owner Andrew Paterson
Organization Id ⓘ 00D4K00000160Gj	Latest Score
Description Enter a useful description of what the child org is used for.	
Classification	
Data Classification Internal	Org Type Production
Status	
Active ⓘ ☒	Current Org ☐
Point of Contact	
Point of Contact Pot Anderson	External Contact Email ⓘ
Integration	
Token 	Sync Status Inactive
Cancel Save & New Save	

Create Central Security Health Check Record (3/3)



3

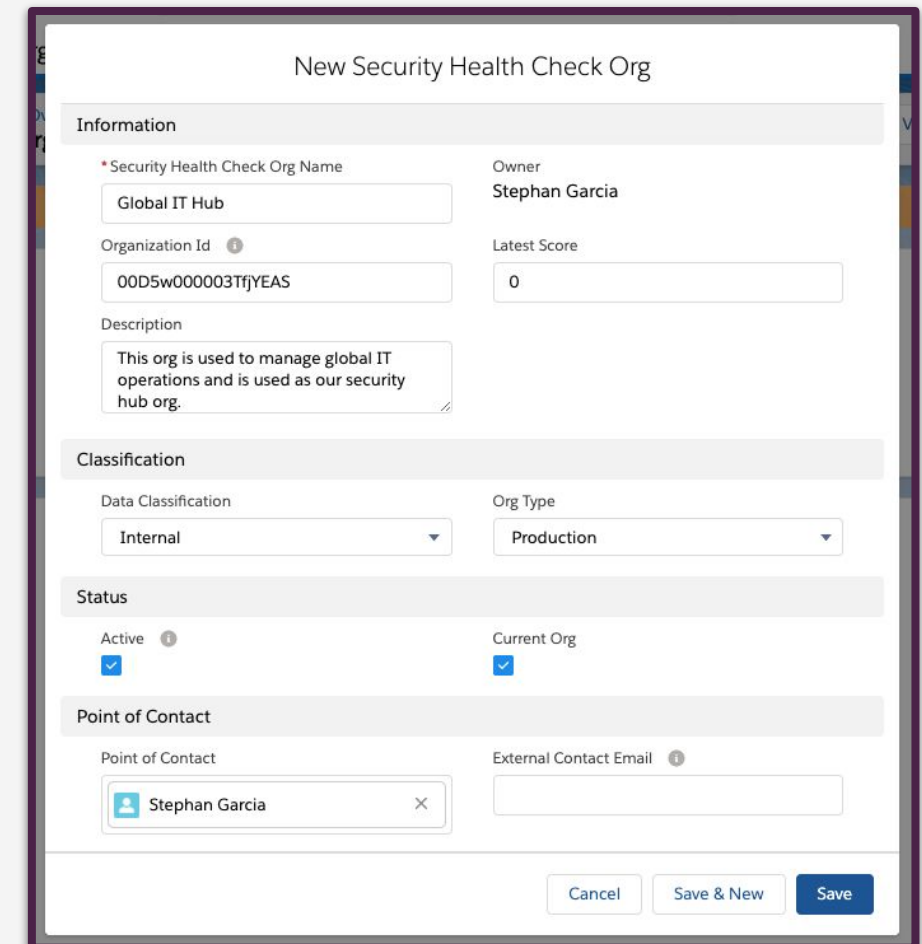
Refresh Token : This is used when receiving data via the endpoint, to ensure that the data is from this child org.

Check this option on to ensure that the token is generated on save. (If you need to re-generate the token then edit the record and check the option on again).



The image shows a section of a form titled "Integration" with a dropdown arrow. It contains two fields: "Token" with the value "pKBSTcjKI/X58R+htcO96oxkCoAFJ1epr/1BPwVCgNU=" and "Refresh Token" with an unchecked checkbox. Both fields have edit icons on the right.

Take note of the token that is generated as you will need this in **step 14** when configuring the custom metadata type.



The image shows a "New Security Health Check Org" form. It is divided into several sections: "Information" with fields for "Security Health Check Org Name" (Global IT Hub), "Owner" (Stephan Garcia), "Organization Id" (00D5w000003TfjYEAS), "Latest Score" (0), and "Description" (This org is used to manage global IT operations and is used as our security hub org.); "Classification" with "Data Classification" (Internal) and "Org Type" (Production); "Status" with "Active" (checked) and "Current Org" (checked); and "Point of Contact" with "Point of Contact" (Stephan Garcia) and "External Contact Email". At the bottom are "Cancel", "Save & New", and "Save" buttons.

Set Up And Configure The Child Org (1/4)



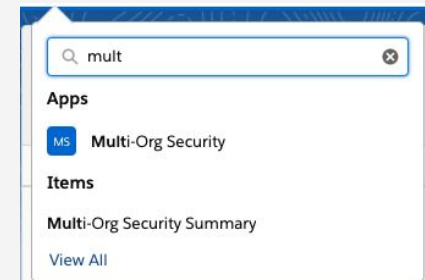
Start by **installing** the package in the **child** org. We will then work through and configure this org to send data to the central org on a daily basis.

4

Open the *Multi-Org Security* app via the app launcher

5

Open the *Security Health Check Orgs* tab and click *New* to create the org record for this child org. This is needed so that details about the org can appear in the summary page. [See the next page for details of what to provide]



Set Up And Configure The Child Org (2/4)



Security Health Check Org

The security health check org record is used to categorize and store security health checks against the relevant org.

Name: The name of the Org

Organization Id: The Id of the Org. This can easily be found in the *Company Information* section in *Setup*.

Description: Provide an overview of the purpose of the org

Data Classification: The level of security applied to the org

The screenshot shows the 'New Security Health Check Org' form in Salesforce. The form is divided into several sections: Information, Classification, Status, and Point of Contact. The 'Information' section includes fields for 'Security Health Check Org Name' (Global IT Hub), 'Organization Id' (00D5w000003TfjYEAS), 'Description' (This org is used to manage global IT operations and is used as our security hub org.), 'Owner' (Stephan Garcia), and 'Latest Score' (0). The 'Classification' section includes 'Data Classification' (Internal) and 'Org Type' (Production). The 'Status' section includes 'Active' (checked) and 'Current Org' (checked). The 'Point of Contact' section includes 'Point of Contact' (Stephan Garcia) and 'External Contact Email' (empty). At the bottom right, there are buttons for 'Cancel', 'Save & New', and 'Save'.

New Security Health Check Org	
Information	
* Security Health Check Org Name Global IT Hub	Owner Stephan Garcia
Organization Id 00D5w000003TfjYEAS	Latest Score 0
Description This org is used to manage global IT operations and is used as our security hub org.	
Classification	
Data Classification Internal	Org Type Production
Status	
Active ☒	Current Org ☒
Point of Contact	
Point of Contact Stephan Garcia	External Contact Email
Cancel Save & New Save	

Set Up And Configure The Child Org (3/4)



Security Health Check Org cont.

Org Type: Production or Sandbox

Active: True if the org is currently being reported on. Use this toggle to add/remove the org from the summary screens.

Current Org: Set this to true

Point of Contact: The main point of contact for the org

External Contact Email: The email of the point of contact if they are not a user in this Salesforce org

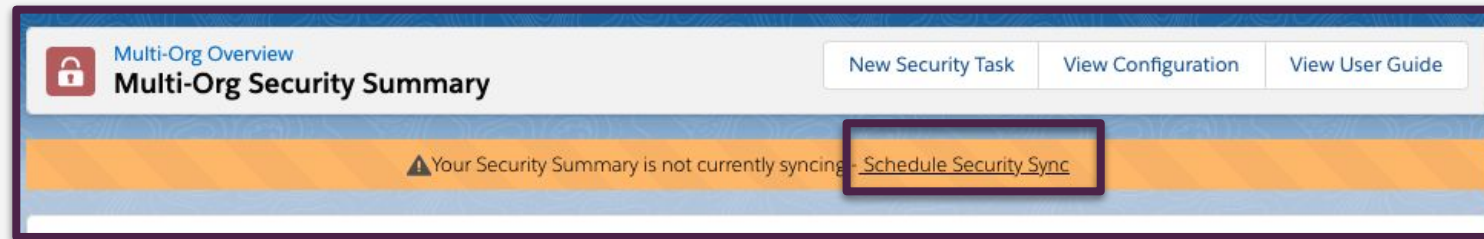
The screenshot shows the 'New Security Health Check Org' form in Salesforce. The form is divided into several sections: Information, Classification, Status, and Point of Contact. The 'Information' section includes fields for 'Security Health Check Org Name' (Global IT Hub), 'Organization Id' (00D5w000003TfjYEAS), 'Owner' (Stephan Garcia), and 'Latest Score' (0). The 'Description' field contains the text: 'This org is used to manage global IT operations and is used as our security hub org.' The 'Classification' section has 'Data Classification' set to 'Internal' and 'Org Type' set to 'Production'. The 'Status' section shows 'Active' and 'Current Org' both checked. The 'Point of Contact' section shows 'Point of Contact' set to 'Stephan Garcia' and 'External Contact Email' as an empty field. At the bottom right, there are buttons for 'Cancel', 'Save & New', and 'Save'.

