# IBM Project Report

## On

# Setup enterprise mobility management to manage and secure devices for connecting organizational networks.


**Developed by: -**
Drishti Motwani (18162171013)
Rutvik Patel (18162171026)
Jhanvi Zala (18162171035)

**Guided by: -**
Prof. Rahul Shrimali (Internal)
Mr. Anoj Dixit (External)


## Submitted to

## Department of Computer Science & Engineering
## Institute of Computer Technology


## Year: 2022

# CERTIFICATE

This is to certify that the **IBM** Project work entitled **"Setup enterprise mobility management to manage and secure devices which connect organizational networks"** by Drishti Motwani (Enrolment No.18162171013), Rutvik Patel (Enrolment No.18162171026) and Jhanvi Zala (Enrolment No.18162171035) of Ganpat University, towards the partial fulfillment of requirements of the degree of Bachelor of Technology – Computer Science and Engineering, carried out by them in the CSE (CS) Department. The results/findings contained in this Project have not been submitted in part or full to any other University / Institute for award of any other Degree/Diploma.

Name & Signature of Internal Guide

Name & Signature of Head

**Place: ICT - GUNI**

**Date: 06-05-2022**

# ACKNOWLEDGEMENT

IBM project is a golden opportunity for learning and self-development. I consider myself very lucky and honored to have so many wonderful people lead me through in completion of this project. First and foremost, I would like to thank Dr. Hemal Shah, Principal, ICT, and Prof. Dharmesh Darji, Head, ICT who gave us an opportunity to undertake this project. My grateful thanks to Prof. Rahul Shrimali & Mr. Anoj Dixit (Internal & External Guides) for their guidance in project work Setup enterprise mobility management to manage and secure devices which connect organizational networks, who despite being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where would have been without his/her help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

**Jhanvi Zala (18162171035)**
**Rutvik Patel (18162171026)**
**Drishti Motwani (18162171013)**

# ABSTRACT

Enterprise Mobility Management (EMM) is one of the important part of Enterprise Mobility Ecosystem. EMM basically emphasize on security& management of mobile applications, its data & the devices that are being used. EMM also helps enterprise users to be more productive as EMM provides them with the tools that they need to perform work-related tasks on mobile devices. EMM consists of Enterprise App Store Mobile E-mail management, Mobile Content Management, Mobile Billing Management, Mobile Device Management, Mobile Application Management. It is possible that there might be some of the overlap of features between these management sub modules but can be understood differently with simple approaches which can really help the Enterprise and its users at its best.

# INDEX

# CHAPTER: 1 INTRODUCTION

# CHAPTER 1 INTRODUCTION

## Enterprise Mobility Management (EMM)

Now a day's mobile devices are becoming an essential requirement in the workplace so due to that EMM is becoming a critical IT necessity. In the last few years, mobile devices like smartphones and tablets have been updated in many ways. So due to that, they get used for so many industrial purposes. One of the main advantages of this is that employees can work from any remote location at any time. One main disadvantage of this is that if this device is used for industrial purpose and are not properly handled it will endanger the company's data and network security. To overcome this issue nowadays companies are adapting EMM solutions to protect their employee's devices having different platforms like iOS, Android, and windows.

To manage mobile devices with better monitoring and control IT companies are adapting EMM solution which includes a different set of tools. It has services like mobile device management(MDM), mobile application management(MAM), Mobile content management(MCM), identity access and management(IAM). Employees having devices with secure services can use the company's application, document, tools, etc. from any place at any place without endangering the device, company, and network integrity.

In the last few years, the demand for Android and iOS devices has increased tremendously as they have more features than older OS available. So do that, employees are demanding to the company to allow employees to bring their own devices to the workplace and from that time bring your own device(BYOD) policy get encouraged. Now due to this, there are so many benefits for IT company's as expenses get reduced, the productivity of employees gets increased, the efficiency of work and also enjoyment option also get increased for employees.

## Mobile Device Management (MDM)

MDM refers to Mobile Device Management and it belongs to managing devices of employees that they are using for work purposes like laptops, tablets, smartphones, etc. With an enrollment of devices an administrator will have rights like managing mobile devices, and their operating system's entire lifecycles, it also contains device inventories, configuration, and information about the device.

