Introduction

Orgplus is a Salesforce specific AppExchange package which can help the subscribers view various aspects of security in a user friendly manner.

Post Installation Configuration Guide

Note - Various functionalities of this application leverage Salesforce APIs such as Tooling API to present the data in a meaningful way. To provide access to these APIs securely, this app leveraged Named Credential, Auth Provider and Connected App combination. These components need to be created and configured to work for the specific org or sandbox.

Since we do use REST APIs to provide some of the data in this application, please be mindful of your org's API limits.

Once the managed package is installed, following steps are to be followed to configure the app:

1. Assign the "OrgPlus Viewer" permission set to the appropriate users.
2. Create a Connected App.
3. Create an Auth. Provider.
4. Create a Named Credential.
5. Update the Custom Setting "OrgPlus Configuration" to add a setting for the org default.

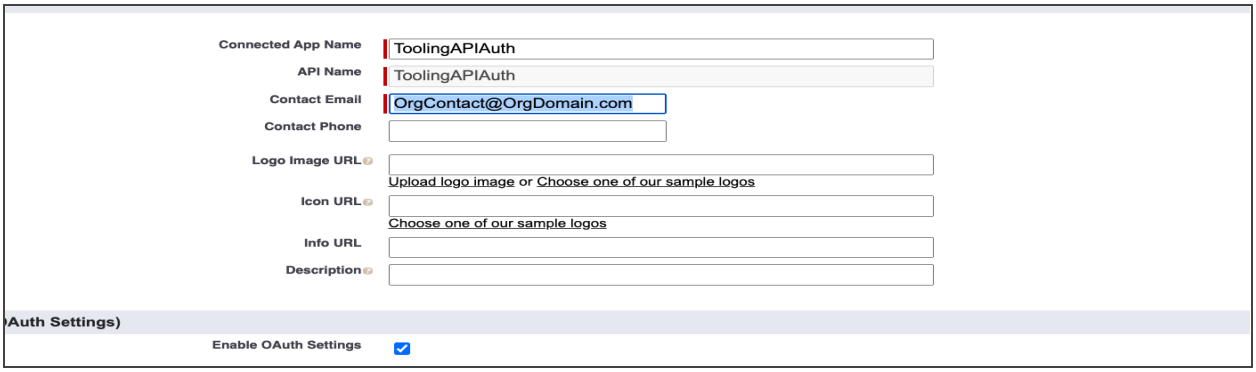
Assign Permission Set

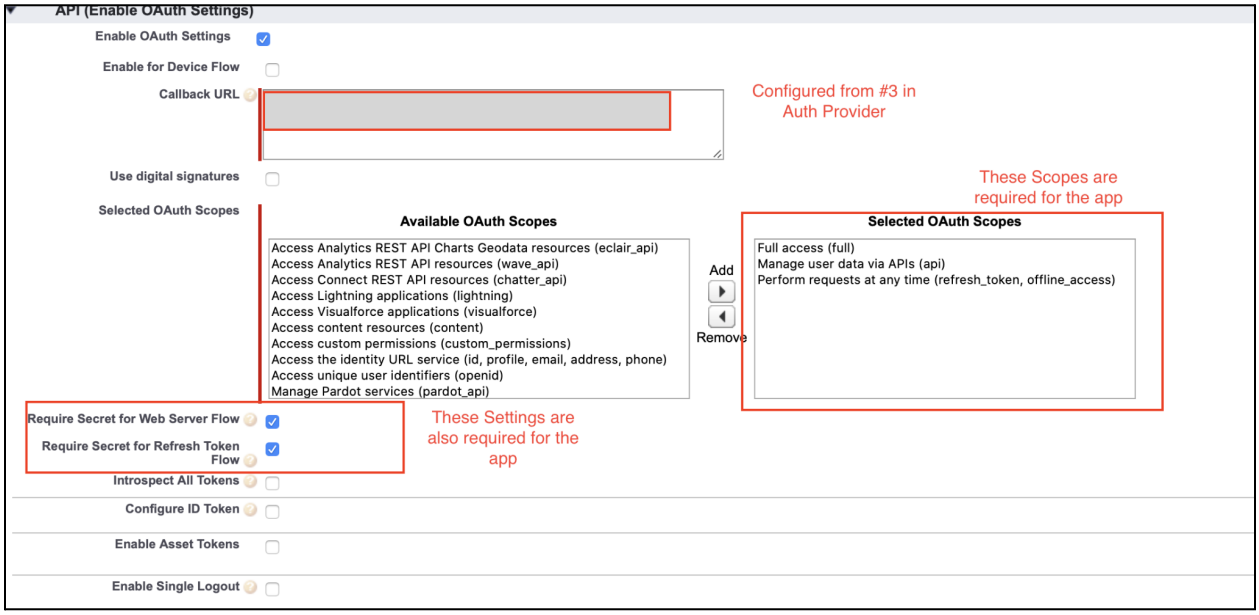
This app has been granted access to using a Permission Set "OrgPlus Viewer". To initiate the process, first assign this permission set to an administrator who'll perform other configurations for this app. This administrator needs to be assigned a "System Administrator" profile or any comparable custom profile which grants various administrative accesses in the org or sandbox.

Connected App Configuration

Create a connected app to authorize your credentials against the org for Tooling API. This is to establish the best practices and ensure that access tokens that this app will use can't be misused in any case.

Create a connected app like the one shown in the screenshot below. The name can be whatever you want, just make sure it is descriptive enough so that when you look at it, you know what it's purpose is. In our example, we use the name "ToolingAPIAuth".