New Security Health Check Org	
Information	
* Security Health Check Org Name Global IT Hub	Owner Stephan Garcia
Organization Id 00D5w000003TfjYEAS	Latest Score 0
Description This org is used to manage global IT operations and is used as our security hub org.	
Classification	
Data Classification Internal	Org Type Production
Status	
Active ☒	Current Org ☒
Point of Contact	
Point of Contact Stephan Garcia	External Contact Email
Cancel Save & New Save	

Set Up And Configure The Child Org (4/4)



6 Navigate to the summary page and you should see the following information.

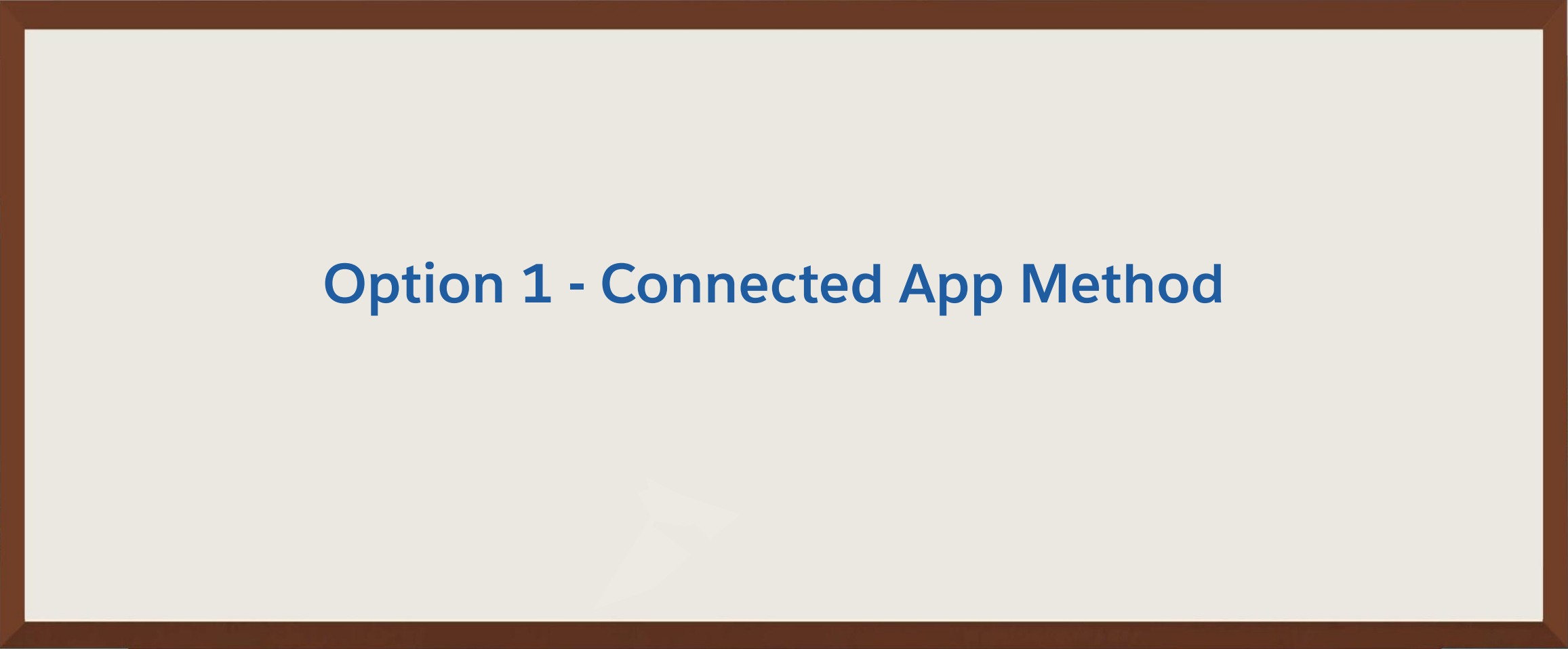


We will return later to set up and run the sync job. Before that we need to configure the reporting end point and appropriate security method.

If you are using the *Connected App* method for sending data to the central org, then proceed with Step 7.

If you are using the *Salesforce site public service* method, you can jump ahead to step 13.



A large, rectangular billboard with a thick brown wooden frame. The billboard is mounted on a grey stone base. The background of the billboard is a light cream color. The text "Option 1 - Connected App Method" is centered on the billboard in a dark blue, sans-serif font. The billboard is set against a light blue background with stylized hills and some green foliage at the bottom corners.

Option 1 - Connected App Method

Child Org - Connected App Method (1/5)



7 Create an Auth Provider

Navigate to Setup > Auth. Providers

Create a new Auth Provider

Provider Type: Salesforce

Name: Designate it a memorable name

Consumer Key & Consumer Secret:
From the central org connected app we created

Child Org

The screenshot shows the 'New Auth Provider' configuration page in Salesforce. The 'Provider Type' is set to 'Salesforce'. The 'Name' is 'Parent Security Org' and the 'URL Suffix' is 'Parent_Security_Org'. The 'Consumer Key' and 'Consumer Secret' are masked with asterisks. The 'Authorize Endpoint URL' is 'https://parent-org.my.salesforce.com/services/oauth2/authorize' and the 'Token Endpoint URL' is 'https://parent-org.my.salesforce.com/services/oauth2/token'. The 'Default Scopes' are 'refresh_token api'. The 'Include Consumer Secret in API Responses' checkbox is checked. The 'Custom Error URL' and 'Custom Logout URL' are empty. The 'Registration Handler' is set to 'Automatically create a registration handler template'. The 'Execute Registration As' dropdown is set to '--None--'. The 'Icon URL' is empty, with a link to 'Choose one of our sample icons'.

Central Org

The screenshot shows the 'API (Enable OAuth Settings)' section in the Salesforce setup. It displays the 'Consumer Key' and 'Consumer Secret' for a connected app, both of which are masked with black boxes.

Child Org - Connected App Method (2/5)



8

Create an Auth Provider (cont.)

Authorize Endpoint: `https://central-org-domain.my.salesforce.com/services/oauth2/authorize`

Token Endpoint: `https://central-org-domain.my.salesforce.com/services/oauth2/token`

Default Scopes: `refresh_token api`

Include Consumer Secret In Api Responses: `True`

Authorize Endpoint URL	https://parent-org.my.salesforce.com/services/oauth2/authorize	
Token Endpoint URL	https://parent-org.my.salesforce.com/services/oauth2/token	
Default Scopes	refresh_token api	
Include Consumer Secret in API Responses	☒	

Child Org - Connected App Method (3/5)



9

Save the auth. provider

When saved, copy the callback URL. We need to copy this into the **central** connected app configuration.

Salesforce Configuration	
Test-Only Initialization URL	https://multioass-hub-6.my.salesforce.com/services/auth/test/MultiOrgSecuritySummary
Existing User Linking URL	https://multioass-hub-6.my.salesforce.com/services/auth/link/MultiOrgSecuritySummary
OAuth-Only Initialization URL	https://multioass-hub-6.my.salesforce.com/services/auth/oauth/MultiOrgSecuritySummary
Callback URL	https://multioass-hub-6.my.salesforce.com/services/authcallback/MultiOrgSecuritySummary
Single Logout URL	https://multioass-hub-6.my.salesforce.com/services/auth/rp/oidc/logout

10

Update the connected app record

Open the central connected app configuration and populate the Callback URL. If this is the first child org you will need to replace the Temporary Callback URL we set earlier. **Note:** You can have one callback url per line.