Devices will get registered by some specifics vendors like apple, google, Microsoft, QR codes, emails, and SMS. During adding of devices administrators have to configure and manage them. After enrolling once, devices are then managed and set up remotely. Mobile device management will work on software-as-a-service so they are cost-effective, simple to manage, and scalable. As they are working on SaaS MDM service can be installed on both local and cloud servers

## Mobile Application Management (MAM)

MAM refers to mobile application management means with this an administrator can deploy, manage and patch applications that have to use by employees. It may happen that an employee will share that application and data contained in that application with some outsider. So for that company will put security and control on applications and also keep them from personal applications.

Employees are also using the EMM solution to get information about application stores. Inventory management, application lifecycle management, and software license configuration are all required services of EMM solutions. This all can help to remove an application from an employee's devices if any security breach will occur from the application.

## Mobile Content Management (MCM)

Every company will have some confidential documents, some files that are to be shared with some people. So MCM company can share the document with employees to make it more productive. MCM is a secure tool with which employees can access, share and also save work files on their mobile devices securely. MCM service also has a feature to help with the decision of the company's data and network. Sometimes companies became a victim of some cyber-attack so with help of MCM service IT professionals can block access to the network. MCM service will make it easier for employees to interact.

## Mobile Identity Management (MIM)

All company data is valuable and not all data is available to all. So, it should be accessed by those who are authorized to them. Businesses must adopt a zero-trust security policy as their workforces become increasingly mobile, distributed, and remote. This can be done when employees have to confirm their identification whenever they are connected to the company's network

Whenever MIM services will find some suspicious activity during configuration at that time they refuse to authenticate that user. To validate user identification MIM service will use Multifactor authentication(MF), device-specific information or biometrics, and password management.

## Unified Endpoint Management (UEM)

UEM refers to Unified Endpoint Management services in a frame after MDM and MAM.

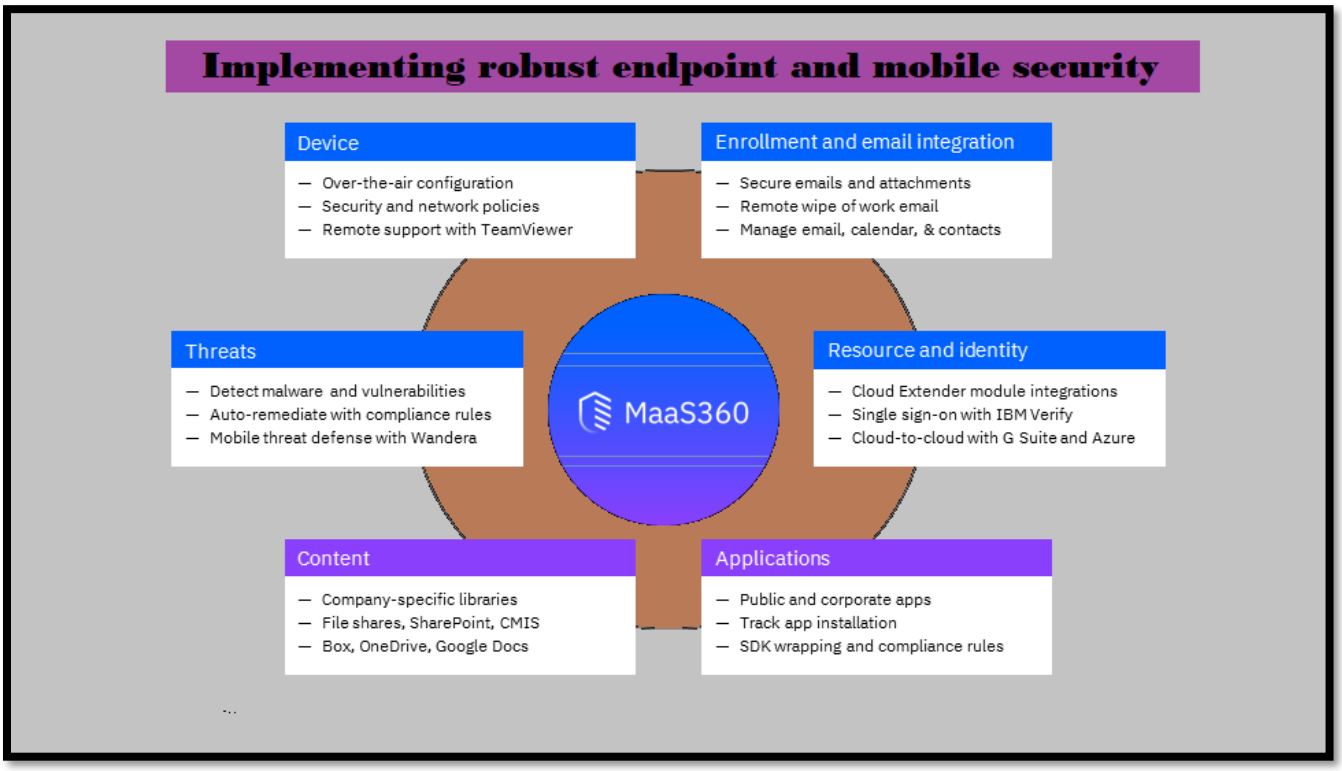
MDM is being used to manage mobile devices but companies can also use UEM. Also, UEM is used for endpoints connected to company networks like routers, servers, the Internet of Things, and wearables devices. If a company has a UEM tool, then it is not required to have an EMM tool as it lowers IT costs and improves department capability to manage mobile devices connected to the company's network.