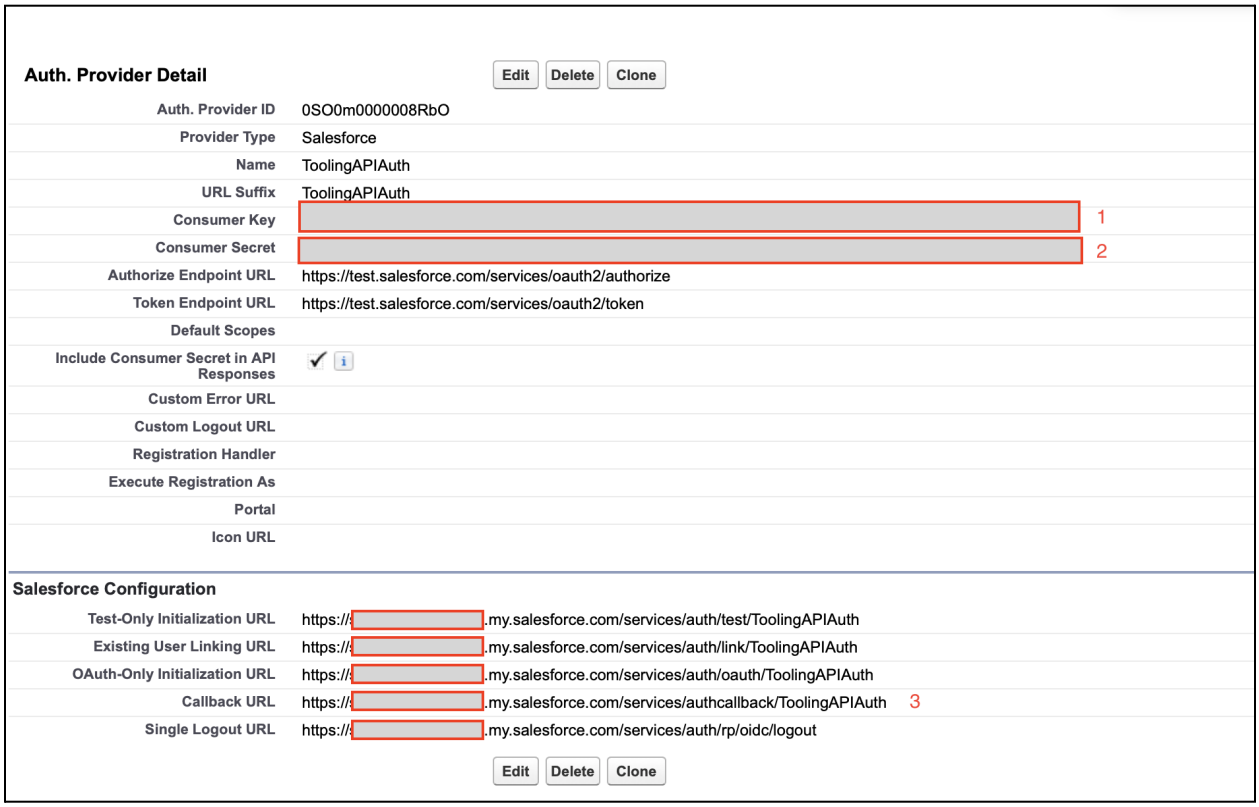
Save the Connected App. After that, Consumer Key and Consumer Secret will be generated for this app.

Once Consumer Key and Consumer Secret is generated, update the Auth provider with the appropriate values

Note - Callback URL is a mandatory parameter to create a Connected App. While creating the connected app first time, it can be marked as "http://localhost" as a placeholder. However, once the auth provider configuration is completed, it will generate the appropriate callback URL that needs to be configured back in the connected app definition. Keep in mind, any change to connected app definition may take up to 10 minutes to reflect. So if you get any error in the authorization step, wait for 10 minutes before retrying it once again to avoid getting repetitive errors of "Invalid Callback URL"

Auth Provider Configuration

Create a Salesforce auth provider as shown below screenshot.



Few key aspects that need to be configured and managed in the later parts of the configuration document.

1 - Consumer Key - This will be **Consumer Key** value from Connected App config

2 - Consumer Secret - This will be **Consumer Secret** value from Connected App config

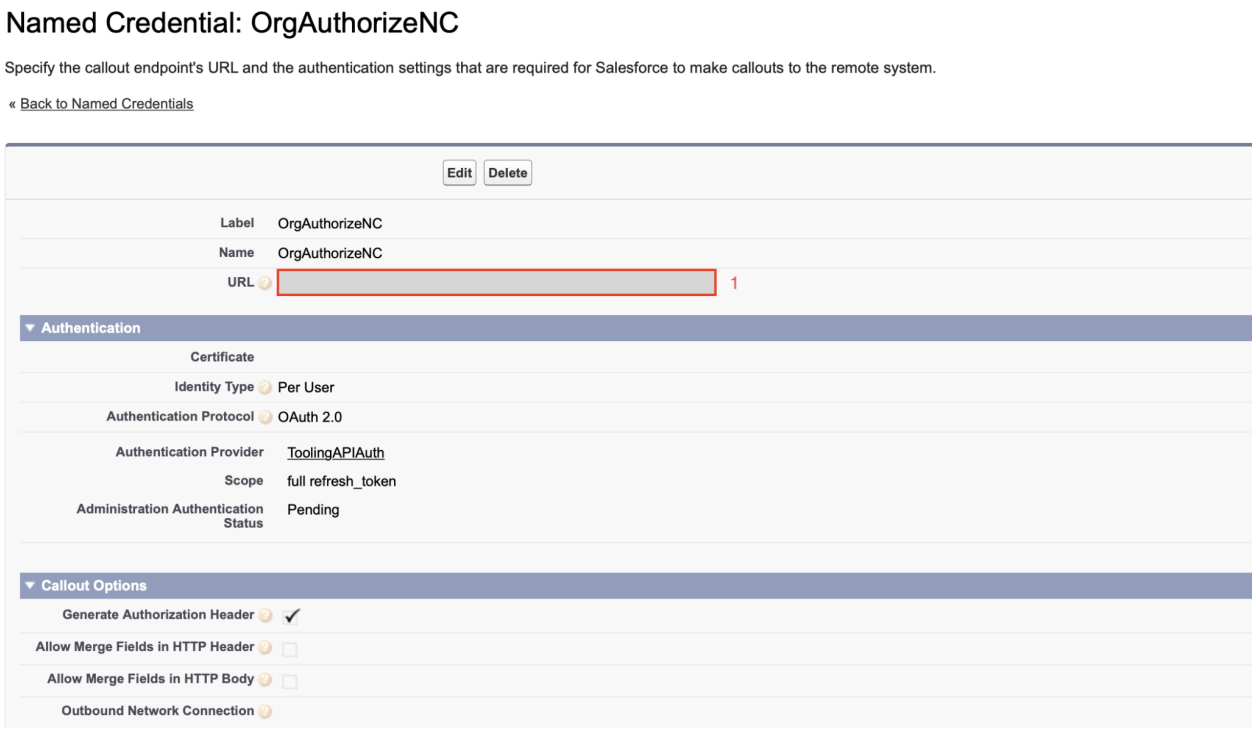
3 - Callback URL - Generated "Callback URL" after saving the Auth Provider will be configured back into the Connected app configuration as "Callback URL" parameter of the connected app.

