



Service Manager

Configuration Database (ConfigDB) Guide

2021.4

Copyright Notice

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2021, Ivanti. All rights reserved.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Protected by patents, see <https://www.ivanti.com/patents>.

Last updated: 2/1/2022

Contents

Copyright Notice	2
About this Guide	5
Using the Service and Asset Manager Configuration Database (ConfigDB)	5
Intended Audience	5
Document Organization	5
Related Documentation	6
How to Contact Us	6
About Logging into the Configuration Database	7
Workspaces that Already Exist	8
Internal Use Only Workspaces	9
Workspaces Populated by the System Configuration Wizard	10
Central Config API Authentication	11
Install/upgrade Ivanti Service Manager System Configuration Wizard	11
Disabling the Centralconfig API Key Feature	12
Impacted webconfig file list:	12

Custom Installation of SCW	13
Setting up the Teams Bot Integration	15
What the Powershell Script does?	15
Setting up the Central Config API Key	15
Executing the PowerShell Script	16
Troubleshooting	16
Workspaces that Can Be Used	18
Configuring the Message Queue	18
Configuring the Message Queue Handler	18
Configuring Email	19
Viewing All Logs	20
Setting the Log Level	20
Viewing the Logs	20
Working With Customer Contacts	21
About this Workspace	21
Viewing Customer Contacts	21
Adding a Customer Contact	22
Editing a Customer Contact	22
Deleting a Customer Contact	22
Working With Tenants	23
About the Tenants Workspace	23
Resetting the Cache for a Tenant	23
Adding a Certificate to a Tenant	24
Capturing Discovery Messages for Debugging	24
Configuring Attachment Options	25
Setting Production Metadata to Read-Only	25
Setting the Login URL	26

Setting the Alternate Login URL (Vanity URL) for an MSP	26
Configuring Manual Load Partitioning	26
About Manual Load Partitioning	27
Configuring the Workflow Service Configuration File	28
Assigning Tenants to the Workflow or Email Service	28
Viewing the Results of the Manual Load Partitioning	29
Setting the Log Level for the Workflow or Email Service	29
Viewing the Workflow or Email Manual Load Partitioning	29
Viewing a Report of the Manual Load Partitioning	30
Firestore Configuration for Mobile Push Notification	32
Creating a new Project in Firestore	32
Configure iOS and Android app in Firestore.	34
Apply iOS Certificate for iOS app	41
Configure Firestore in Config Database of ISM	46

About this Guide

"Using the Service and Asset Manager Configuration Database (ConfigDB)" below

"Intended Audience" below

"Document Organization" below

"Related Documentation" on the next page

"How to Contact Us" on the next page

Using the Service and Asset Manager Configuration Database (ConfigDB)

Use the Service and Asset Manager configuration database (ConfigDB) for the following:

To manage different instances (such as production, staging, and UAT) of tenants.

To update your environment. The information in the ConfigDB is originally populated by the System Configuration Wizard, which is used when installing Service and Asset Manager.

This is the master configuration database for your Service and Asset Manager system. Do not make any changes here, except in the few areas described in the 'Workspaces that Can Be Used' section. Making unauthorized changes to the ConfigDB can lead to disastrous results and may be unrecoverable. Use the ConfigDB with extreme caution.

Intended Audience

The Configuration Database Guide for Service and Asset Manager Version 2021.4 is intended for advanced on-premise Service and Asset Manager administrators and Ivanti Software personnel.

Document Organization

This guide lists the workspaces in the ConfigDB and what, if any, tasks can be performed. This document contains the following sections:

Information about logging in. See "About Logging into the Configuration Database" on page 7.

Workspaces that are also available in the Service and Asset Manager Service Desk Console or the Service and Asset Manager Configuration Console. See "Workspaces that Already Exist" on page 8.

Workspaces that are for internal use only. See "Internal Use Only Workspaces" on page 9.

Workspaces that are populated by the System Configuration Wizard. Do not make any changes to these workspaces. See "Workspaces Populated by the System Configuration Wizard" on page 10.

Workspaces where you may make changes. See "Workspaces that Can Be Used" on page 18.

Related Documentation

Ivanti Service Manager has online help available within the application.

Additional documentation is available through

The [Ivanti community](#) website. You may need to request user access if you cannot log in.

Or through

The [Ivanti Product Documentation](#) website. Click the Service Manager tile to see a list of the documents available.

How to Contact Us

To contact us about the documentation, or if you have any other questions or issues about Service and Asset Manager, contact Ivanti Global Support services by logging an incident via Self Service at: <https://www.ivanti.com/support/ivanti-support>.

About Logging into the Configuration Database

To use the Service and Asset Manager configuration database (called ConfigDB), you must log in first. Only administrators can log into the ConfigDB.

By default, the system displays a drop-down menu allowing you to choose either ConfigDB (the Service and Asset Manager configuration database) or ISM (the Service and Asset Manager application database).

Logging in to the ConfigDB

Ivanti'. Further down, it says 'Copyright © 2005-2017 Ivanti. All rights reserved.' and provides links for 'Privacy Policy' and 'Legal Terms and Notices'." data-bbox="115 316 670 439"/>

If you do not see the Application drop-down menu, you must configure Service and Asset Manager to show it. For instructions on doing this, see the "Logging into Service and Asset Manager" section of the Installation and Deployment Guide for Service and Asset Manager .

Workspaces that Already Exist

The following workspaces found in the ConfigDB also exist in the Service and Asset Manager Console or the Service and Asset Manager Configuration Console. Therefore, they are not described in this document. For information about these workspaces, see the Service and Asset Manager online help within the application as well as at the Ivanti Product Documentation website. Click the "Service Manager" tile to see a list of the documents available.

Employee

All Logs

Logging Configuration

Notification

Patch Log

Encryption Key

FRS Application Update Notes

Ivanti Release Package

Ivanti Release Project

Ivanti Transaction Detail

Ivanti Transaction Set

Logon History

Public Key

Schedule Entry

WS Mapping

WS Proxy

Internal Use Only Workspaces

The following workspaces in the ConfigDB contain information that you can view, but that you should never change. These workspaces are only used by Ivanti for internal system use.

Do not change the values in any of these workspaces! Changing any values can lead to system degradation.

CMDB Import History

Feature Management

IM Client Agent Version

Installer Types

Logging Server Configuration

Modules

Remote Host Blocked List

Service Names

User Feature Settings

Workspaces Populated by the System Configuration Wizard

The following workspaces found in the ConfigDB contain information that was populated based on information entered in the System Configuration Wizard when Service and Asset Manager was installed.

We recommend that you do not change any of the values in these workspaces.

For complete information about the System Configuration Wizard and the Service and Asset Manager installation, see the Installation and Deployment Guide for Service and Asset Manager Version 2021.4

Database Servers

Log Operations Locations

Integration Services Configuration

Metrics Server

Report Server

Survey Information

Trusted IP Addresses

Web Servers

Central Config API Authentication

APIs in the Central Config can be accessed only by known users by authenticating the API call. The API Header will pass the API Key which will be authenticated and passed by the Central Config server. This prevents un-authorised users from accessing the APIs.

Install/upgrade Ivanti Service Manager System Configuration Wizard

On installing or upgrading the Service Manager System Configuration Wizard, the API Key is auto-generated in the Central Config DB. This key is used to to authenticate the API calls to the Central Config Server. However, the following should be monitored while installing/upgrading.

Verify the webconfig file

Once the installation/upgradation is complete, verify the webconfig file has the following:

In the config section:

```
<section name="CentralConfigApiKey" type="System.Configuration.NameValueSectionHandler" />
```

In the new protected section:

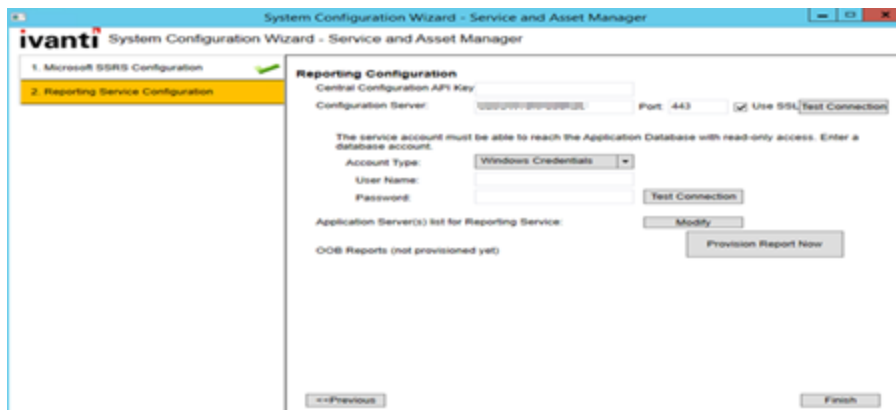
```
<CentralConfigApiKey> <add key="CentralConfigApiKey" value="" /> </CentralConfigApiKey>
```

Update for Teams Bot Service

If you have installed Teams Bot Service, update the CentralConfigApiKey value in appsetting file. from `C:\inetpub\TeamBotService\appsettings.json`. Get the CentralConfigApiKey from the Central Config DB table (Frs_data_api_key).