# CHAPTER: 2 PROJECT SCOPE

## CHAPTER 2 PROJECT SCOPE

According to this study, using an EMM solution leads to a superior degree of data protection and security for mobile devices. The investigation focuses on the verification of selected data in both a secure and a non-secure environment. The test environment consists of an Android-based mobile device, two analytic tools, and a commercial EMM cloud service.

Employees can also work from any location and at any time. They can, however, jeopardize a company's data and network security if not properly handled. From this conclusion is that today all IT company required to implement EMM solutions to protect and manage mobile devices with various platforms like android, iOS, and windows.



# CHAPTER: 3 SOFTWARE AND HARDWARE REQUIREMENTS

# CHAPTER 3 SOFTWARE AND HARDWARE REQUIREMENTS

## Minimum Hardware Requirements for IBM Maas360

| | |
|---|---|
| **Processor** | 4.2 GHz |
| **RAM** | 16GB |
| **HDD** | 30GB |

*Table 3.1 Minimum Hardware Requirements*

## Minimum Software Requirements for IBM Maas 360

| | |
|---|---|
| **Operating System** | Google Chrome: 79, 80, 81<br>Firefox: 74, 75, 76<br>Safari: 11, 12, 13<br>Opera: 66, 67, 68<br>Microsoft Edge: 79, 80, 81<br>Internet Explorer: 11 |
| **Programming language** | - |
| **Other tools & tech** | - |