API (Enable OAuth Settings)

Enable OAuth Settings

☒

Enable for Device Flow

☐

Callback URL

https://multioass-hub-6.my.salesforce.com/services/authcallback/MultiOrgSecuritySummary

Child Org - Connected App Method (4/5)



11 Set up the Named Credentials

The child org scheduled service uses Named Credentials when making the call out to the central org.

Back in the child org, navigate to *Setup > Named Credentials*

Name: Designate it a memorable name

URL: <https://mydomain.my.salesforce.com> (This is the central domain URL and needs to be the ...my.salesforce.com URL for Authenticated users or the force.com URL for the sites method)

Identity Type: Named Principal

Authentication Provider: The Auth Provider we just created

The screenshot shows the Salesforce Named Credentials configuration interface. The 'Label' field is 'Parent Security Org' with a user icon. The 'Name' field is 'Parent_Security_Org'. The 'URL' field is 'https://mydomain.my.salesforce.com' and is highlighted with a blue border. Below these fields is a section titled 'Authentication' with a dropdown arrow. It contains the following fields: 'Certificate' (empty text box with a magnifying glass icon), 'Identity Type' (dropdown menu showing 'Named Principal'), 'Authentication Protocol' (dropdown menu showing 'OAuth 2.0'), 'Authentication Provider' (text box showing 'MultiOrgSecuritySumma' with a magnifying glass icon), 'Scope' (text box showing 'refresh_token api'), 'Authentication Status' (text box showing 'Pending'), and 'Start Authentication Flow on Save' (checkbox that is checked). Below the 'Authentication' section is another section titled 'Callout Options' with a dropdown arrow. It contains three fields: 'Generate Authorization Header' (checkbox that is checked), 'Allow Merge Fields in HTTP Header' (checkbox that is unchecked), and 'Allow Merge Fields in HTTP Body' (checkbox that is unchecked).

Child Org - Connected App Method (5/5)



Set up the Named Credentials (cont.)

Scope: refresh_token api

Start Authentication Flow on Save: True - this will allow to authenticate the central org with our credentials

Generate Authorization Header: True

12

Save the named credential

On saving the record you will then ask you to log into the central org. Login, and you're now authorized.

The screenshot shows the configuration page for a Named Credential in Salesforce. The fields are as follows:

- Label:** Parent Security Org
- Name:** Parent_Security_Org
- URL:** https://mydomain.my.salesforce.com

The **Authentication** section is expanded, showing:

- Certificate:** (empty field with a search icon)
- Identity Type:** Named Principal
- Authentication Protocol:** OAuth 2.0
- Authentication Provider:** MultiOrgSecuritySumma
- Scope:** refresh_token api
- Authentication Status:** Pending
- Start Authentication Flow on Save:** ☒

The **Callout Options** section is also expanded, showing:

- Generate Authorization Header:** ☒
- Allow Merge Fields in HTTP Header:** ☐
- Allow Merge Fields in HTTP Body:** ☐

A large, rectangular billboard with a thick brown wooden frame. The billboard is mounted on a grey stone base. The background of the billboard is a light cream color. The text "Option 2 - Salesforce Sites Method" is centered on the billboard in a dark blue, sans-serif font. The billboard is set against a light blue background with stylized hills and some green foliage at the bottom corners.

Option 2 - Salesforce Sites Method

Child Org - Salesforce Sites Method



13

Set up the Named Credentials

Navigate to *Setup > Named Credentials*

Label: Designate it a memorable name

URL: The secure url of the central site you created earlier

Identity Type: Anonymous

Authentication Protocol: No Authentication

Generate Authorization Header: true

You will need the Developer Name (Name field) for the next steps.

The screenshot shows the Salesforce Named Credentials configuration page. The fields are as follows:

- Label:** Parent Security Org Cre
- Name:** Parent_Security_Org_Cre
- URL:** https://multi-org-security-demo.secure.force.com/

The **Authentication** section is expanded, showing:

- Certificate:** (Empty field with a search icon)
- Identity Type:** Anonymous
- Authentication Protocol:** No Authentication

The **Callout Options** section is expanded, showing:

- Generate Authorization Header:** ☒
- Allow Merge Fields in HTTP Header:** ☐
- Allow Merge Fields in HTTP Body:** ☐

Finalise the Child Org Configuration



The following instructions apply regardless of whether you are using Option 1 or Option 2.



Child Org - Metadata configuration (1/2)



14

Clone the Security Health Check Config

Navigate to *Setup > Custom Metadata Types*

Select *Manage Records* for the Security Health Check Config record and then select *Configuration* in the configs list.

Clone the record.

Label: Give this a label that allows you to identify the record

Security Health Check Config Name: Make sure you change this to reflect the Label above. *[If the Name is left as Configuration, it will be ignored and the sync will not work !]*

Central Org URL: Leave as the default

[continue on the next page]

Label	Configuration
Security Health Check Config Name	Configuration
Central Org URL	/services/apexrest/multiorg/SecurityHealthCheckReporting
Token	Add Parent Org Token
Named Credentials	Add Named Credentials
Is this the Central org?	☒
Security Superstar Threshold	10
Created By	Stephan Garcia, 5/1/2020, 2:58 PM

Label	Value
Label	Child Org
Security Health Check Config Name	Child_Org
Central Org URL	/services/apexrest/multi
Token	S3AJU53jaM5vB8y8Tq+
Named Credentials	Parent_Security_Org_Cr
Is this the Central org?	☐
Security Superstar Threshold	10

Child Org - Metadata configuration (2/2)



Token: Enter the token belonging to the **child** org that was created earlier in the **central** org.

This token will be sent with the reporting data and needs to match the central org record to be saved.

Named Credentials: The name of the named credential you've just created.

Is this the central org: False. This setting controls whether you see the multi-org version of the app page, or the single org version.

Security Health Check Config

EditClone

Detail

Label	Configuration
Security Health Check Config Name	Configuration
Central Org URL	/services/apexrest/multiorg/SecurityHealthCheckReporting
Token	Add Parent Org Token
Named Credentials	Add Named Credentials
Is this the Central org?	☒
Security Superstar Threshold	10
Created By	Stephan Garcia, 5/1/2020, 2:58 PM

EditClone

Information

Label	Child Org
Security Health Check Config Name	Child_Org
Central Org URL	/services/apexrest/multi
Token	S3AJU53jaM5vB8y8Tq+
Named Credentials	Parent_Security_Org_Cr
Is this the Central org?	☐
Security Superstar Threshold	10

15

Save the record

Create Remote Site Settings



Create Two Remote Site Settings in the Child Org

Navigate to *Setup > Remote Site Settings*

- 16 **Create Remote site Setting 1:** <https://central-org-mydomain.my.salesforce.com>
The mydomain url for the central org will allow us to send the health checks

A screenshot of the 'Remote Site Settings' form in Salesforce. The form is enclosed in a dark purple border. It contains the following fields: 'Remote Site Name' with a text input field; 'Remote Site URL' with a text input field; 'Disable Protocol Security' with an unchecked checkbox and an information icon; 'Description' with a large text area; and 'Active' with a checked checkbox.