Updates if Service Manager System Configuration Wizard and Service Manager Reporting Wizard are installed on different machines

If the Service Manager System Configuration Wizard and Service Manager Reporting Wizard are installed on different machines, update the Centralconfig api key when installing the Reporting Wizard as shown in the below image. Get the CentralConfigApiKey from the Central Config DB table (Frs_data_api_key).



Updating the CentralConfigAPIKey

In case you wish to update/change the CentralConfigAPIKey, do so by following the below steps:

Stop all services that are referencing the centralconfig.

Log in to Service Manager with Admin credentials and open the Configuration console.

Select Security Controls > CentralCofigAPIKeyGroup and note down the description .

Delete the existing CentralConfigAPIKey and recreate a new key inside the CentralConfigAPIKeyGroup as shown in the below image.

Configure :: Security Controls :: API Keys:: New API Key

Reference ID: **2583A758AF-424DB-4B1F689966DACC25A6**

☒ Activated

Description: CentralConfigApiKey

On Behalf Of: Not Set

In Role: Not Set

Not limited by IPs from which it can be used

[Add New IP](#) [Save Key](#) [Back](#)

Once the Key is created in the CentralConfig tenants, re-run the System Configuration Wizard to update the webconfig and appconfig files.

Restart your machine.

The CentralConfigAPIKey should be unique, duplicate/multiple keys will break the feature.

Disabling the Centralconfig API Key Feature

Log in to the application with Admin credentials and open the Configuration console.

Select Security Controls > API Key and delete the CentralConfigAPIKey.

Ensure you Delete and not De-activate to disable.

Impacted webconfig file list:

AppDomains	Configuration Files
AppServer	Web.config
WorkFlow	WorkflowService.exe.config

Excalation	EscalationService.exe.config
email	EmailWindowsServiceapp.exe.config
bulkupload	KMBulkUploadTool.exe.config
integrationserver	IntegrationServiceHost.exe.config
systemconfigwizard	ServerConfigurationWizard.exe.config
release tool	ReleaseTool.exe.config
Frsloggingservice	FRSLoggingService.exe.config
metric	HEAT.MetricsServer.exe.config
message queue	MessageQueueServiceHost.exe.config
License service	LicenseServerWindowsService.exe.config
report provinising	reportserver\ReportProvisioning.exe.config
Neurons	appsettings
Teams Bot Service	appsettings
DynamicWebServices	web.config
OpsConsole	web.config
FrsSurvey	web.config
FrsSurveyProxy	web.config
IM	IMServer\IMServices\AssetProcessor\Web.config
IM	IMServer\IMServices\DiscoProcessor\Web.config
IM	IMServer\IMServices\DiscoUtils\Web.config
IM	IMServer\IMServices\IMReadOnlyDataService\Web.config
IM	IMServer\IMServices\TaskProcessor\Web.config
IM	IMServer\WebServices\ClientTransportProcessor\Web.config
reports	C:\Program Files\Microsoft SQL Server\MSRS12.MSSQLSERVER\Reporting Services \ReportServer\Web.config

Custom Installation of SCW

When customers try to install the Configuration Server in one machine and other components in another machine, user has to copy the Central Config API Key from Configuration Server and update the key in the Central Configuration Settings page as show in the following image.

Sample image of Custom Installation of SCW

System Configuration Wizard - Service and Asset Manager

ivanti

System Configuration Wizard - Service and Asset Manager

1. Central Configuration API Key Settings

2. Application Server Settings

3. Other Feature Settings

4. Metrics Server

5. Discovery Application Server

6. Discovery Web Server

Central Configuration API Key Settings

Central Configuration API Key

Note: You can retrieve the API Key from Central Configuration Server Settings

Next>>

Setting up the Teams Bot Integration

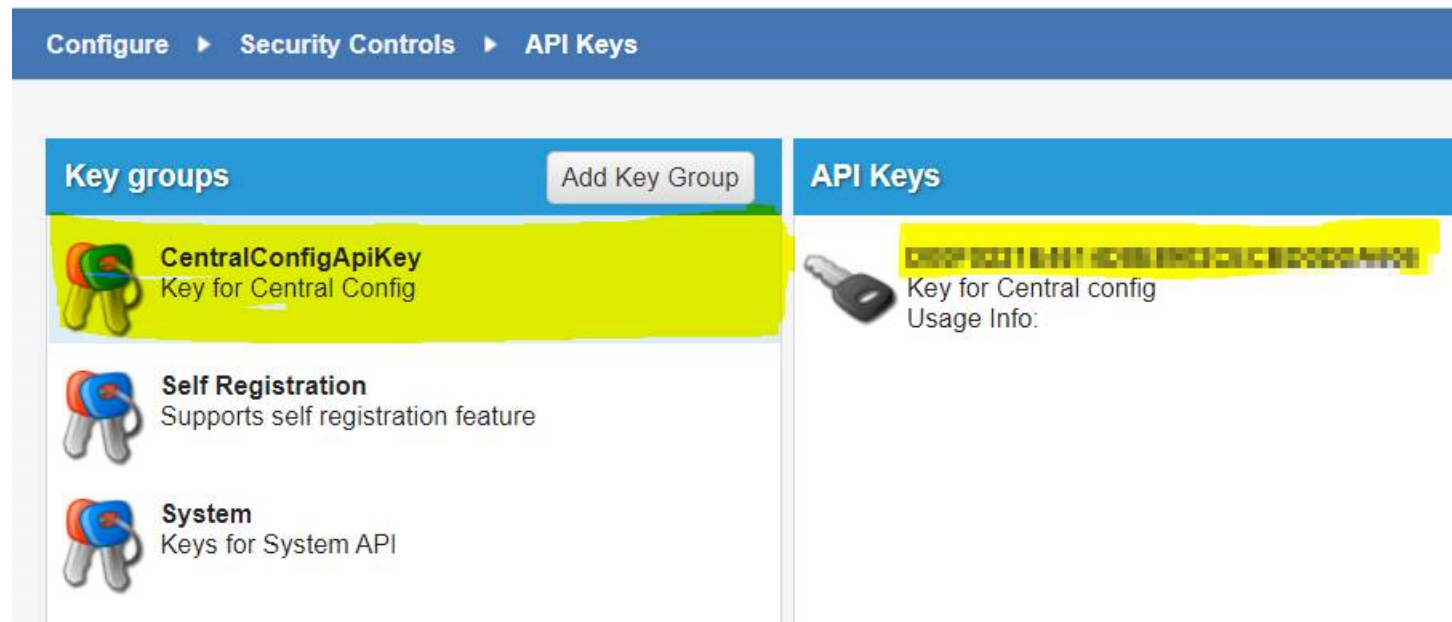
For integrating Microsoft Teams with Ivanti Service Manager, on-premise users should first setup the environment by downloading the package from [Ivanti MarketPlace](#) and executing PowerShell script.

What the Powershell Script does?

- Creates the directory in the inetpub folder.
- Creates a new application pool and sets item property for it.
- Creates a new web application and sets item property for it.
- Silently installs the required application, as in you might not get any prompts to proceed with the installation.
- Copies the required binaries to the destination folder.
- Creates the appsetting.json once the ipaddress/machine name/local host name is provided.

Setting up the Central Config API Key

- 1.Log in to the CentralConfig > Configure Application > Security Controls > ApiKeys.
- 2.Find the CentralConfigApiKey as shown below and copy the value.



- 3.Paste the copied value in the appsettings.json file for the CentralConfigApiKey. For example, CentralConfigApiKey="xx"

Executing the PowerShell Script

- 1.Download the zip file to a relevant folder in your machine.
- 2.Extract the zip file.
- 3.Open PowerShell as Administrator.
- 4.Go to the location where the PowerShell script is located, that is, the location where you extracted the zip file.
- 5.Run the script - `.\TeamsBot.ps1`.
- 6.You will be prompted for the Appserver as well as the Central Config ipaddress/ Machine name/ localhost name. Enter the appropriate Address/Machine name/localhost.

The configuration is done.

Troubleshooting

Incorrect ipaddress/machine name/local host name

If you provide incorrect IP address/machine name/local host name, open the Appsetting.json file from the folder intepub >Teams Bot Service and replace the AppserverIPAddress with the correct one.