*Table 3.2 Minimum Software Requirements*

# CHAPTER: 4 PROCESS MODEL

# CHAPTER 4 PROCESS MODEL

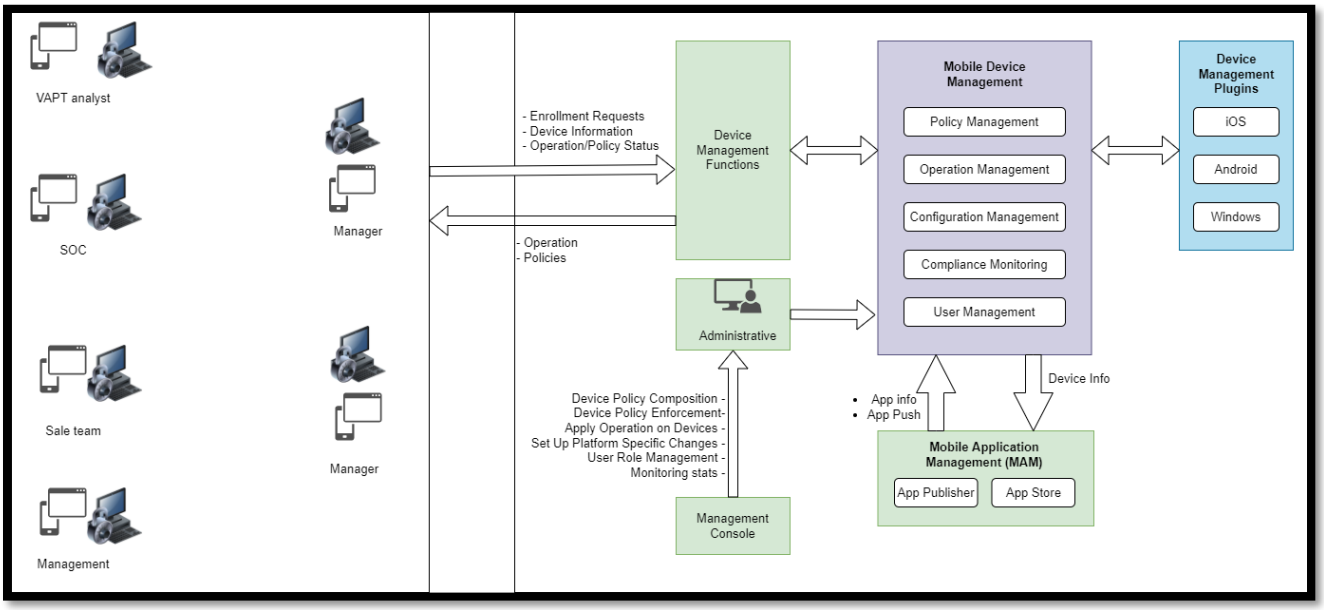



*Figure 4.1 Process Model of Project*

# CHAPTER: 5 PROJECT PLAN

# CHAPTER 5 PROJECT PLAN

## 5.1 List of Major Activities

**Task1:** Created a checklist to implement checklist

**Task2:** Architecture design

**Task 3:** Configuring device enrollment settings in the MaaS360 Portal

**Task 4:** Configuring user settings in the MaaS360 Portal

**Task 5:** Configuring app settings in the MaaS360 Portal

**Task 6:** Configuring administrator settings in the MaaS360 Portal

**Task 