Note - If you're installing this in Production instance, please configure "Authorize Endpoint URL" and "Token Endpoint URL" to login.salesforce.com domain instead of test.salesforce.com

Once the Callback URL from the auth provider is configured back into connected app configuration, it takes 10 mins to reflect in the connected app definition. Wait till 10 mins after updating the connected app with the callback URL before starting to configure Named Credential.

Named Credential Configuration

Once the connected app is created and Auth provider is configured, next step would be to configure Named Credential. Create a new Named credential should be created as shown in the screenshot below



URL - This is the URL that should be directed to the same sandbox where the security details will be viewed. As an example, if mydomain for the sandbox is "SampleDemoOrg" then the URL would be "https://SampleDemoOrg.my.salesforce.com/services/data/v51.0/"

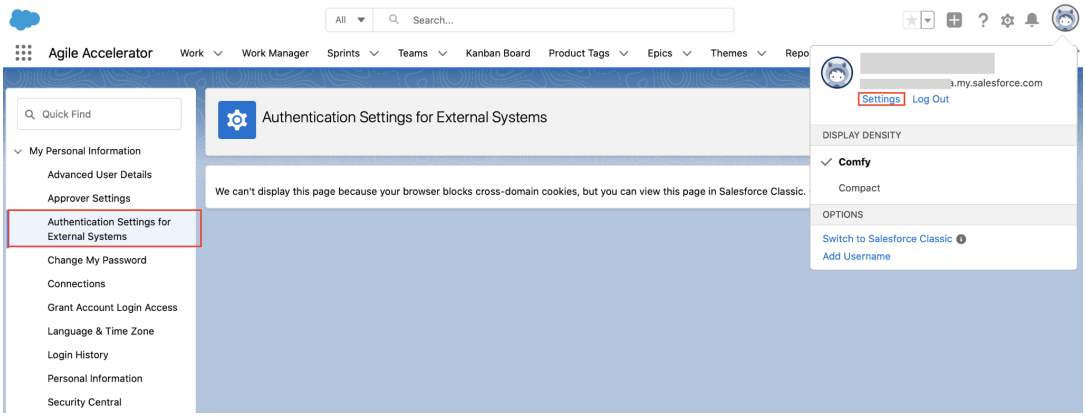
Note - Make sure to use the MyDomain URL with the "my.salesforce.com" and not the "lightning.force.com" domain.

Note - The "scope" field must have the following value: full refresh_token

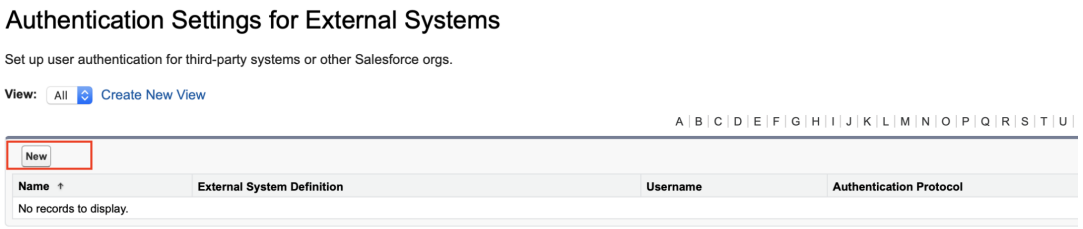
Note - API version in the URL parameter of this configuration can be mentioned as the latest version available

Few notes -

1. Once the “Authentication Protocol” is set as “OAuth 2.0”, “Administration Authentication Status” value will be set as Pending. That is expected
2. After the Named Credential is created, it may take some time for the Connected App to accurately reflect the “CallBack URL”. Because of that authentication may fail initially. Retry after 10-15 minutes and it should give an appropriate response.
3. We recommend setting up “Identity Type” as per user basis so that every user can authorize for themselves to see the data. Depending on the Identity type, authorization flow screen would differ.
    a. If “Identity Type” set as “Per User”
        i. Click on Right hand corner icon on your profile and click on Settings