Example of the AppSetting.json file:

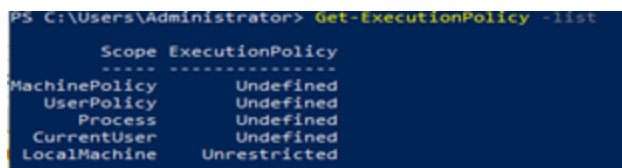
```
{ "MicrosoftAppId" = ""; "MicrosoftAppPassword" = ""; "IPCMURL" = "http://$Appserver-
IPAddress/HEAT/ServiceApi/IPCService.asmx"; "WorkflowURL" = "http://$Appserver-
IPAddress/HEAT/ServiceApi/WorkflowService.asmx"; "ConfigURL" =
"http://$CentralConfigIPAddress/CentralConfig/ConfigServiceAPI.asmx"; "RetrieveTenantLogLevel_ws_
url" = "http://$CentralConfigIPAddress/CentralConfig/RetrieveTenantLogLevel.ashx"; "EnableCen-
tralLogging" = false; "LoggingService_ws_url" = "http://$Appserver-
IPAddress/Heat.Logging.Service/api/LoggingService/HeatServiceManagementLogging";
"ElapsedSecondsToFlushLog" = 60; "ItemSizeToFlushLog" = 1000; "LogSettingCacheTimeoutInMinutes" =
5; "SendLogFileLocation" = "C:\logs"; "WriteLogFileLocation" = "C:\logs"; "SendLogWaitInterval" = 300;
"WriteLogWaitInterval" = 300; "EnableLogging" = true; "CacheTimeout" = "30"; "isOnPremise": false; "Cen-
tralConfigApiKey" = "" }
```

Make sure that Boolean values (true/false) don't not have double quotes.

To know the execution policy list

Run the command - `PS C:\Users\Administrator>Get-ExecutionPolicy - List`

Sample image of the policy list



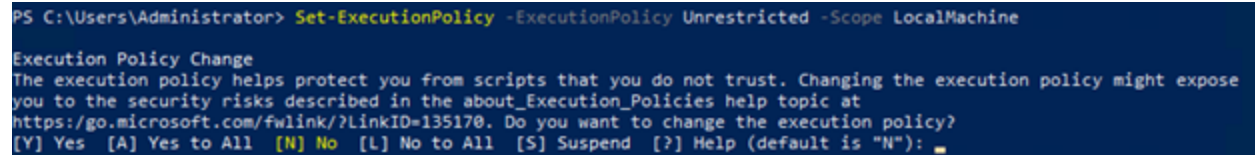
```
PS C:\Users\Administrator> Get-ExecutionPolicy -list

Scope ExecutionPolicy
-----
MachinePolicy Undefined
UserPolicy Undefined
Process Undefined
CurrentUser Undefined
LocalMachine Unrestricted
```


To set the execution policy

Once the PowerShell script is executed successfully, execute the command - `Set-ExecutionPolicy -ExecutionPolicy "PROVIDE PREVIOUS VALUE" -Scope LocalMachine` to set the execution policy.

Sample image of setting execution policy



```
PS C:\Users\Administrator> Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope LocalMachine

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): 
```

Workspaces that Can Be Used

There are very few workspaces in the ConfigDB that can be used by administrators. See the following topics for information:

"Configuring the Message Queue" below

"Configuring the Message Queue Handler" below

"Configuring Email" on the next page

"Viewing All Logs" on page 20

"Working With Customer Contacts" on page 21

"Working With Tenants" on page 23

"Configuring Manual Load Partitioning" on page 26

Configuring the Message Queue

Use the Message Queue Configuration workspace to create and configure a message queue.

Follow these steps:

Log in to the ConfigDB.

From the workspace selector bar, select Message Queue Configuration. The system displays the Message Queue Configuration workspace.

Enter information into the fields.

Parameter	Description
Polling Interval (sec)	Specifies how often to check the message queue. The default value is 120.
Processor Threads	Specifies the number of threads. The value depends on the specifications (such as memory and CPU) of your system. The default value is 250.
Metadata Refresh Interval (min)	Specifies the interval for which to refresh the metadata pertaining to the tenant, which is the amount of time for which to retain the cache. After this amount of time, the system purges the cache and reloads it. The default value is 10.

Click Save.

Configuring the Message Queue Handler

Use the Message Queue Handler workspace to configure the message queue handler.

Follow these steps:

Log in to the ConfigDB.

From the workspace selector bar, select Message Queue Handler. The system displays the Message Queue Handler workspace.

Enter information into the fields.

Parameter	Description
Name	Name of the message queue handler web service.
Endpoint	The URL of the message queue handler web service to which queued tasks are dispatched. An example is <code>http://IP_address/IntegrationService.svc</code> .
Dispatch Method	The name of the web method that is implemented as part of the handler web service (which the message queue invokes to dispatch tasks). For example, the Service and Asset Manager XSLT email handler implements a web method called <code>HandleMessage</code> . NOTE: The name of the dispatch web method is case sensitive.
Batch Size	The maximum number of tasks that the message queue can dispatch to a message queue handler.
Active	Specifies if the message queue handler is on or off.
Priority	Specifies the order of this handler, in relation to any other handlers that are defined.
Process Timeout Interval (minutes)	Amount of time to wait for a response from the message queue handler before logging an error or before retrying, if you have not exceeded the number of attempts specified by the Max number of attempts parameter.
Include Data with Dispatch	Specifies whether to include the data when this dispatch web method is called. If you do not check this option, the message queue handler must call the dispatch web method to get the data.
Max number of Attempts	The maximum number of times to resend the data before logging an error.
Archive on Completion	Specifies whether to archive the message queue journal, which contains the tasks that the message queue handler has processed. Use this information for troubleshooting purposes. Enabled by default.
Purge Archive after (days)	Set to 30 days by default. The amount of days after which the archive is purged.
Description	A description of the message queue handler.

Click Save.

Configuring Email

Use the Email Configuration workspace to configure the inboxes for email.

Follow these steps:

Log in to the ConfigDB.

From the workspace selector bar, select Email Configuration. The system displays the Service Provider Email Configuration workspace.

Enter information into the fields.

Field	Description
Message Queue Handler Name	The name of the message queue handler to use. This must be the same name entered in the Name field in the Message Queue Handler workspace. See "Configuring the Message Queue Handler" on page 18.
Mailbox Poll Interval	The amount of time, in seconds, after which email configuration changes take affect.

Click Save.

Viewing All Logs

If there are any problems with the ConfigDB, such as email issues or workflow errors, they are reported in the logs. Review the logs to determine the underlying issue and to help resolve it.

"Setting the Log Level" below

"Viewing the Logs" below

Setting the Log Level

You can set the amount and detail of information in the logs by adjusting the Log Level. You can do this by going to the **Logging Configuration** workspace. See the Service and Asset Manager Online Help.

Viewing the Logs

Follow these steps to view all of the logs associated with the ConfigDB:

Log in to the ConfigDB.

From the workspace selector bar, select All Logs. The system displays the LogsAll workspace with the following information:

Field	Description
Log Entry Id	A unique ID for this log entry.
Log Time	The time at which the log entry was originally created on the server.
Log DB Time	The time when the log was uploaded into the database.
Client	The IP address of the service that generated the log, such as the workflow server.

Field	Description
IP Address	
SubSystem Id	The subsystem of the service that generated the log. (Each module has predefined subsystems. For example, for the email server, polling is a subsystem.)
Login Id	The login ID for the user who experienced the log event.
Tenant Id	The tenant instance that is experiencing the log event.
Error Code	The category of the error. An example is "trigger not found".
Current Role	The role assigned to the user if the error is generated by a user. If the error is generated by the system, this field is empty.
Host Name	The machine that is reporting the error.
Thread Name	Internal thread ID. Not applicable.

Double-click any log entry to view the log details.

To refresh the data, click Refresh.

Working With Customer Contacts

This section contains the following topics:

"About this Workspace" below

"Viewing Customer Contacts" below

"Adding a Customer Contact" on the next page

"Editing a Customer Contact" on the next page

"Deleting a Customer Contact" on the next page

About this Workspace

This workspace is for deployments with multi-tenant configurations.

You can add, edit, or delete a primary contact for a particular tenant. This is the person you contact for all communications regarding the particular tenant.

This information is also listed in the Account Information workspace in the Service and Asset Manager Configuration Console.

Viewing Customer Contacts

Follow these steps to view information associated with customer contacts:

Log in to the ConfigDB.

From the workspace selector bar, select Customer Contacts. The system displays the Contacts workspace with the following information:

Field	Description
Login ID	The login ID for the customer contact.
Full Name	The full name of the customer contact.
Primary Email	The primary email address for the customer contact.
Primary Phone	The primary phone number for the customer contact.

Double-click any entry to view the details.

To refresh the data, click the refresh icon.

Adding a Customer Contact

Log in to the ConfigDB.

From the workspace selector bar, select Customer Contacts. The system displays the Contacts workspace.

Click New Contacts. The system displays the Contacts page.

Enter information into the fields.

Click Save.

Editing a Customer Contact

Log in to the ConfigDB.

From the workspace selector bar, select Customer Contacts. The system displays the Contacts workspace.

Double-click the entry to edit.

Change the entry.