7:** Service implementation (MDM, MAM, Secure email, secure browser, IAM)

## 5.2 Estimated Time Duration in Days

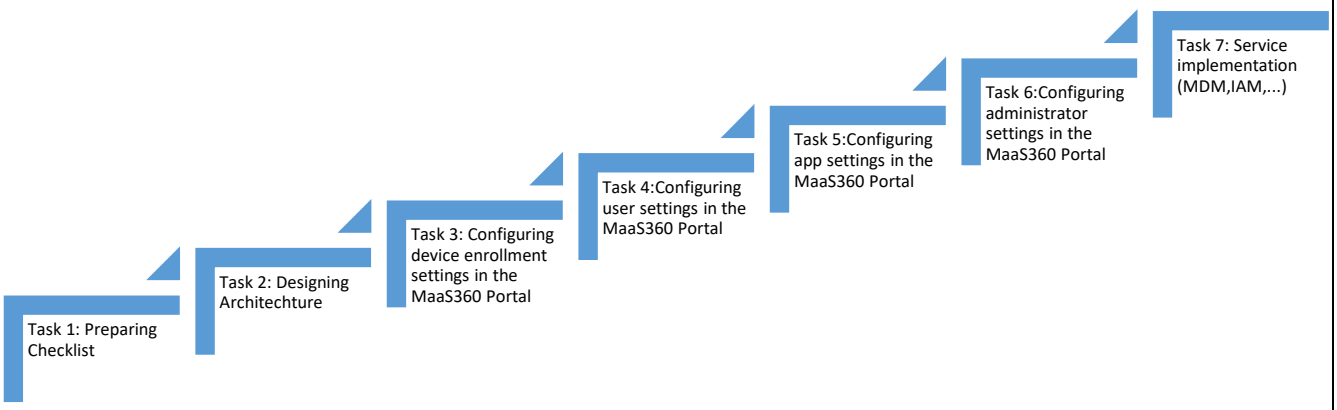



*Figure 5.1 Task Completion Estimated Time Duration in Days*

# CHAPTER: 6 IMPLEMENTATION DETAILS

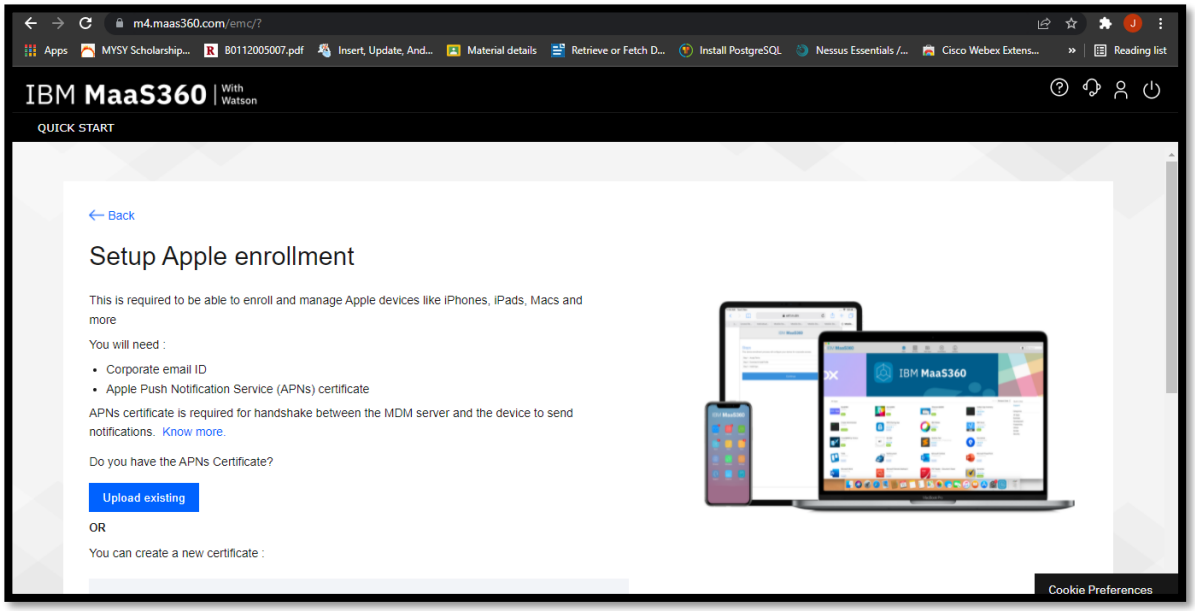
# CHAPTER 6 IMPLEMENTATION DETAIL

## 6.1 Mobile Device Management

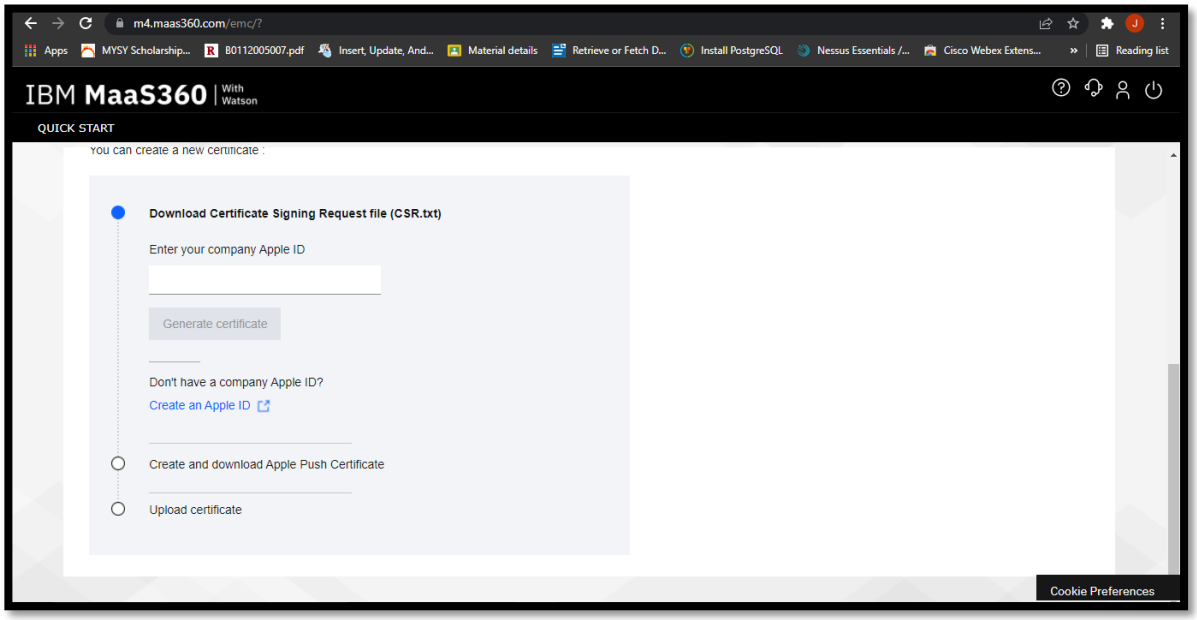
### 6.1.1 Setup of IBM Maas360

To setup IBM Maas360 first we need to configure apple device, android device and windows. So for that click on quick start and there we get option of setting up apple ID and APNs certificate.