Remote Site Name	
Remote Site URL	
Disable Protocol Security	☐
Description	
Active	☒

- 17 **Create Remote Site Setting 2:** <https://this-org-mydomain--c.visualforce.com>
This link for the child org will allow us to get the Health Check from the Tooling API



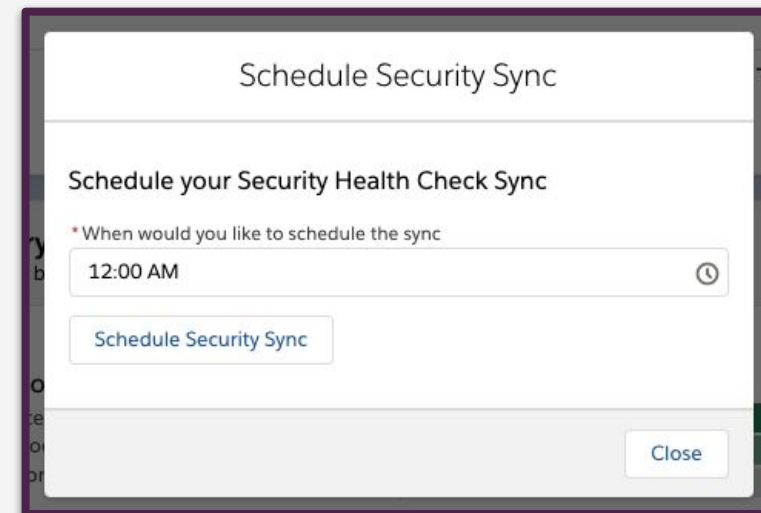
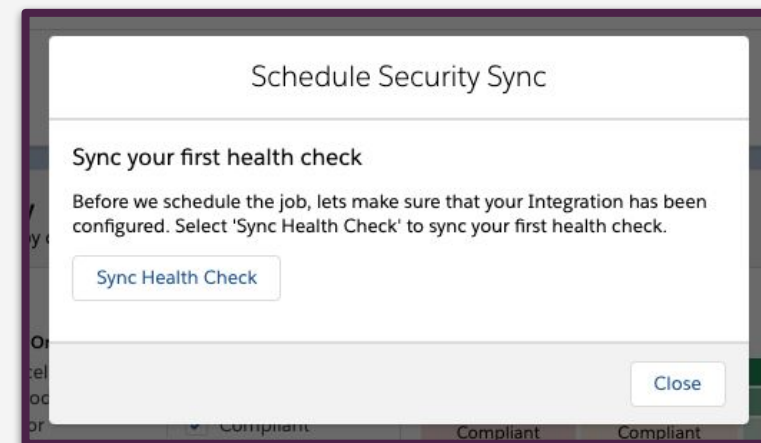
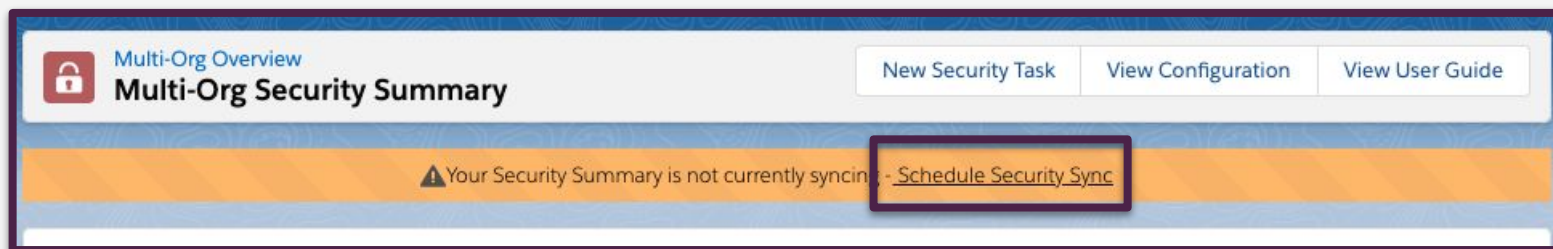
Schedule the Health Check Sync



18

Navigate to the Multi-Org Security Summary tab in the child org and select '*Schedule Security Sync*' from the warning banner that is displayed.

This will allow us to sync the first health check and write the data to this org. Once completed, schedule the daily sync from the next prompt. This can be changed at any time.



[illegible]

Child Org Checklist

salesforce

That should be the child org configured and ready to go. Ensure that you have:-

- Set Up The Child Configuration
- Set up the Reporting Method
 - Connected App Method
 - OR**
 - Public Site Method
- Finalised the Child Org Configuration



Current Security Status

From the multi-org security summary you can see the status of the security health check across your company's Salesforce instances. Once configured, your orgs will report on a daily basis, allowing insight into changes made and areas for improvement.

Multi-Org Statistics

Active Production Orgs	Active Sandbox Orgs	Average Security Score ⓘ	Total Open Security Tasks
2	0	75	0

Daily Security Summary

Explore the org security settings by date

Filter

Select Date
May 2, 2020

Select Org Status

- ☒ Excellent
- ☒ Good
- ☒ Poor

Select Risk Status

- ☒ Critical
- ☒ Warning
- ☒ Compliant

Key

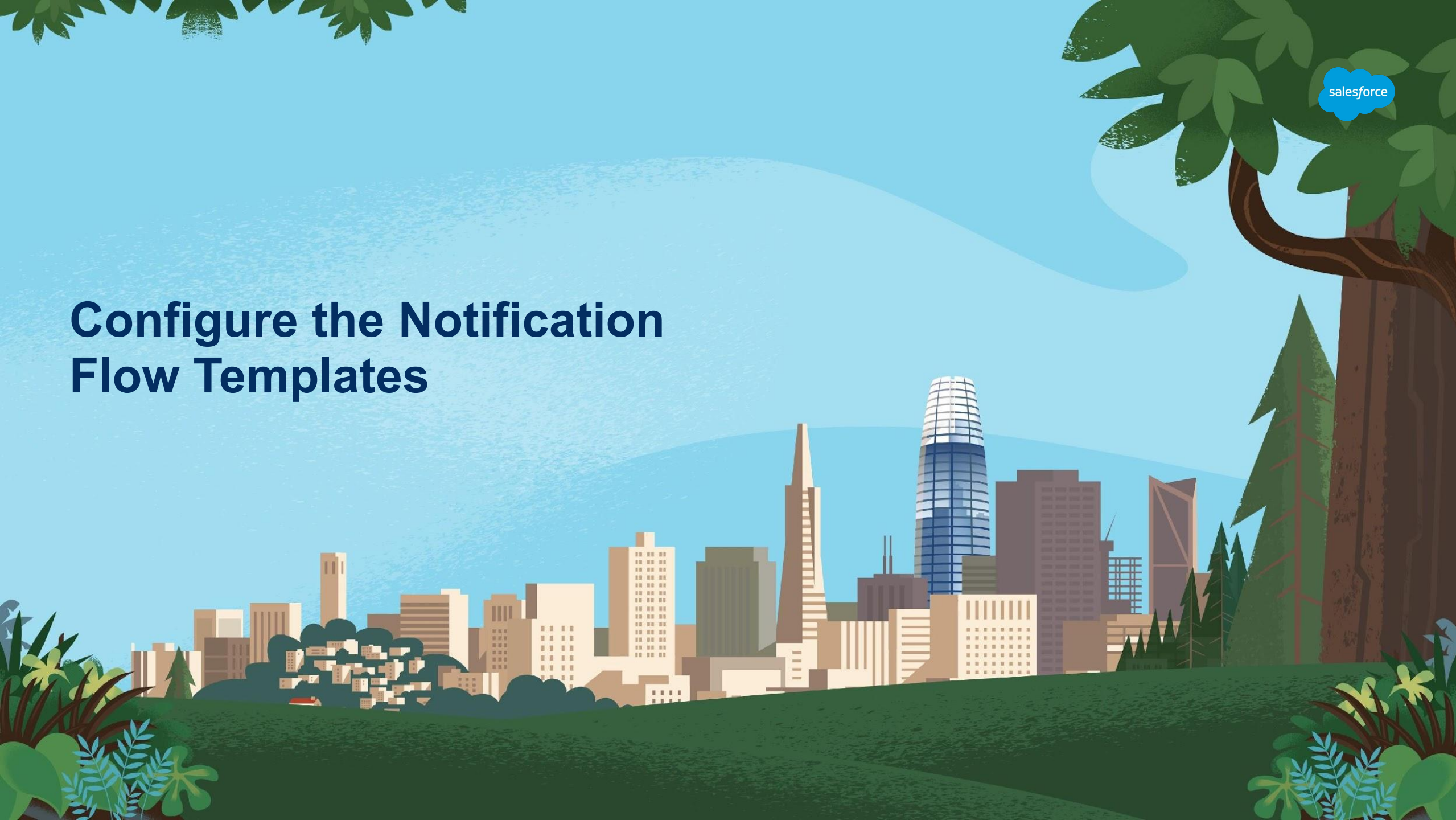
High Risk	Medium Risk	Low Risk	Informational
Critical	Critical	Critical	Critical
Warning	Warning	Warning	Warning
Compliant	Compliant	Compliant	Compliant

Sort Order
By Name

81 Global Sales

68 Global IT Hub

Configure the Notification Flow Templates



Create A Custom Notification Type



A custom notification type will be used to alert your admins when the status of their security health check has changed.