Click Save.

Deleting a Customer Contact

Log in to the ConfigDB.

From the workspace selector bar, select Customer Contacts. The system displays the Contacts workspace.

Highlight the entry to delete.

If there are dependencies on other items, the system display a confirmation message. Click Continue.

Working With Tenants

"About the Tenants Workspace" below

"Resetting the Cache for a Tenant" below

"Adding a Certificate to a Tenant" on the next page

"Capturing Discovery Messages for Debugging" on the next page

"Configuring Attachment Options" on page 25

"Setting Production Metadata to Read-Only" on page 25

"Setting the Login URL" on page 26

"Setting the Alternate Login URL (Vanity URL) for an MSP" on page 26

"Working With Tenants" above

About the Tenants Workspace

The information on this page is populated by the System Configuration Wizard.

Although there is a lot of information in this workspace, you should only do the following tasks from within this workspace:

Reset the cache for a tenant. See "Resetting the Cache for a Tenant" below.

Add a certificate. If you want to use SAML authentication, you must upload a certificate and password so that end users can download it. See "Adding a Certificate to a Tenant" on the next page.

Capture audit files from ISM Discovery, to help with troubleshooting. See "Capturing Discovery Messages for Debugging" on the next page.

Configure how users attach files. See "Configuring Attachment Options" on page 25.

Set metadata to read-only. See "Setting Production Metadata to Read-Only" on page 25.

Set the login URL. See "Setting the Login URL" on page 26.

Resetting the Cache for a Tenant

Service and Asset Manager caches information about each tenant in the ConfigDB. Because of this, changes to the tenant, such as updating the status, database information, and so on, are not immediately reflected in the corresponding tenant. This can lead to situations where Service and Asset

Manager allows a user to log into a tenant, even though the status of the corresponding tenant in the ConfigDB is set to closed.

To manually reset the cache for a specific tenant, do the following:

Log in to the ConfigDB.

From the workspace selector bar, select Tenants. The system displays the Tenants workspace.

Highlight the tenant to reset the cache for.

Click Reset Tenant Cache.

Adding a Certificate to a Tenant

If your implementation includes multiple tenants, the certificate should be for the domain and not the specific tenant. For example, the certificate for Cloud tenants is for *.saasit.com, not for a specific tenant such as mytenant.saasit.com.

Log in to the ConfigDB.

From the workspace selector bar, select Tenants. The system displays the Tenants workspace.

Double-click the tenant for which to add a certificate.

Click Add Certificate.

Navigate to the certificate location. Highlight it and click Open.

Enter the password for the certificate in the Certificate Password field.

Click Save.

Capturing Discovery Messages for Debugging

Perform the following procedure if you are using Discovery and you need to capture the audit files sent to the server from the Discovery client agents. After you capture the audit files, you can review them in a debug environment to find out more details about the problem. The logging can be very long, so be careful about using this feature. For more information, see the Service and Asset Manager online help.

Log in to the ConfigDB.

From the workspace selector bar, select Tenants. The system displays the Tenants workspace.

Double-click the tenant to configure logging for.

Check Log Failed IM Message.

Click Save.

Configuring Attachment Options

Perform the following procedure to configure how attachments are saved. You may need to change the format for storing files if users regularly store very large files, such as system log files. After you configure this, when a user saves an attachment to a record, the attachment is stored in the location that you specified here. For information about saving attachments as a file stream, see <https://msdn.microsoft.com/en-us/library/gg471497.aspx>.

We recommend that for system data, such as icons and images, you select Database for the Attachment Save Type field.

Log in to the ConfigDB.

From the workspace selector bar, select Tenants. The system displays the Tenants workspace.

Double-click the tenant for which to configure attachment options.

For the Attachment Save Type field, select a type: **Database**, **FILESTREAM**, **File system**, Amazon S3, or Azure Blob.

For the Attachment Path field, enter the default path where attachments are saved.

Click Save.

Setting Production Metadata to Read-Only

If a user makes a change to the metadata in the production instance of the tenant, such as when configuring a workflow for a request offering, but does not make the same change in the UAT or staging instance of the tenant and then pushes the data from the UAT or Staging instance of the tenant to the production instance of the tenant, the data becomes corrupt and the workflow fails.

To avoid this, set the metadata on the production instance of the tenant to read-only. Follow these steps:

Log in to the ConfigDB.

From the workspace selector bar, select Tenants. The system displays the Tenants workspace.

Double-click the tenant for which to set the production metadata to read-only.

Check **Is Production Metadata Read-only**.

Click Save.

If a user tries to edit the workflow for a request offering, the system displays a message stating that the production metadata is read only and cannot be edited. See "Working with Request Offerings" in the Service and Asset Manager online help for more information.

Setting the Login URL

Set the login URL in the following scenarios:

When configuring Service and Asset Manager Active Directory authentication using Windows Integrated Security (WIS). This feature allows users to access Service and Asset Manager without entering their user name and password. This procedure is only valid for the on-premises version of Service and Asset Manager.

When configuring the Service and Asset Manager on-premises URL for mobile users.

Follow these steps:

Log in to the ConfigDB.

From the workspace selector bar, select Tenants. The system displays the Tenants workspace.

Double-click the tenant for which to set the login URL.

In the Login Url field, enter the URL where users go to log in.

Click Save.

Setting the Alternate Login URL (Vanity URL) for an MSP

Besides setting the login URL as described above, you can also specify an alternate login URL, also known as a vanity URL, for a Managed Service Provider (MSP).

Follow these steps:

Log in to the ConfigDB.

From the workspace selector bar, select Tenants. The system displays the Tenants workspace.

Double-click the tenant for which to set the alternate login URL (vanity URL).

At the bottom, click the Alternate Login URL tab.

Click New TenantUrlAlias. The system displays the New TenantUrlAlias dialog box.

In the Url field, enter the alternate login URL (vanity URL).

Click Save.

Configuring Manual Load Partitioning

"About Manual Load Partitioning" on the next page

"Configuring the Workflow Service Configuration File" on page 28

"Assigning Tenants to the Workflow or Email Service" on the next page

"Viewing the Results of the Manual Load Partitioning" on page 29

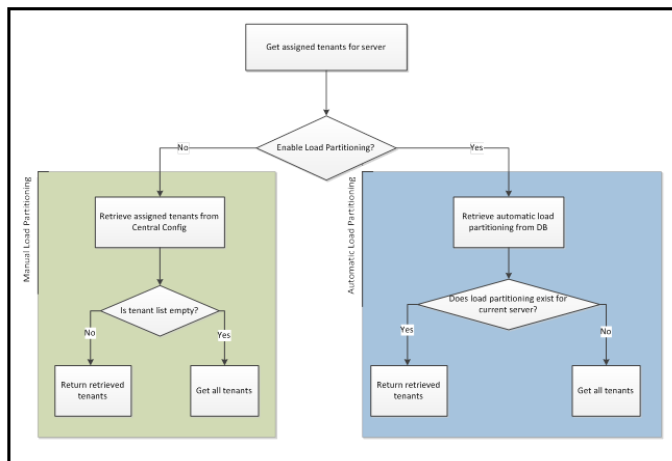
About Manual Load Partitioning

Use the Service Server workspace to configure the manual load partitioning feature. The manual load partitioning feature allows you to allocate the load between workflow or email service instances based on your knowledge of the tenant load and server capacity.

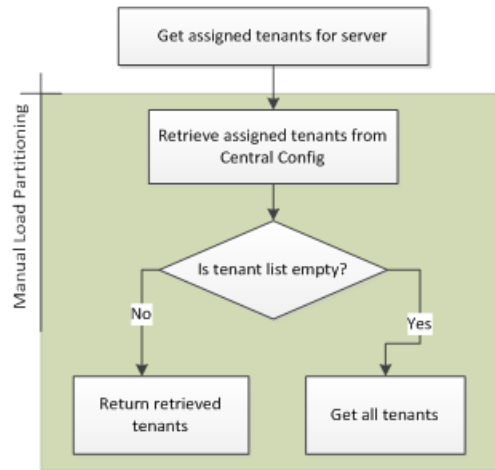
If you do not use the manual load partitioning feature, the workflow or email service load balancing automatically balances the tenants among the participating workflow or email service instances. This guarantees that the tenants are balanced evenly among the servers. However, this creates race conditions among the service instances when starting up and subscribing to events, which can lead to workflow or email subscription failure and deadlock issues.

When you start up the services, the workflow and email services retrieve the list of assigned tenants. The services only process the tasks for the assigned tenants. The system updates the list of assigned tenants in predefined time intervals. If the list of tenants is empty, the system falls back to the default behavior of processing all of the tenants.

Workflow Load Balancing Flowchart



Email Load Balancing Flowchart



Configuring the Workflow Service Configuration File

For the email service, all load partitioning is done manually.

For the workflow service, you can select either manual or automatic (default). To select manual load partitioning for the workflow service, do the following:

Navigate to the workflow binary folder and open the file called WorkflowApp.config with a text editor.