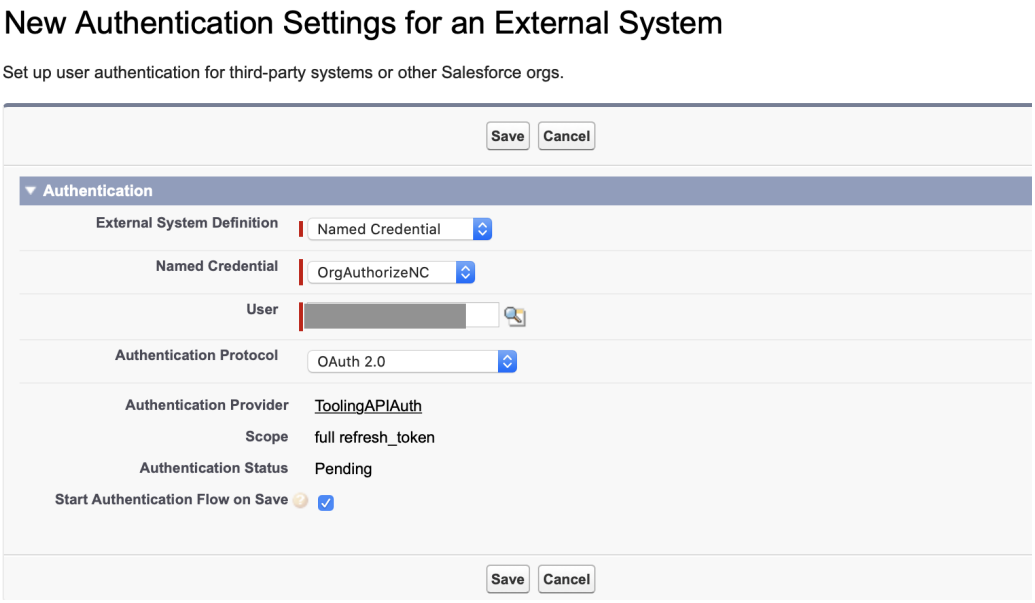
        ii. Click on “Authentication Settings for External Systems”. In the subsequent screen, click on New



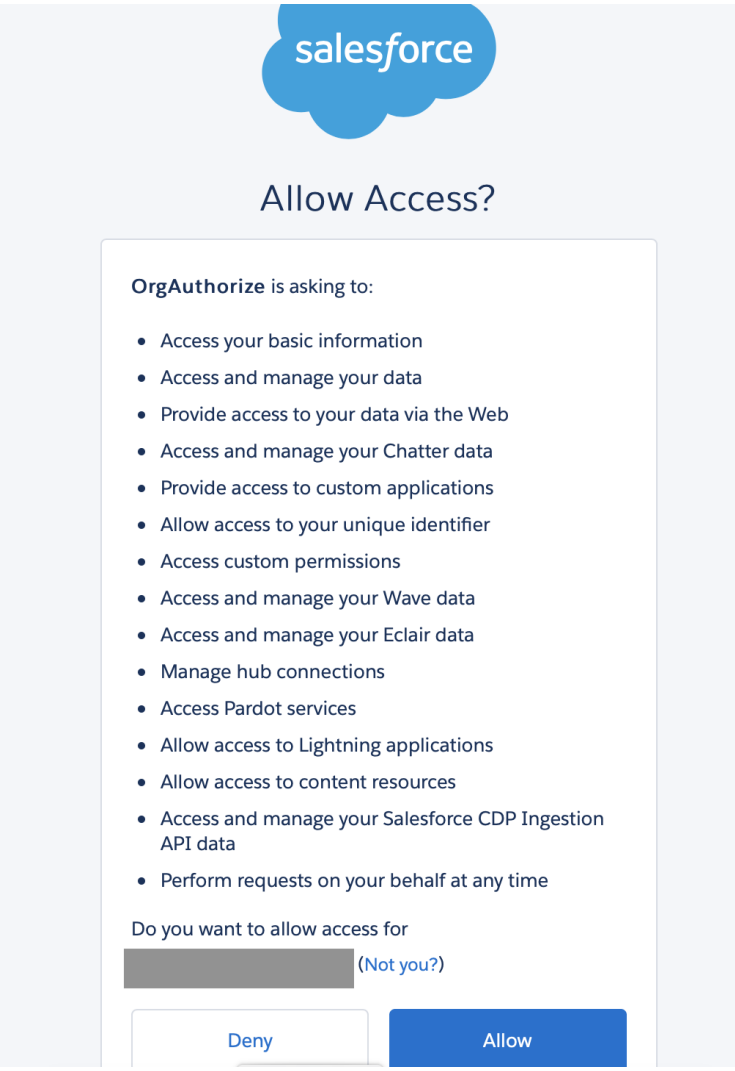
Note - Once you configure the Named Credential with an “Identity Type” of “Per User”, you will see the standard oAuth screen asking “Allow Access?”. Even if you allow access here, you still need to complete the steps noted above by going to your user’s personal settings screen as

described in 3.a above before the system will allow access to the APIs. If not using “Per User”, no need to complete the steps in the user’s personal settings.

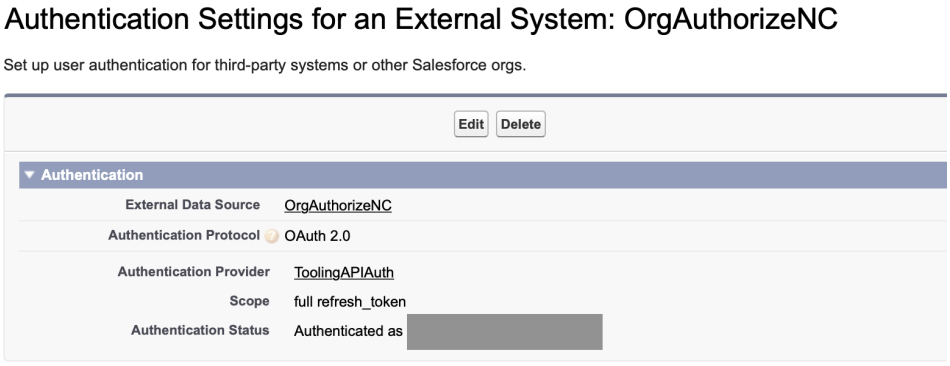
iii. On the subsequent screen, create a new



iv. Click “Save”. This will take you to the login screen. Provide login credentials and then you should see the authorization approval screen