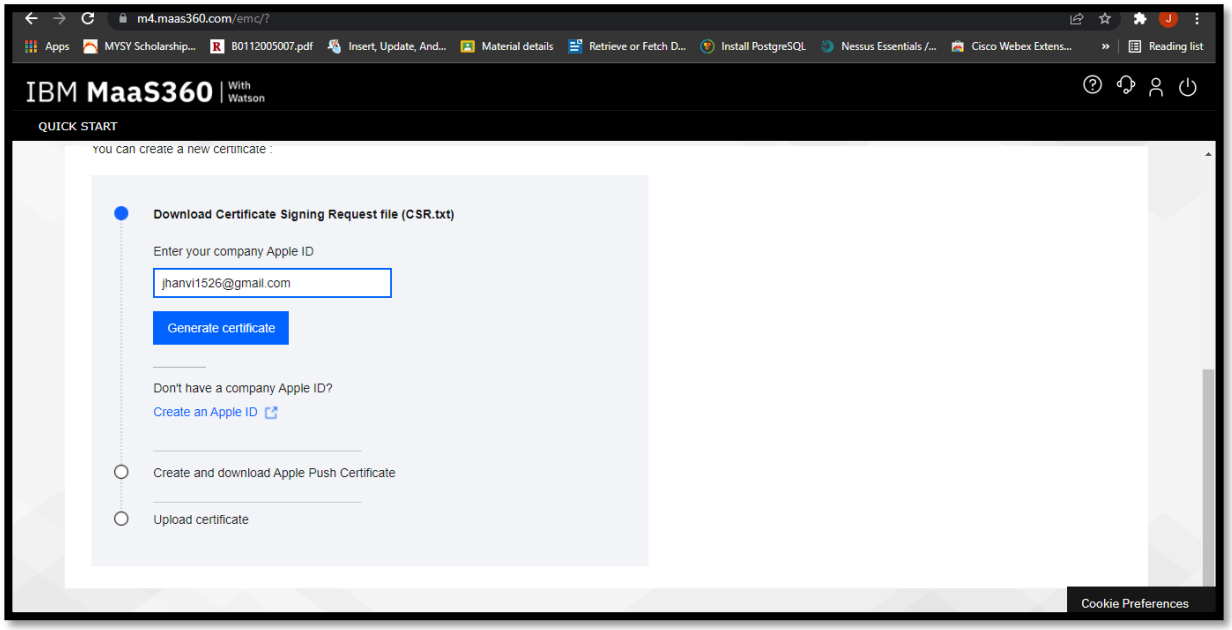
1. Click Setup iOS Now. Use either the Safari, Chrome, or Firefox web browser to download the certificate.