Find the key called EnableLoadPartitioning and set it to false.

Save the file.

Assigning Tenants to the Workflow or Email Service

When you configure workflow or email service servers, ensure that at least one server is defined as the "catch all" server. A "catch all" server manages all of the live tenants, even if it does not have any tenants associated with it. Each host should have at least one "catch all" server. This server processes workflow and email events for all tenants.

For each server, you must enable either the email service, the workflow service, or both. If you do not enable a service on the server but the service is running, the service gets an empty tenant list and it runs as a "catch all" server.

If a service instance crashes or stops, the system deletes the partition details from the database and no other instance will pick these tenants except for the "catch all" server.

Log in to the ConfigDB.

From the workspace selector bar, click More....

Select Service Server. The system displays the Service Server workspace.

Click New Service Server.

Enter the host name in the Host Name field.

If the email service will run on this server, check Is Email Service Enabled.

If the workflow service will run on this server, check Is Workflow Service Enabled.

If the server is a catch all server, check Is Catch All.

If the server is not a catch all server, do the following:

Click the Tenants tab.

Click Link.

Highlight a tenant from the list and click Select.

Click Save.

Viewing the Results of the Manual Load Partitioning

You can view the results of the manual load partitioning in one of two ways:

- Viewing the INFO log for a service. See "Setting the Log Level for the Workflow or Email Service" below and "Viewing the Workflow or Email Manual Load Partitioning" below.
- Viewing a report of the load partitioning through Microsoft SQL. See "Viewing a Report of the Manual Load Partitioning" on the next page.

Setting the Log Level for the Workflow or Email Service

To configure the logs, do the following:

Log in to the ConfigDB.

Open the Logging Configuration workspace.

Open the WorkflowService service.

Change the value of the Log Level field to INFO.

Open the EmailService service.

Change the value of the Log Level field to INFO.

Click Save.

Viewing the Workflow or Email Manual Load Partitioning

After you configure the logs, to view the results, do the following:

Log into the ConfigDB.

Open the Logs workspace.

Use a saved search to show all logs with a service name of WorkflowService or a service name of EmailService.

Logs Saved Search

The screenshot shows the Ivanti ConfigDB interface. At the top, there's a navigation bar with tabs like Tenants, Modules, Trusted Host Addresses, Web Servers, DB Servers, Metrics Server, Logs, All Logs, Customer Contacts, and More... Below this, there's a 'New Saved Search' section with a search criteria table. The criteria are: where Logs icName (Service Name) Equal to WorkflowService, and Logs icName (Service Name) Equal to EmailService. Below the search criteria, there's a table of results with columns: Log Entry Id, Log Time, Log DB Time, Client IP Address, Sub-System Id, Login Id, Tenant Id, Error Code, Service Name, Current Role, Host Name, Thread Name, and Log Severity. The results show logs for WorkflowService and EmailService. At the bottom right, there's a message box with a long SQL query.

Verify that the tenants listed under the current assigned tenant list match the linked tenants for this server.

Viewing a Report of the Manual Load Partitioning

The workflow or email service retrieves the assigned tenants and updates the Frs_ops_workflow_heart_beat and Frs_ops_workflow_partition tables in the ConfigDB.

Before you begin, start the workflow or email service. Keep the current session.

Run the following query in Microsoft SQL on the ConfigDB to see the details of the services that are assigned to each tenant:

```
SELECT ServiceType, HostName, InstanceNumber, TenantId
```

```
FROM Frs_ops_workflow_heart_beat heartbeat
```

```
JOIN Frs_ops_workflow_partition partition
```

```
ON heartbeat.Serviceld = partition.Serviceld
```

The following is an example of the partitioning details:

Service Type	Host Name	Instance Number	Tenant ID
Workflow Engine	CA-L02552	1	ConfigDB, ITSM_7_Daily_Build
Email Engine	CA-L02552	1	ConfigDB, ITSM_7_Daily_Build

Firestore Configuration for Mobile Push Notification

A new workspace - **FCM Configuration** is added to ConfigDB. The following are its sections:

Project Id: Project Id of the firebase which we going to configure in future step. This Id is used by the server to send the push notification.

Server Key: Unique key that is present inside the firebase project. This key is used by the Server to send the push notification.

Client configuration for Android: json configuration which is used by android mobile to generate FCM token. This configuration will be present in Firebase project we need to add in config Database

Client configuration for iOS: Configuration which used by iOS device to generate FCM token.

The following steps should be performed for Mobile Push Notification to work:

[Creating a new Project in Firebase console](#)

[Configure iOS and Android app in Firebase](#)

[Apply iOS Certificate for iOS app](#)

[Configure Firestore in config Database of ISM](#)

Creating a new Project in Firestore

Navigate to <https://firebase.google.com/> to create a new project. Since Firestore is from google, you need to sign into your Gmail account so the Firestore project is associated with your Gmail account.

Navigate to firebase.com and click Go to console on the top right corner of the page.

Click the Create a project tile (for new Users) or Add Project (for existing users) in the firebase.

Enter the project name, select the I accept the firebase terms check box and click Continue.

Disable Google Analytics and click Create Project.

✕ Create a project(Step 2 of 2)

Google Analytics for your Firebase project

Google Analytics is a free and unlimited analytics solution that enables targeting and more in Firebase Crashlytics, Cloud Messaging, In-App Messaging, Remote Config, A/B Testing, Predictions and Cloud Functions.

Google Analytics enables:

✕ ~~A/B testing~~ ?

✕ ~~Crash-free users~~ ?

✕ ~~User segmentation and targeting across
Firebase products~~ ?

✕ ~~Event-based Cloud Functions~~

✕ ~~Predicting user behaviour~~ ?

✕ ~~Free unlimited reporting~~ ?



Enable Google Analytics for this project
Recommended

[Previous](#)

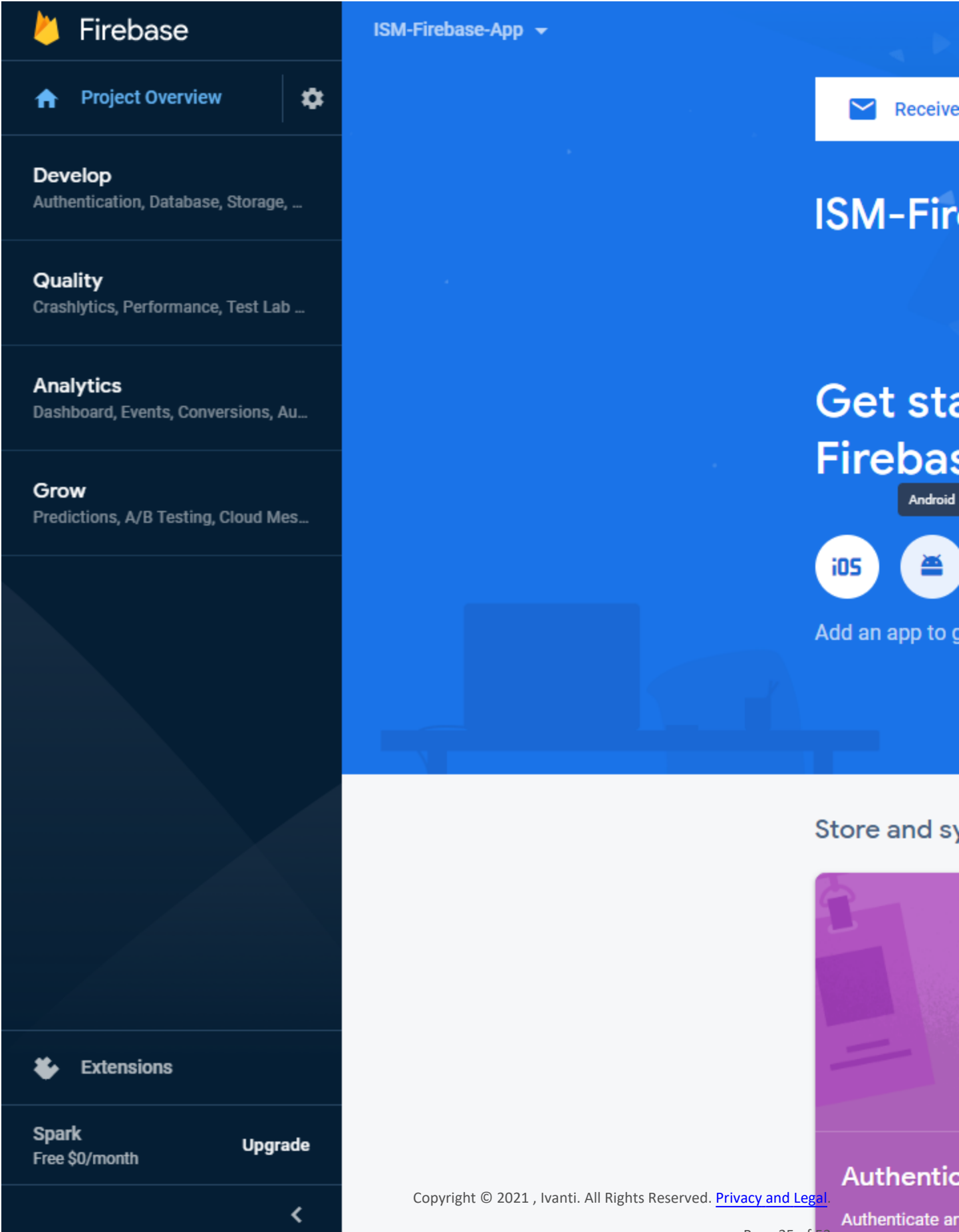
C

Configure iOS and Android app in Firebase.