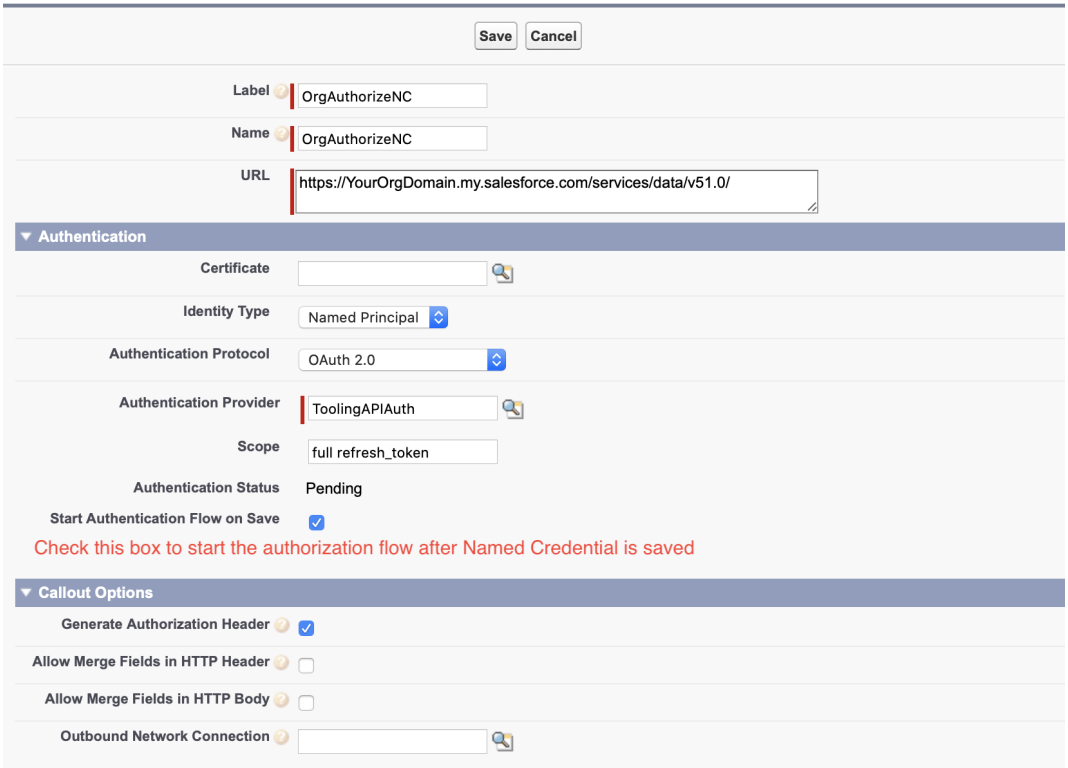


v. Click Allow. That should bring you to the screen showing that the org is now authorized



b. If “Identity Type” is set as “Named Principal”

i. Go to Setup > Name Credential > Create a new Named Credential

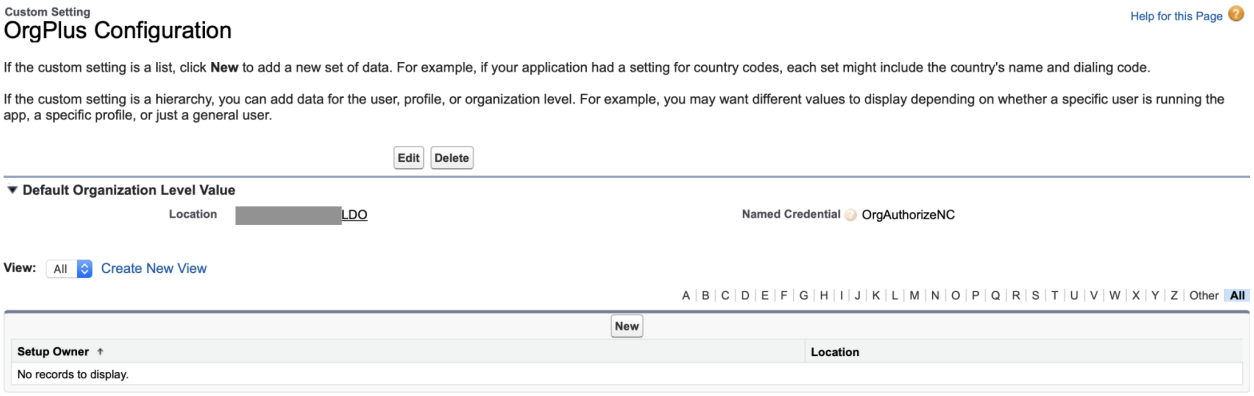


After that, the flow is the same as “Per User” Identity Type configuration. Only difference between “Per User” and “Named Principal” is that in case of “Per User” Identity type requires every user who will use the OrgPlus services to be authenticated individually rather than one user’s access being used for every user who’d use this app.