Navigate to Setup > Custom Notification types

Notification Name: Security Health Check Notifications

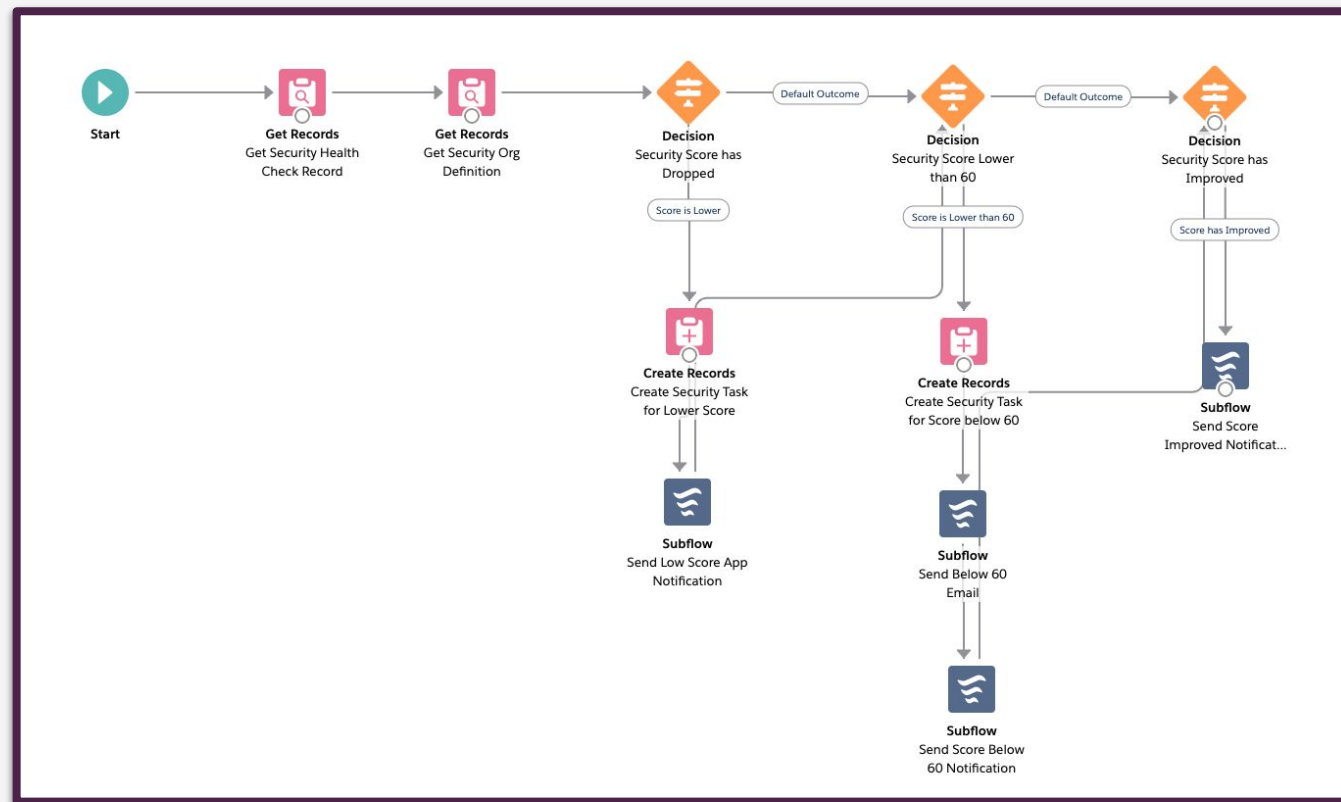
Supported Channels: You can send notifications on the desktop and to users Salesforce mobile app

A screenshot of the 'New Custom Notification Type' form in Salesforce. The form has a title bar at the top that says 'New Custom Notification Type'. Below the title bar, there are two required fields: 'Custom Notification Name' and 'API Name'. The 'Custom Notification Name' field contains the text 'Security Health Check Notifications'. The 'API Name' field contains the text 'Security_Health_Check_Notifications'. Below these fields, there is a section titled 'Supported Channels' with two checkboxes: 'Desktop' and 'Mobile', both of which are checked. At the bottom right of the form, there are two buttons: 'Cancel' and 'Save'.

Security Summary Evaluation Flow Template



Using flow, you have the ability to evaluate the Security Health Check when it has been created and check for any anomalies.



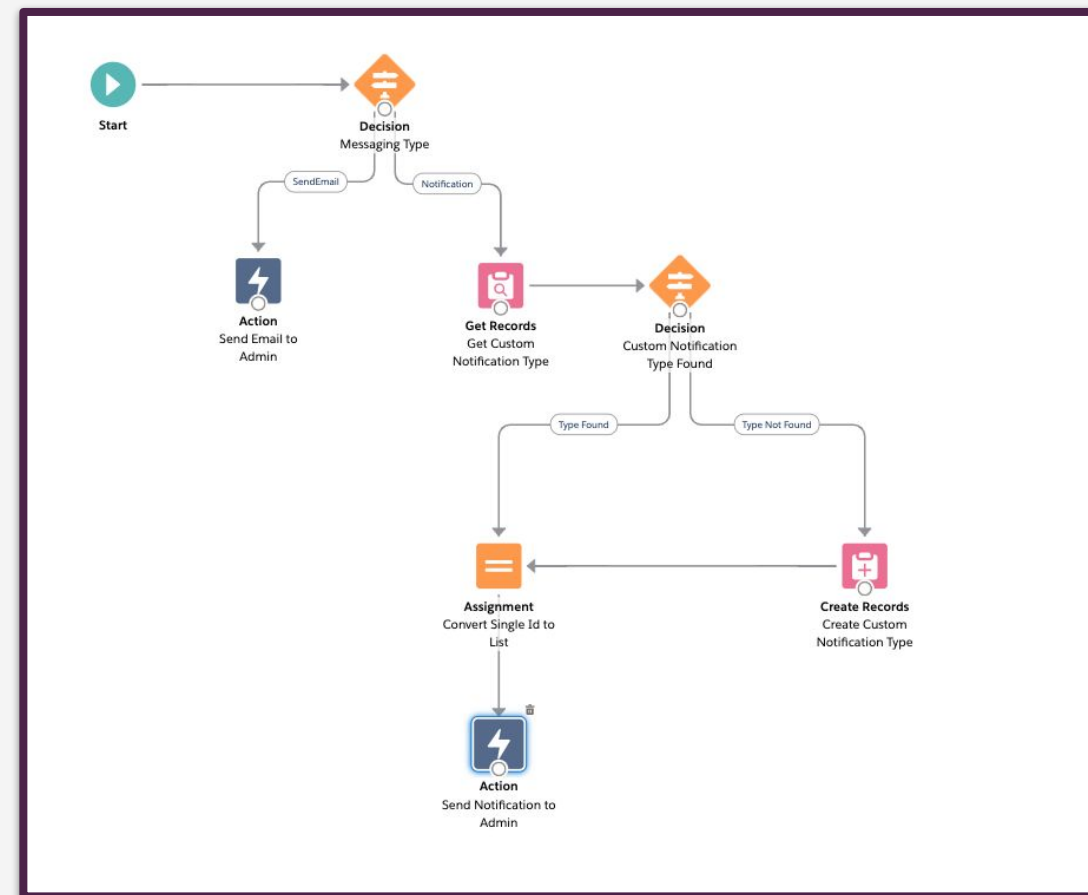
Security Summary Notification Flow Template



Using flow, you have the ability to send email and in-app notifications to Admin users who have had a security report generated.

You must supply the type of notification, email or notification. Then supply either the Admins email address or record Id.

This will then let them know that they have a security action that needs to be taken care of.



Security Tasks



Security Health Check Tasks



Security Tasks are used to assign actions to your team of admins who are responsible for managing the security of your salesforce orgs!

Subject - the instructions that you would like your user to action.