In this step, you will create iOS and Android app in the firebase project.

Navigate to the newly created project.

Click on the **Android** icon to create new Android app.



Enter the name of the package - it should always be **com.ivanti.sm** in the **Android Package name** and enter any name in **App Nickname**. Ensure the package name is right and click on **Register app**.

×

Add Firebase to your Android app

1

Register app

Android package name ?

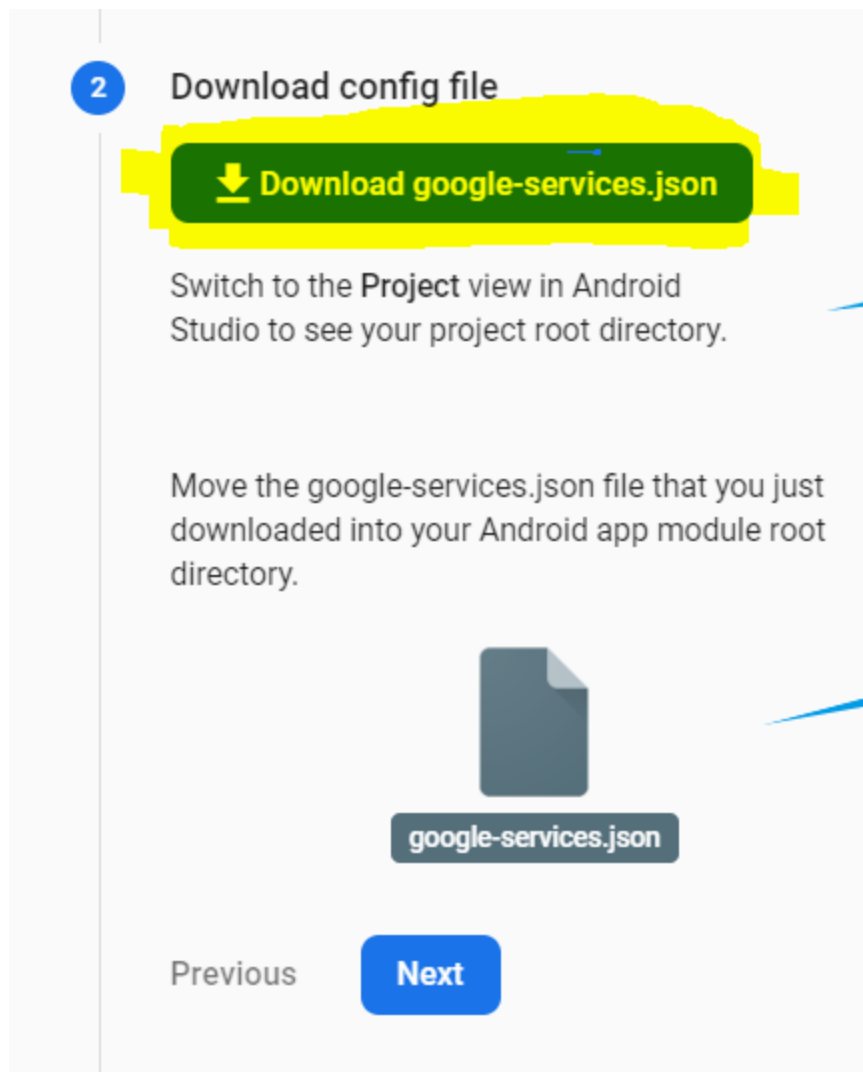
App nickname (optional) ?

Debug signing certificate SHA-1 (optional) ?

Required for Dynamic Links, Invites and Google Sign-In or phone-number support in Auth. Edit SHA-1s in Settings.

Register app

Click on **download google.service.json** which is json configuration for Android. Download this file and click **Next**.



Skip Step 3 by clicking on **Next – (Add Firebase SDK)**


Click **Continue to the console.**

If you see “**Run your app to verify installation**” step then you can click on “**Skip this step**” and then click **Continue to console.**

4

Read the getting started guide for Android

You're ready to start building with Firebase!

Follow the [Firebase getting started guide for Android](#) , where you'll find details about the various Firebase SDKs that you can add to your app and more.

Or, continue to the console to explore Firebase.

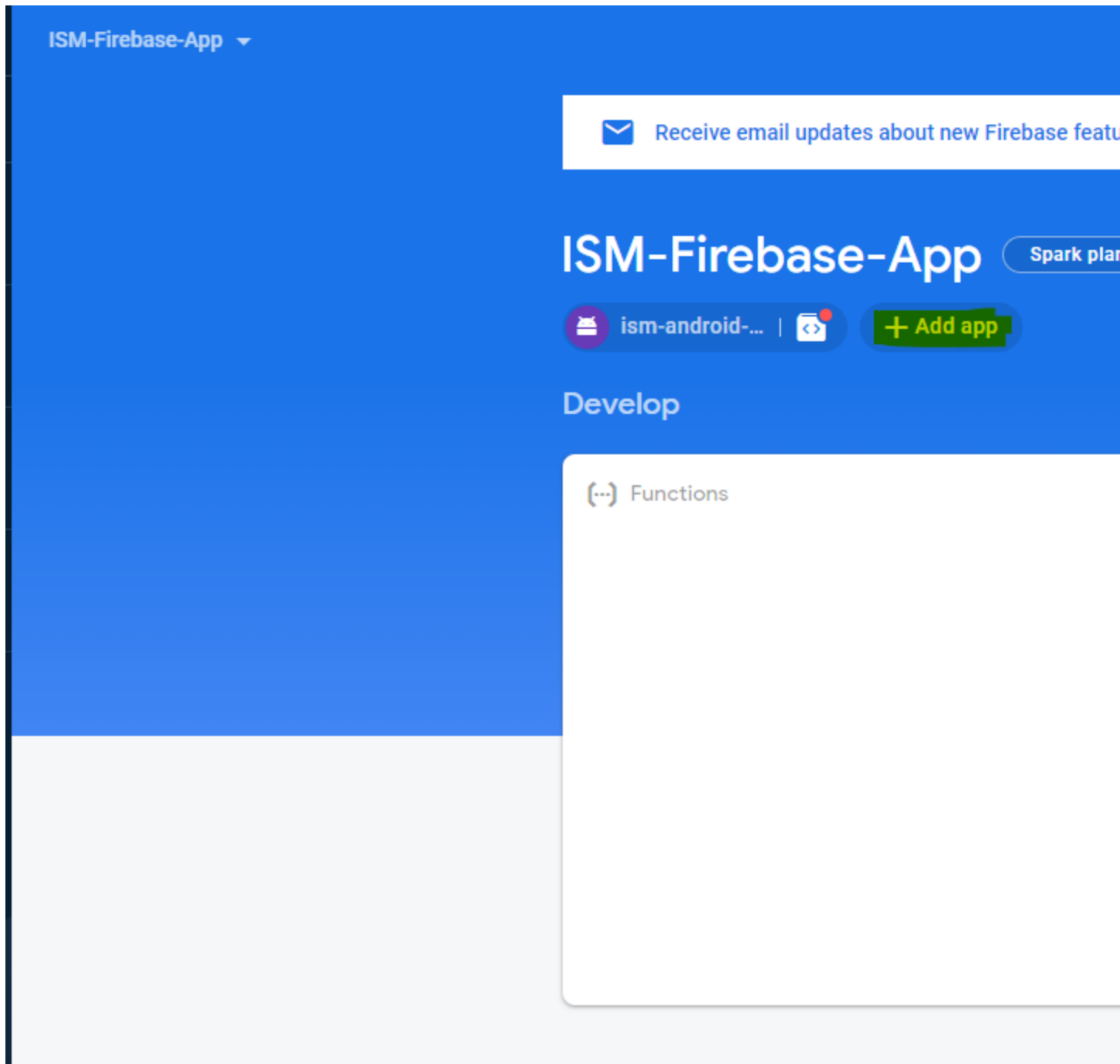
Previous

Continue to the console

Once all these steps are completed, you have the Android app ready in the firebase project.

Now, do the same for iOS.

Click on **Add app** again in the firebase project and select iOS.