Custom Setting Configuration

This custom setting “OrgPlus” is installed as part of the managed package. Once the above steps are completed, name of the named credential will have to be added to finish configuration The newly configured name of the Named Credential is to be created as Org Default in “OrgPlus

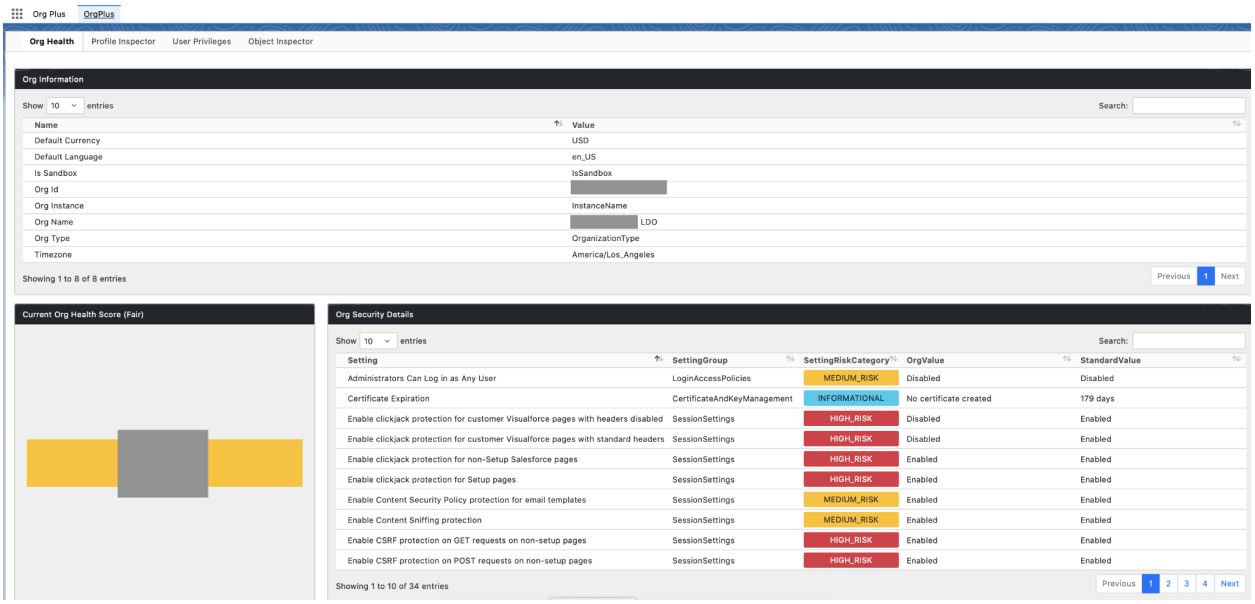
Configuration” hierarchical custom setting as shown in the screen below



While it's possible to set different named credentials for different profiles / users but since we also have the option to use “Per User” name credential, we’d not have to define different Named Credentials for different profiles / individuals.

Configuration verification

Once all configurations are completed, Go to AppLauncher and Open “Org Plus” app. If you’re able to see a view the first tab of Org Plus application with Org Health score displayed



If you see this page, then you have configured Org Plus correctly.

User Guide

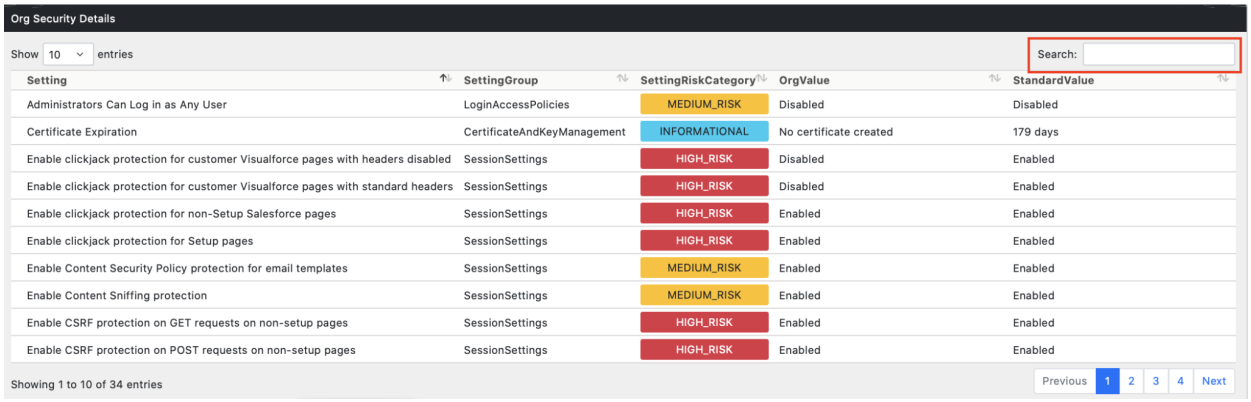
OrgPlus app is created for better visualization of various security controls of the organization. This app has multiple tabs which displays specific information about the security controls. In this guide, we'll walk you through the steps to better utilize this application.

Usability Controls

First, we'll start from the various usability features of this app. These are user intuitive features that help use the app better

Search Boxes

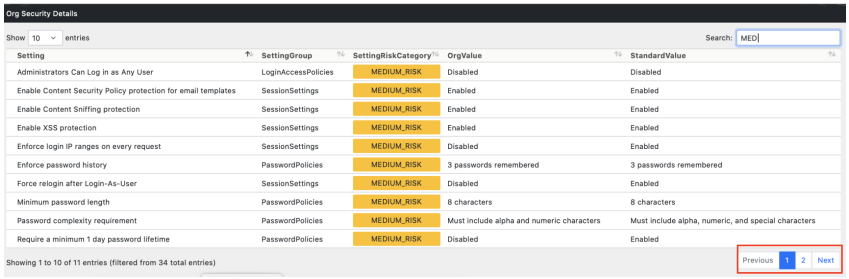
All throughout the app, you can find search boxes. These search boxes will search for any free form text that is displayed on that specific grid.



These search boxes allow free form search. "Enter" key press is not required to search. As and when you type the characters, the table shown below will be filtered to show all matching rows which match the search text in the search box.