Assigned to: Designate an Admin to complete this task

Related to Org: Select which org this security task is related to

Related to Risk: The risk that this task is associated to.

A task does **NOT** need to be associated to a specific org, risk or user

Security Health Check: Create Task

Use this form to track tasks relating to improving security scores for orgs and/or risks.

* Subject
Update the login password policies to our company standards in accordance with the docs. ⓘ

Due Date
May 15, 2020 ⓘ

* Severity
High ▼

Assigned To
Stephan Garcia ×

Related To Org
Global IT Hub ×

Related To Risk
SECRISK-0004 ×

Cancel Create Task

Security Health Check Tasks



Open Task Notifications

When you are viewing the multi-org overview or a single org, you can see the number of relevant open tasks.

Current Security Status

From the multi-org security summary you can see the status of the security health check across your company's Salesforce instances. Once configured, your orgs will report on a daily basis, allowing insight into changes made and areas for improvement.

Multi-Org Statistics

Active Production Orgs	Active Sandbox Orgs	Average Security Score ⓘ	Total Open Security Tasks
7	1	50	7

Security & Privacy Hub

This org is used for managing all of our security operations, privacy, & data governance.

Org Details

Org Id:	a004R00000gcdZVQAY	Current Security Score 68 0 days ago	Open Security Tasks 3
Category:	Sandbox		
Data Classification:	Mission Critical		
Admin:	Stephan Garcia		

Security Health Check Tasks



If the Security Task is linked to a risk - the Admin will have direct access to any relevant documentation that will help them fix the vulnerability.

Security Tasks					
Security Administrator					
Subject	Severity	Status	Assigned to	Due Date	
This community needs to require 2-factor, please implement this.	Medium	Created	Todd Chavez	May 20, 2020	▼
Can you please decrease the number of login attempts?	Low	Created	Sarah Lynn	May 9, 2020	▼

View Security Task

Details

Subject

Can you please update the password policies, they're far to relaxed in this org.

Severity

Medium

StatusSecurity DetailsOrg Details

Security Setting

Require a minimum 1 day password lifetime

Your Value

Disabled

Standard Value

Require a minimum 1 day password lifetime

Information Links

[Set Password Policies](#)

CloseUpdate

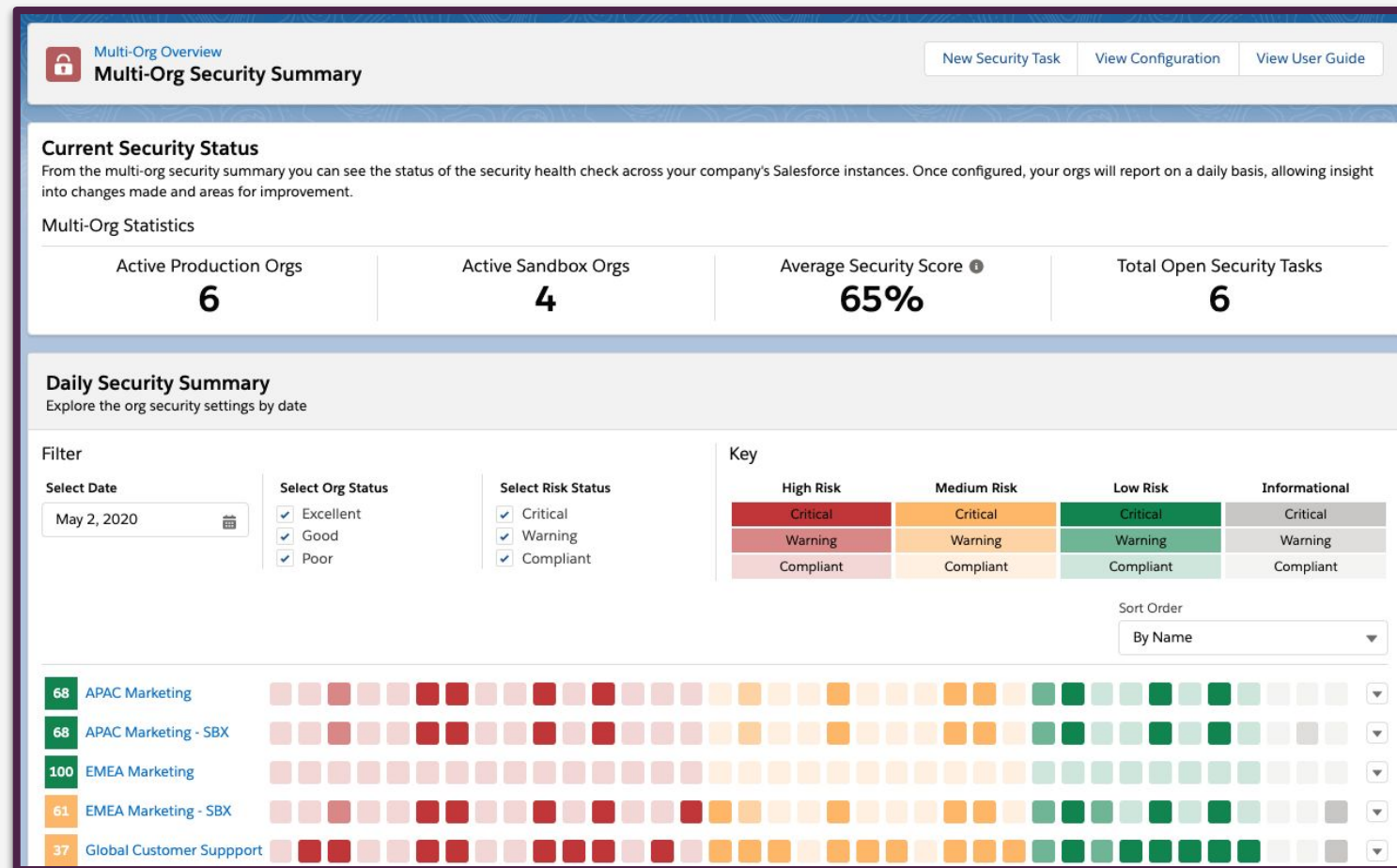
Navigating Multi-Org Security Summary



Navigating Multi-Org Security Summary



Now that we have the app setup - lets take a look at it's features.



Navigating Multi-Org Security Summary



Central Org - Multi-Org Security Status

When you first navigate to the Multi-Org Security Summary - you can see an overview of all of the associated orgs that are syncing to your central org, along with their stats.

 [Multi-Org Overview](#)

Multi-Org Security Summary

[New Security Task](#) [View Configuration](#) [View User Guide](#)

Current Security Status

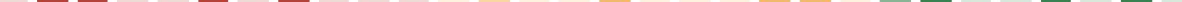
From the multi-org security summary you can see the status of the security health check across your company's Salesforce instances. Once configured, your orgs will report on a daily basis, allowing insight into changes made and areas for improvement.

Multi-Org Statistics

Active Production Orgs	Active Sandbox Orgs	Average Security Score ⓘ	Total Open Security Tasks
11	16	68%	23

The daily security summary is where you will find an overview of ALL of your configured Salesforce Orgs

As you can see, the darker the shade of the risk, the more important it is for the risk to be resolved.



Navigating Multi-Org Security Summary



Central Org - Daily Security Summary

When you hover over a risk item, you will be shown a pop-over containing information about the risk.

Description: You can see the security risk that has been selected

Expected Value: The value that Salesforce regards as secure

Actual Value: Your current security setting in this org

Description: Links to the relevant documentation needed to solve the security issue

Actions: You can create a task for the admin that is responsible for this org

A pop-over window with a dark purple border. At the top, there is a row of colored squares (red, light red, pink, yellow, orange, light yellow, white, orange, yellow, light yellow, white). Below this, a green checkmark icon is followed by the text "Compliant". The main content area is divided into sections: "Description" with the text "Require secure connections (HTTPS)", "Expected Value" with the text "Enabled", and "Actual Value" with the text "Enabled". Below these is a section titled "Information Links" containing three blue links: "Knowledge Article", "Winter 15: Release Notes", and "Salesforce Sites Security Spring 20: Critical Update". At the bottom of the main content area is a section titled "Actions" with a button that has a list icon and the text "Create Task". A red banner at the very bottom of the pop-over contains the text "High-Risk Security Setting" in white.