Specify the same package name **com.ivanti.sm** in the iOS bundle ID, enter the **App nickname** and click on **Register app**.

× Add Firebase to your iOS app

1

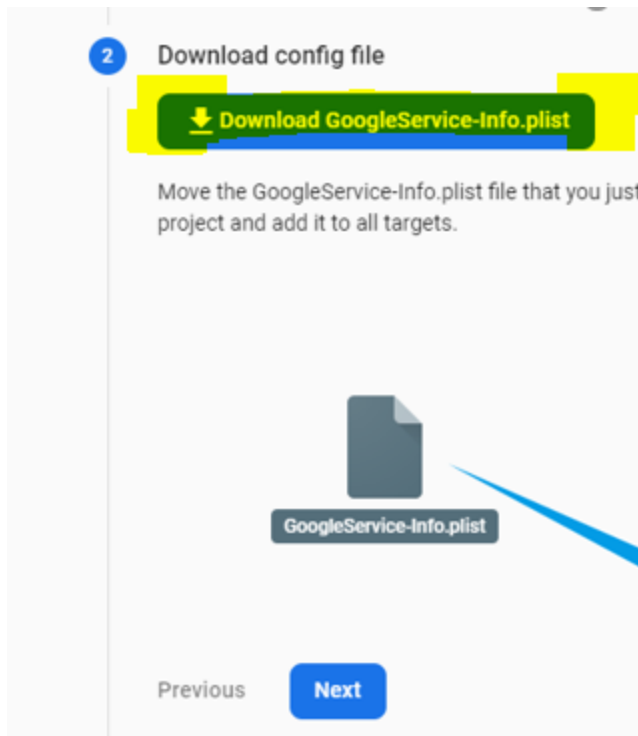
Register app

iOS bundle ID ?

App nickname (optional) ?

App Store ID (optional) ?

Click on **Download GoogleServiceInfo.plist** which contains the configuration for iOS device. and click **Next**.



Skip Step 3 by clicking on **Next – (Add Firebase SDK)**.

Skip Step 4 by clicking on **Next – (Add Initialisation code)**.

Click **Continue to Console** in step 5.


If you see Run your app to verify installation step, click **Skip this step** and then click **Continue to console**.



Once these steps are completed, you have iOS and Android app configuration is ready in the firebase.

Apply iOS Certificate for iOS app

Ivanti will provide the APNs Certificate for iOS app. You can find the certificate at [Ivanti Market Place](#).

Click the **Setting** button from top left and click on **Project settings**.

 **Firebase**


 **Project Overview** 

Develop
Authentication, Database, Storage, ...

Quality
Crashlytics, Performance, Test Lab ...

Analytics
Dashboard, Events, Conversions, Au...

Grow
Predictions, A/B Testing, Cloud Mes...

 **Extensions**


Spark
Free \$0/month **Upgrade**

ISM-Firebase-App ▾


Project settings

Users and permissions

Usage and billing

 Receive

ISM-Fir

 2 apps |

Store and sy

Copyright © 2021 , Ivanti. All Rights Reserved. [Privacy and Legal.](#)

Page 42 of 53


Click the **Cloud Messaging** tab.

ISM-Firebase-App ▾



Settings

- General
- Cloud Messaging
- Integrations
- Service accounts
- Data privacy
- Users and permissions

Project credentials

Key	Token
Server key	AAAA_i4bXQ4:APA91bEx Zf31hwUw750rm1VimFfw
Sender ID 	
1091695238414	

iOS app configuration

iOS apps		Firebase with APNs
	ism-ios-app Not configured for Cloud Messaging	APNs Au  File <div>No AP</div>
		APNs Co

Scroll down to the **APNS Certificate** section and click the **Upload** button.

iOS app configuration

iOS apps

iOS

ism-ios-app

Not configured for Cloud Messaging

Firebase Cloud Messaging can use either an APNs authentication key or an APNs certificate with APNs

APNs Authentication Key

★

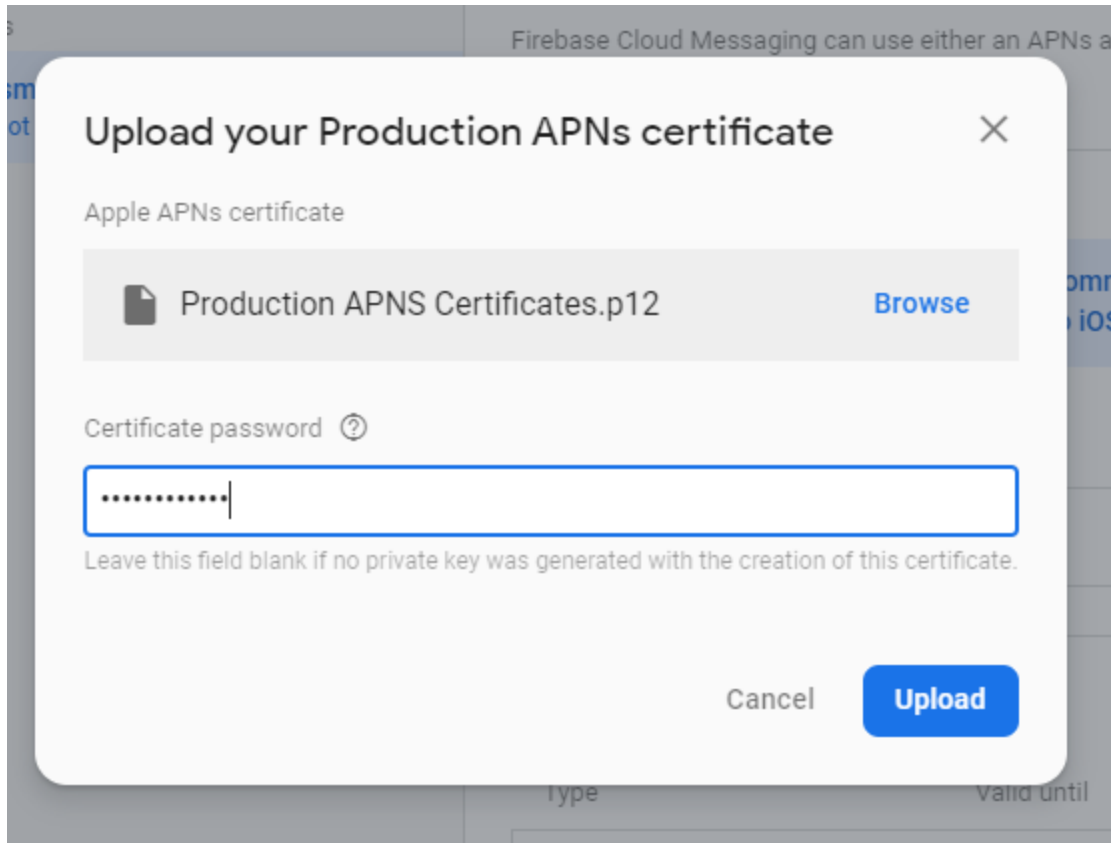
Configuration with auth keys is recommended as the preferred method for sending notifications to iOS