Pagination

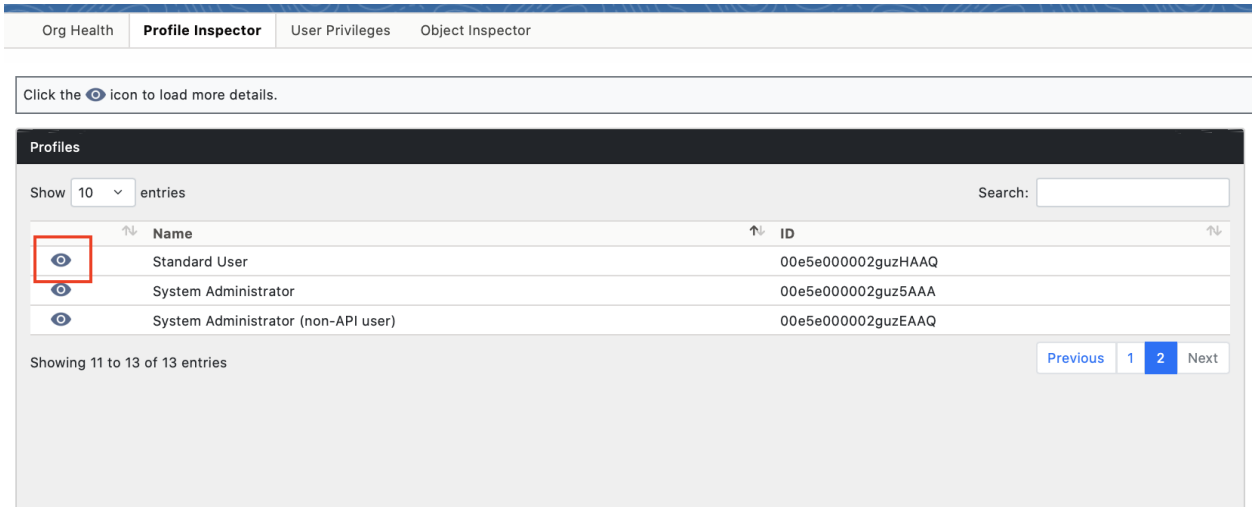
Everyone in the app, you will also find that the grids are paginated. These paginations are at the bottom right hand corner of the grid.



So if you're looking for an element or property and don't find it in the first page, look for that item in the next page of that grid.

Lookup

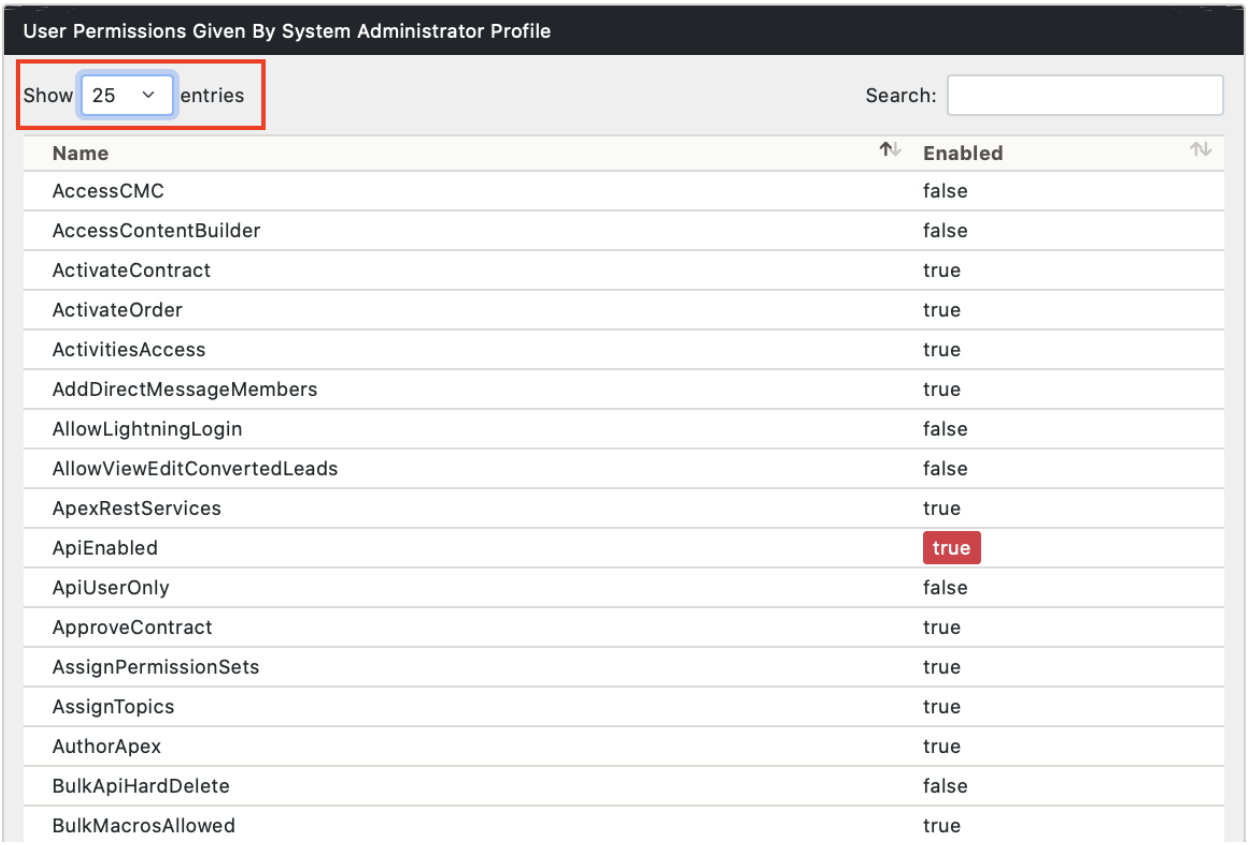
There are some grids which get populated only when the specific profile or User is selected. Use those lookup icons wherever applicable to load more details about the security control you're trying to understand



Clicking on these icons will allow you to get more information on that specific element.