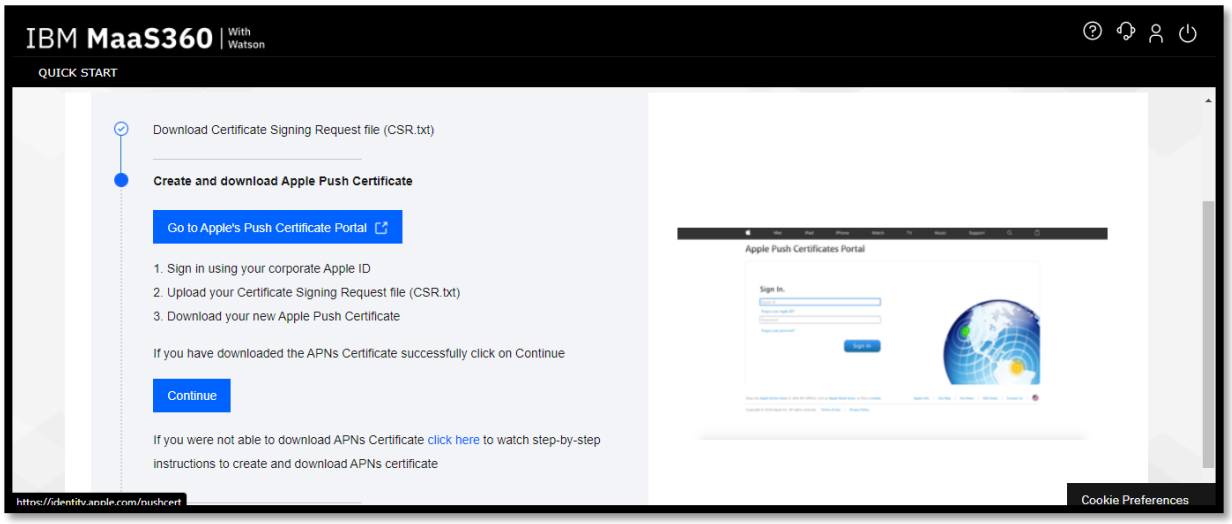

2. Type your corporate Apple ID and click Next.You must use the same Apple ID every year when you renew your APNs certificate. If you do not have an Apple ID, mouse over Create ID and click Apple Website to access a page where you create a corporate Apple ID.



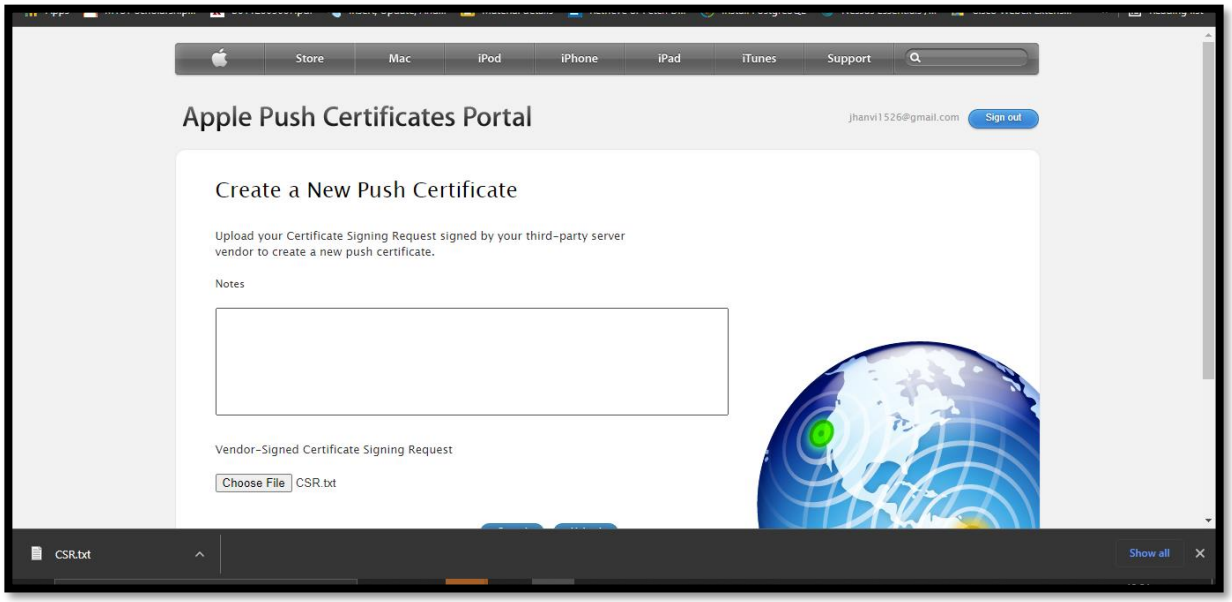
3. To create a PEM file. Click on generate a Certificate.