File	Key ID	Team ID
No APNs auth key		

APNs Certificates

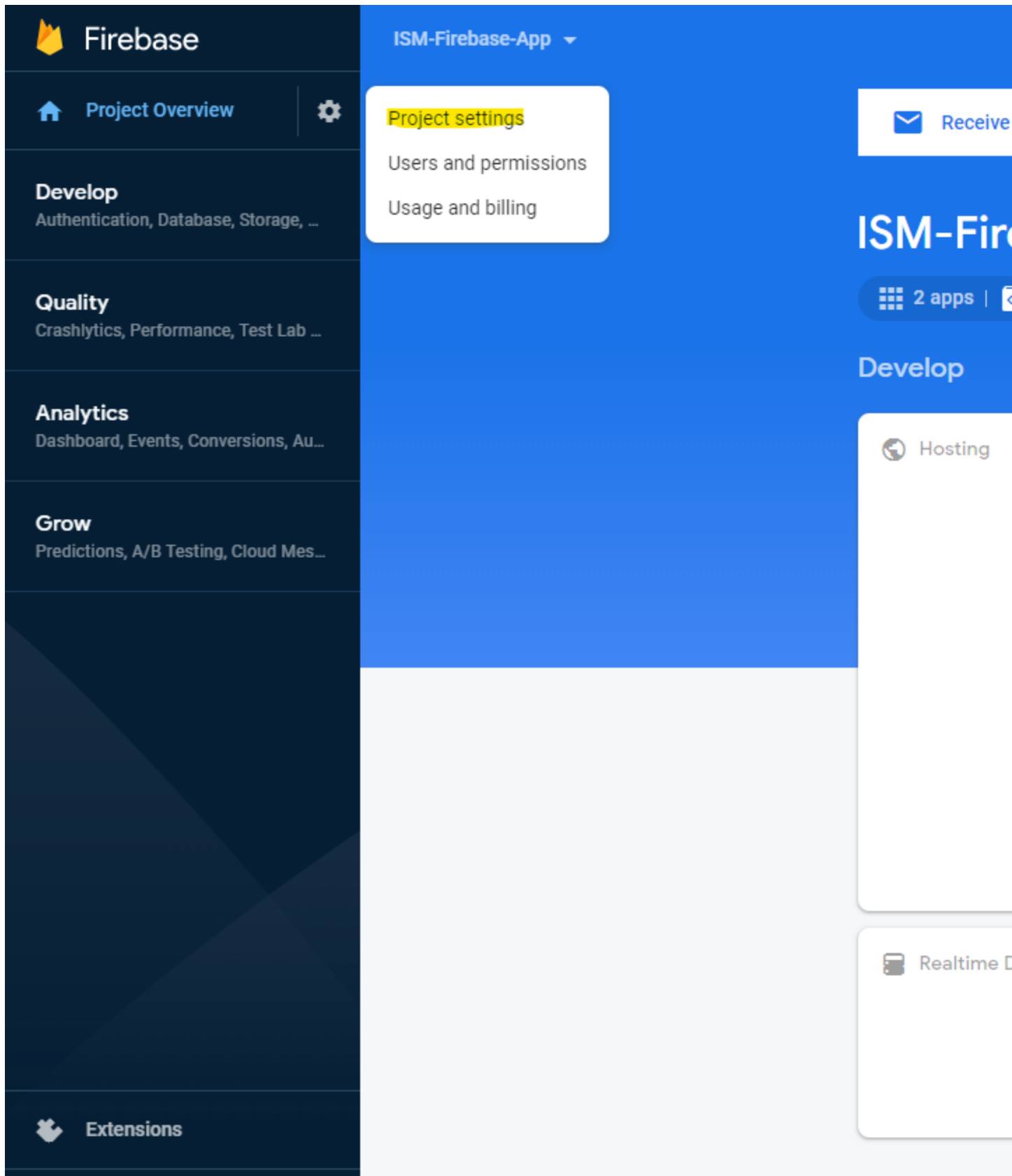
Type	Valid until
No development APNs certificate	
No production APNs certificate	

Upload the APNs Certificate with password.

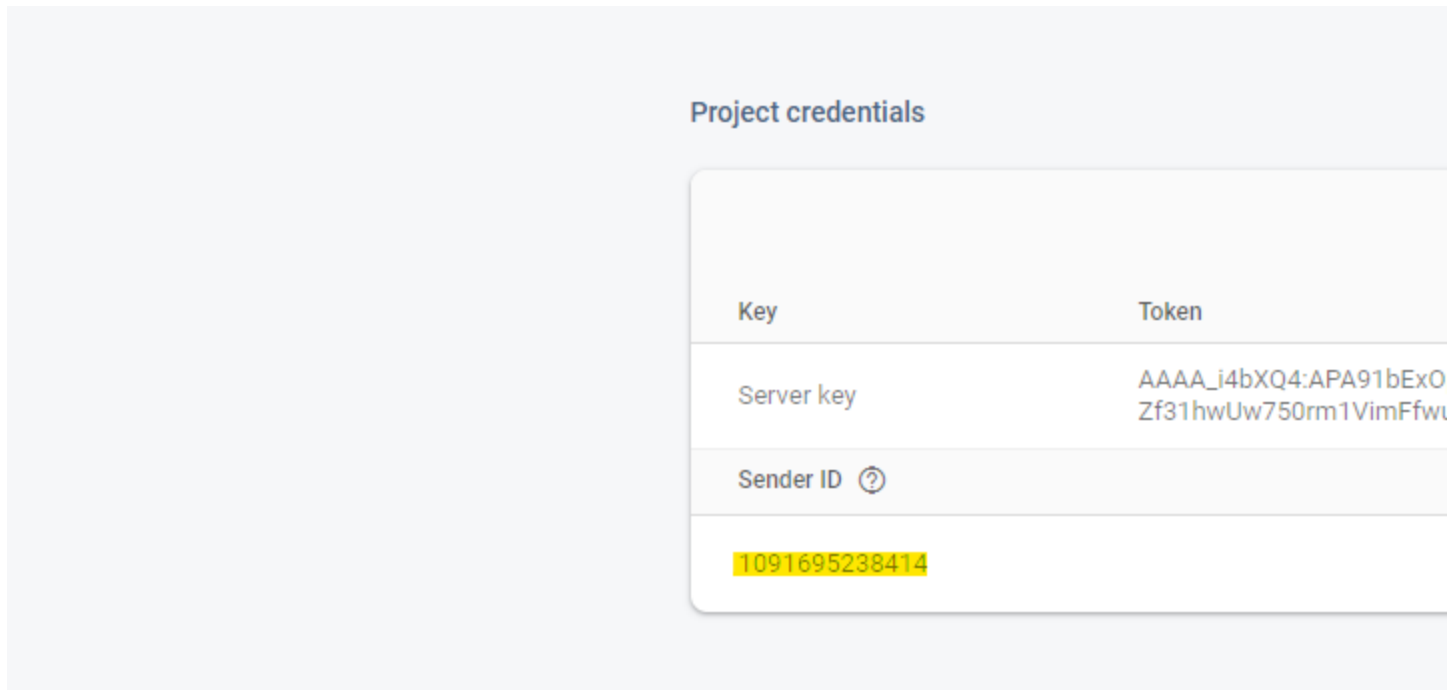


Configure Firebase in Config Database of ISM

Navigate to **Project settings** from the main page of Firebase Project.



Navigate Cloud Messaging Copy the Sender ID.



Go to **ISM CentralConfig**, open **FCM Configuration** workspace and paste **Sender ID** which is copied to the **Project ID** in workspace.


Project Id *	1091695238414
Server Key *	
Client Configuration For Android	
Client Configuration For iOS	

Copy the **Server Key** from **Cloud Messaging** tab.

Project credentials

Key	Token
Server key	AAAA_i4bXQ4:APA91bExOp8i0r3yeoC9eP9SlctoUYypUz9cqO0RBYyi-uePW9dXEA Zf31hwUw750rm1VimFfwuyggcF96HjJvKWMYVIXTqz8MYX8YxM-3G4Q-ybELCzzC
Sender ID ?	
1091695238414	


Paste the **Server Key** in **FCM Configuration** workspace.

Save 

Project Id *	1091695238414
Server Key *	AAAA i4bXQ4:APA91bExOp8i0r3yeoC9eP9SloctoUYypUz9cqO0RBYji-uePW9dXEA2SZlsL2zY5968P0Zf31hwUw750rm1VimFfwuyggcF96HjJvKWMYVIXTMYX8YxM-3G4Q-ybELCzzOzwDdIW

Client Configuration For Android

Copy the entire content from **google-service.json** which is downloaded from Step – 3 and paste in the **Client Configuration** for Android.

Save


Project Id *	1091695238414
Server Key *	AAAA_i4bXQ4:APA91bExOp8i0r3yeoC9eP9SloctoUYypUz9cqO0RBYyi-uePW9dXEA2SZlsL2zY5968P0Zf31hwUw750rm1VimFfwuyggcF96HjJvKWMYVIXMYX8YxM-3G4Q-ybELCzzOzwDdlW
Client Configuration For Android	<pre> { "appinvite_service": { "other_platform_oauth_client": [{ "client_id": "1091695238414-m3suoafm936ddhkoho9g562qgro6if6s.apps.googleusercontent.com", "client_type": 3 }, { "client_id": "1091695238414-giditv69o2sm7b4obmr7m3brosnbpsq4.apps.googleusercontent.com", "client_type": 2, "ios_info": { "bundle_id": "com.ivanti.sm" } }] } }, { "configuration_version": "1" } </pre>

Finally, you need to add the **iOS FCM configuration** in **config DB**. Copy the entire content from **GoogleService-Info.plist** which is downloaded in step-3 and paste it in the **Client Configuration for iOS** and **Save**.

Save 

Client Configuration For iOS

```

    }
  }
]
}
}
},
"configuration_version": "1"
}

```

```

<key>BUNDLE_ID</key>
<string>com.ivanti.sm</string>
<key>PROJECT_ID</key>
<string>ism-firebase-app</string>
<key>STORAGE_BUCKET</key>
<string>ism-firebase-app.appspot.com</string>
<key>IS_ADS_ENABLED</key>
<false></false>
<key>IS_ANALYTICS_ENABLED</key>
<false></false>
<key>IS_APPINVITE_ENABLED</key>
<true></true>
<key>IS_GCM_ENABLED</key>
<true></true>
<key>IS_SIGNIN_ENABLED</key>
<true></true>
<key>GOOGLE_APP_ID</key>
<string>1:1091695238414:ios:db8afa9f2d1aa8f1424b5f</string>
<key>DATABASE_URL</key>
<string>https://ism-firebase-app.firebaseio.com</string>
</dict>
</plist>

```