Navigating Multi-Org Security Summary



Central Org - Selected Org

You can select the name of the child org and navigate to a detailed view of that org.

 [Multi-Org Overview](#) > [Global IT Hub](#)
Multi-Org Security Summary

[New Security Task](#) [View Configuration](#) [View User Guide](#)

Global IT Hub

This org is used to manage global IT operations and is used as our security hub org.

Org Details

Org Id:	a015w00001Cqgu5AAB
Category:	Production
Data Classification:	Internal
Admin:	Stephan Garcia

Current Security Score

68

0 days ago

Open Security Tasks

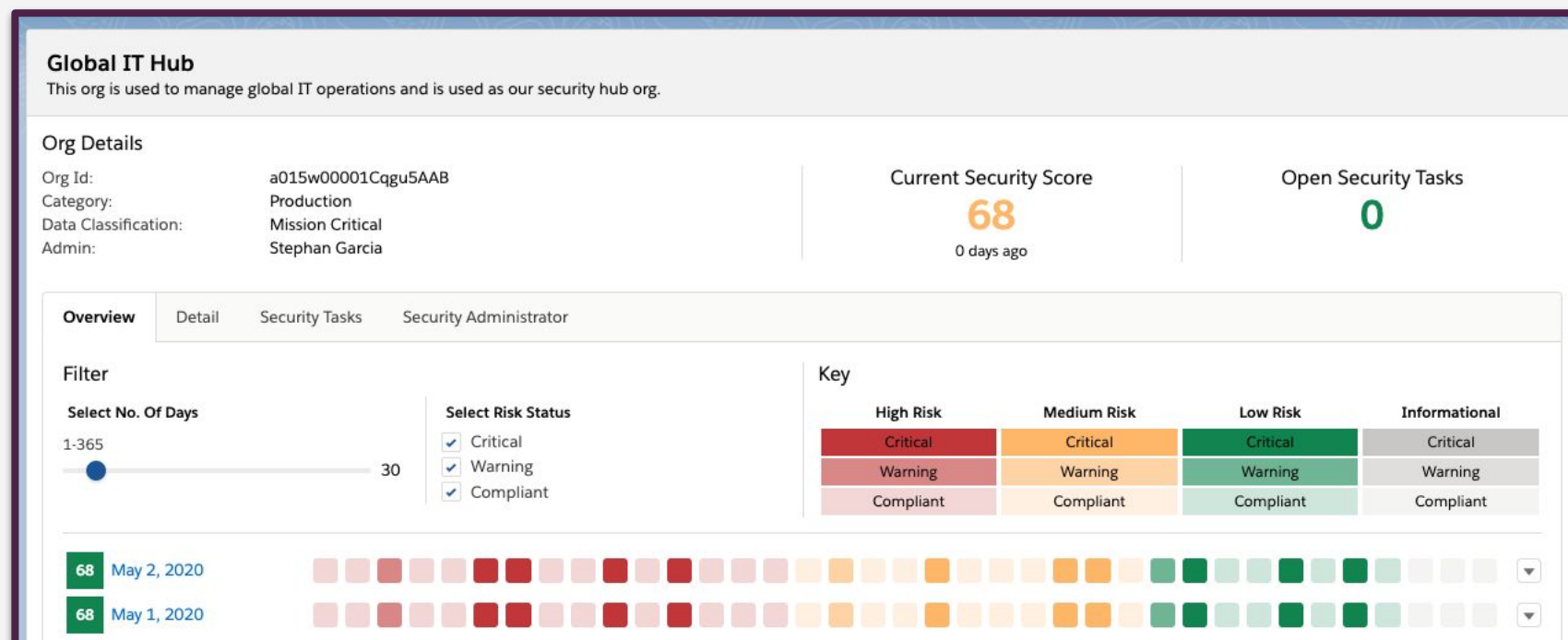
5

Navigating Multi-Org Security Summary



Central Org - Selected Org

You can select the name of the child org and navigate to a detailed view of that org. The single org view will give you the options to view the daily overview, the detail of health check, the security tasks, and the admin.

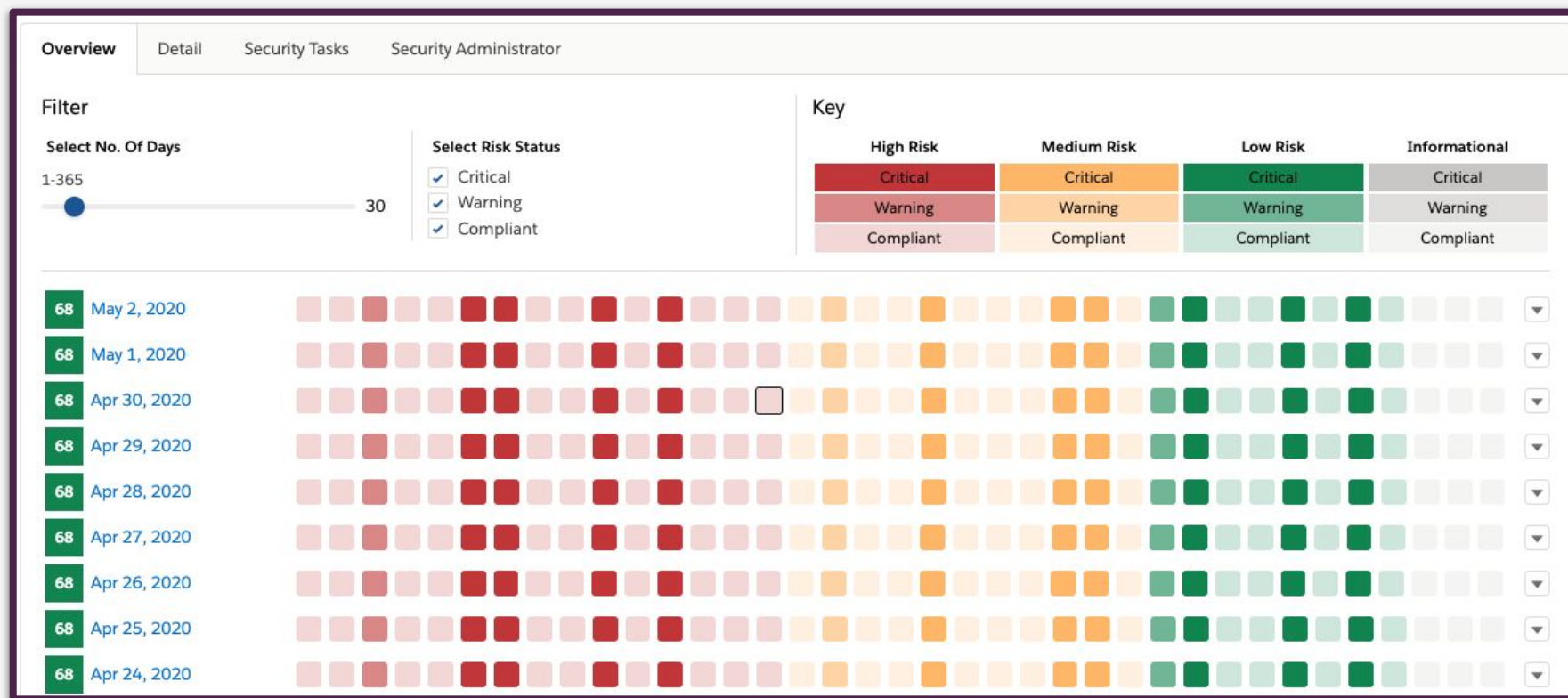


Navigating Multi-Org Security Summary



Selected Org - Overview

This tab will show you all of your health checks for this org sorted by date, this way you can track security trends and spot changes in the health check.