Items per grid

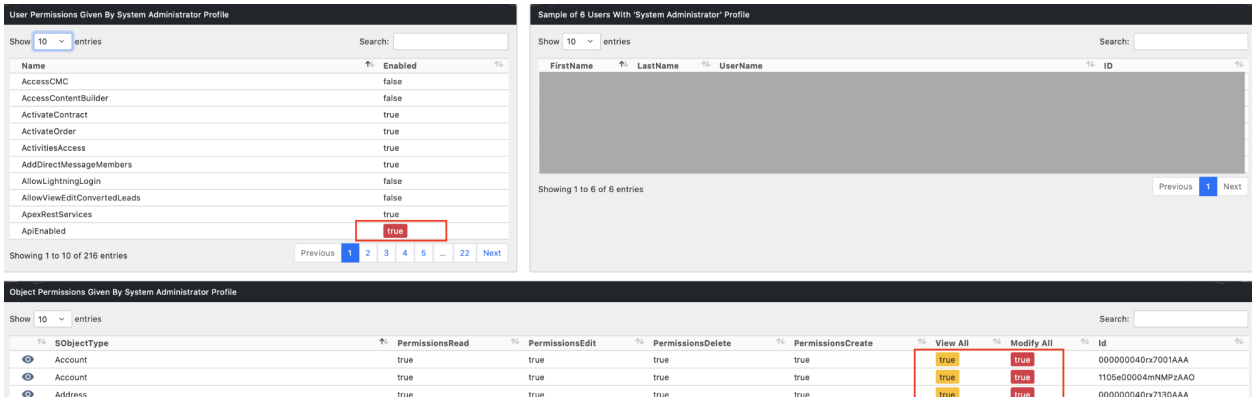
In some of the grids, you'll see an option to select the number of items that can be displayed for that particular grid. This will help you display just the nominal amount of information per your own preference



Adding more items per grid will also elongate the UI. So keep that in mind. You can always revert to the original setting by selecting the desired value from the presets for this control

Color-Coding

Many times, you'd notice that some values are highlighted as "Red", "Amber" or "Blue" in a grid. These represent security risks in a visual way and need to be closely investigated on whether those accesses should be granted. Red denotes high risk and Amber denotes medium risk



This is a visual representation of security risks in the org. These do not necessarily mean that granting those accesses are incorrect / unacceptable in any way. There may be business requirements or in some cases technical requirements (In the case of System Administrator profile) that some controls can't be deactivated and will show up as "Red" and "Amber" in this app. Do not get alarmed by this. Just investigate and take the necessary course of action to rectify, if required, to support your processes and implementations.

Functionality Controls

This app categorizes various security functionalities in 4 major categories. Each category is represented in a tab.

Org Health

This tab represents the overall health of the org. In this tab, following information can be found

- Org Information : High level information about the organization
- Health Score : Org health score from the organization's security health check
- Org Security Details : Various security elements that are configured and pre-set to be checked in the security health check will appear here. Data in this grid is also color-coded based on severity.

Profile Inspector

This tab represents security controls granted by various profiles in the organization. In this tab, following information can be found

- Profiles : Lists the profiles with profileIds. Click on the Lookup icon on each profile to know more details.
- All Profile Highlights : Represents a common use case to see how many profiles grant few specific system permissions like "View All Data", "Modify All Data" and "Api Enabled"
- Profile Highlight : Displays number of users in the profile and two common use cases of objects with "View All" and "Modify All" access. These kind of accesses are considered risky since they override other security and sharing measures implemented in the org.
- User Permissions by Profile : Represents various user / system permissions that are present and the state of access grant in the profile. Some access grants such as "Api Enabled" are color coded
- Sample Users with Selected Profile : On click of lookup icon on a profile, it will bring up some sample users who are granted this profile
- Object Permissions by Profile : State of access grants to various objects in the org by the profile. ViewAll and ModifyAll accesses to any object are color coded. Click on the Lookup icon to view details about object access by the selected profile

- Object Fields : This section is populated only when an object is selected for an already selected profile. This section displays state of FLS for each field in the profile for the selected object

User Privileges

This tab displays user access information across various dimensions of security controls. In this tab, following information can be found

- User Search : Type name of user (Minimum 3 characters) and hit “Search” button to search for a specific user; Alternatively click on “Get All Users” button to list all users
- Users Grid : This grid is populated with results of the User Search action. Click on the Lookup icon to get more details on the user’s access.
- User Permissions : Grid that displays state of various user / system permissions granted to the user because of Profile & PermissionSet assignments
- User Permission Sets : Lists various PermissionSets that are assigned to the user
- Object Permissions : Displays the state of CRUD access for various objects for the user. Use Search Box to filter for specific object if required
- User Record Access Checker : This utility allows you to check a specific record access. UserId would be populated when the lookup icon next to a specific user is selected. Populate the RecordId (18 character Salesforce Id) and click on “Verify Access” button.
- Record Access : This section is populated with the results of the User Record Access Checker to explain record level access to the specific record for the user.

Object Inspector

This tab displays sharing controls in place for an object. Following information can be found for this tab

- Objects : Lists all objects in the organization. Click on the Lookup icon to view various programmatic and configuration related details of the object
- Record Count : Total number of records present for the object in the organization
- Object Limits : Displays various object limits and the utilization of those limits in that object in the organization
- Validation Rules : Lists various validation rules present for the object
- Object Triggers : Lists various triggers present for the object and the trigger event for those triggers.