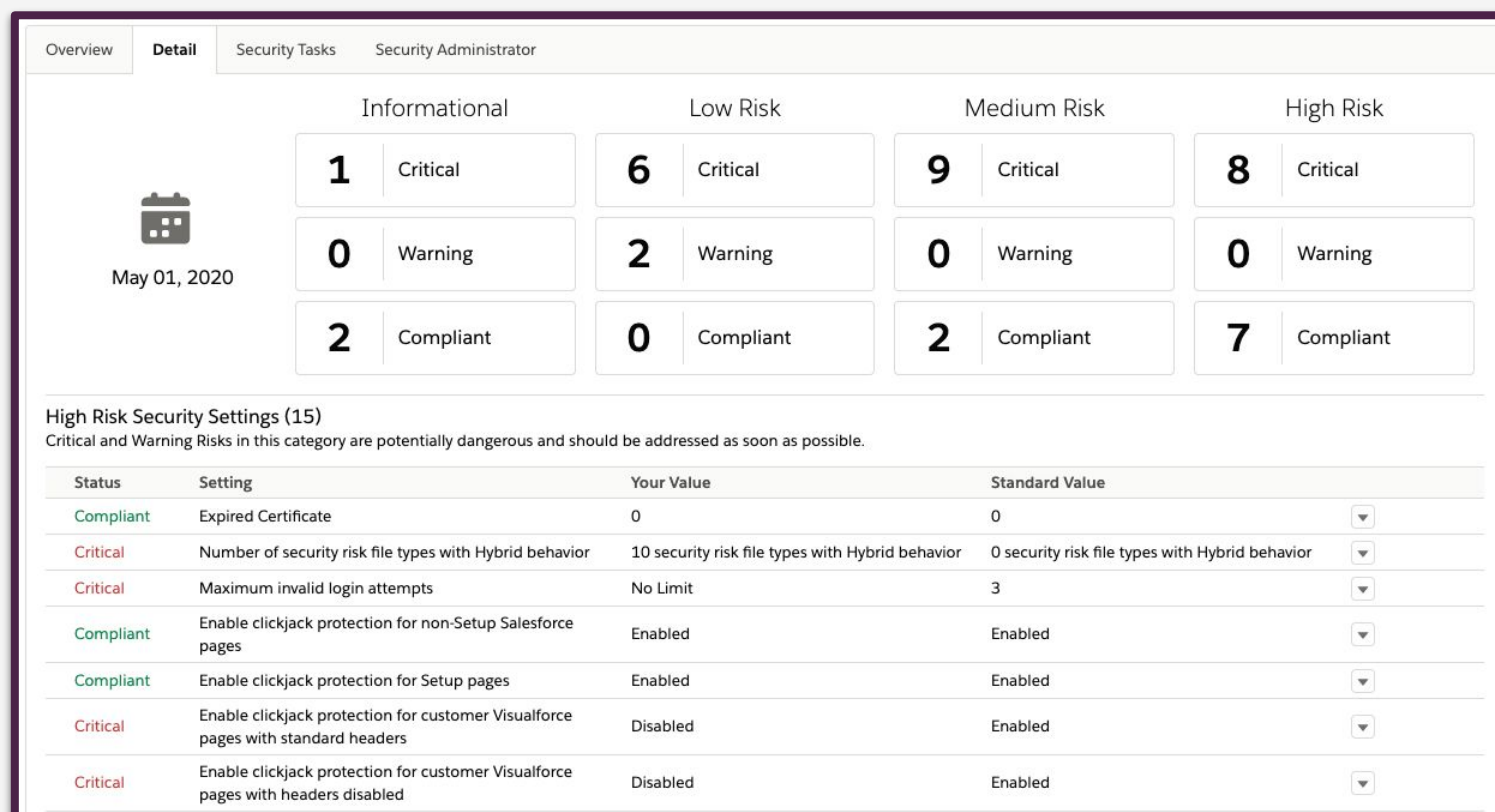


Navigating Multi-Org Security Summary



Selected Org - Details

The detail view will give you an indepth look at each days security health check.



Navigating Multi-Org Security Summary



Selected Org - Security Tasks

The security task detail view gives you a list of all the tasks associated to the selected org.

Overview

Detail

Security Tasks

Security Administrator

Subject	Severity	Status	Assigned to	Due Date	
This community needs to require 2-factor, please implement this.	Medium	Created	Todd Chavez	May 20, 2020	▼
Can you please decrease the number of login attempts?	Low	Created	Sarah Lynn	May 9, 2020	▼

View Security Task

Details

Subject

Can you please update the password policies, they're far to relaxed in this org.

Severity

Medium

Status

Security Details

Org Details

Security Setting

Require a minimum 1 day password lifetime

Your Value

Disabled

Standard Value

Require a minimum 1 day password lifetime

Information Links

[Set Password Policies](#)

Close

Update

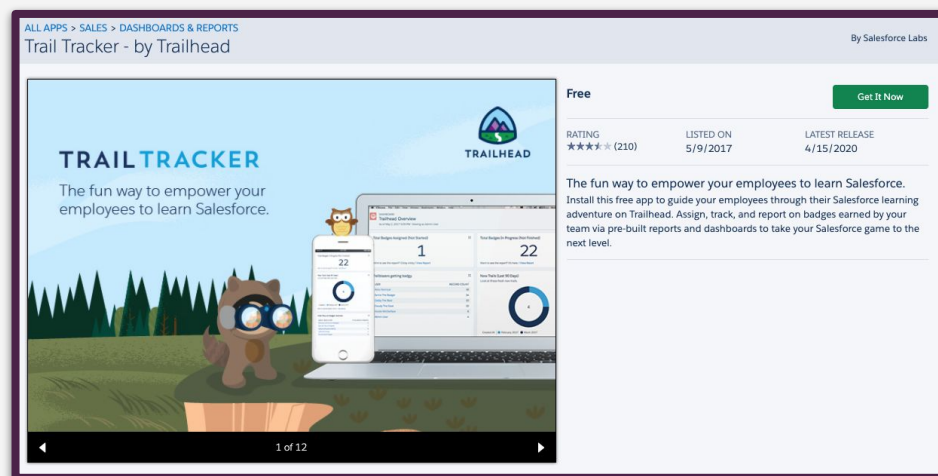
Navigating Multi-Org Security Summary



Selected Org - Security Admin

View the Admin who is in charge of security for the selected org - pull in their user detail from their record and let them show off their security Trailhead badges & certifications.

This functionality could be extended Trail Tracker by Salesforce Labs - available now on the AppExchange!



OverviewDetailSecurity TasksSecurity Administrator



Stephan Garcia

Security Specialist

USA

[Trailblazer.me Profile](#)

I've recently joined the Developer Evangelist Team, based in Las Vegas, NV. Previously I was part of the Cloud/Technical Architect, Platform SE Team in London. Prior to joining Salesforce, I worked across the Public and Private Sectors in the UK as well as the USA. While working with Methods, I helped establish the Salesforce Consulting Practice and bring it to the top of the Public Sector. In 2017, I founded and engineered the Privacy 360 app on the Salesforce AppExchange alongside Elements.Cloud.

* Security Superstar

Certifications

	Name	Description	Skill Level	Link
	Sharing & Visibility Designer Certification	The Salesforce Certified Sharing and Visibility Specialist is designed for architects, analysts, and administrators who want to demonstrate their knowledge, skills, and capabilities to design secure, scalable security models on the Force.com platform.	Advanced	View Course

Trailhead Badges

	Name	Description	Skill Level	Link
	Application Security Basics	Learn about application security and the job of an application security engineer.	Beginner	View Course
	Data Leak Prevention	Learn coding best practices to safeguard your Salesforce data.	Advanced	View Course
	Data Security	Control access to data using point-and-click security tools.	Intermediate	View Course
	Security Specialist	Flex your security muscles by locking down permissions and tracking changes.	Intermediate	View Course

Troubleshooting

Things to check if it doesn't seem to be working and you followed all the steps....

Authenticated Method (Option 1)

- Does the user you have configured in the child Named Credentials have access to the Connected App? [check Step 11 of the Central configuration]
- Does the url you entered in Child step 8 match the domain of the central org? [check it is ...my.salesforce.com]

Authenticated Method (Option 2)

- Does the url you configured in Central step 14 match the value you entered in Child step 13 ?

Both Methods (Metadata configuration)

- In the Central step 17 or Child step 14 - did you rename the Label **and** the Name? If the Name is left as 'Configuration' it will not sync.
- In the Child configuration - Does the Named Credentials in the cloned metadata record match the name you set in the Named Credentials?
- In the Child configuration - Does the Token in the cloned metadata record match the value generated in the central org Security Health Check Org record?





Thank
you

BLAZE
YOUR
TRAIL

salesforce