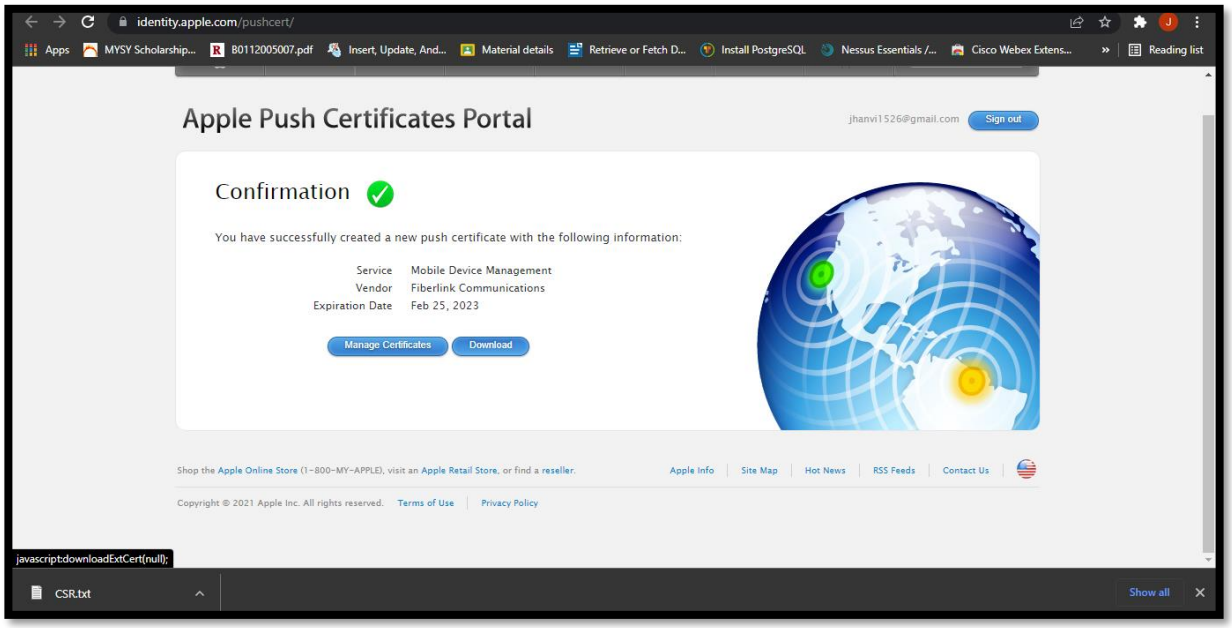

4. After you've completed the previous step. Accept the terms and conditions by checking the box. Then press the accept button.



5. Now to upload a CSR.txt file. We need to first locate that file so for that click on browse and after that upload that certificate file.
6. Click Open, and then click Upload.

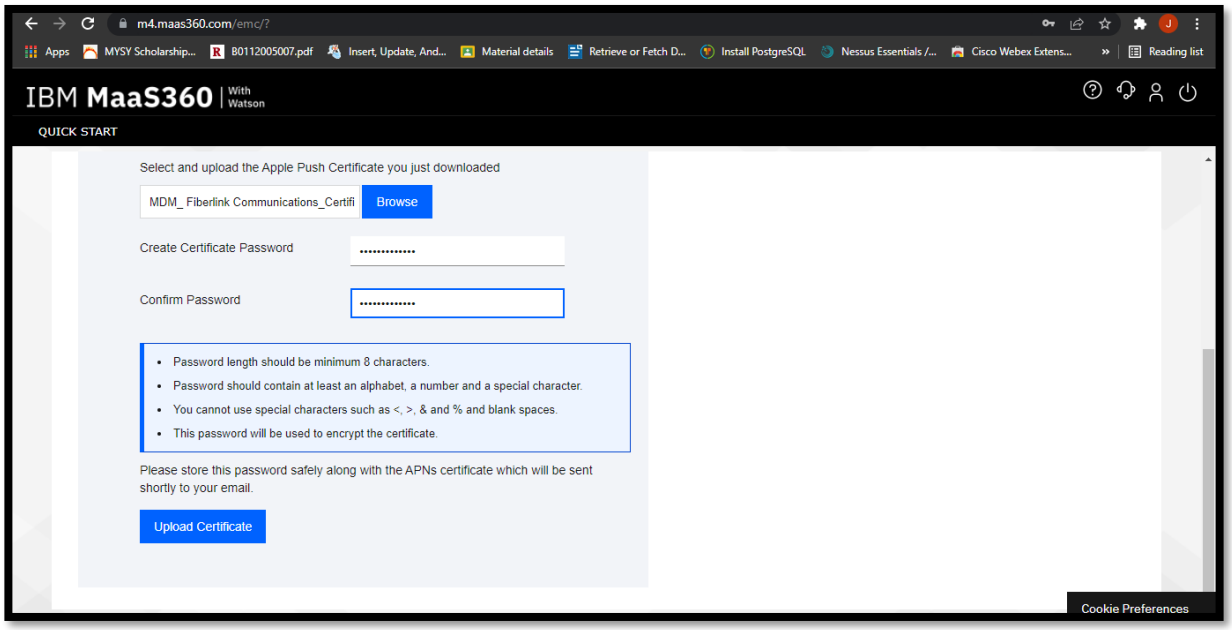



7. Click Download to download the PEM file.

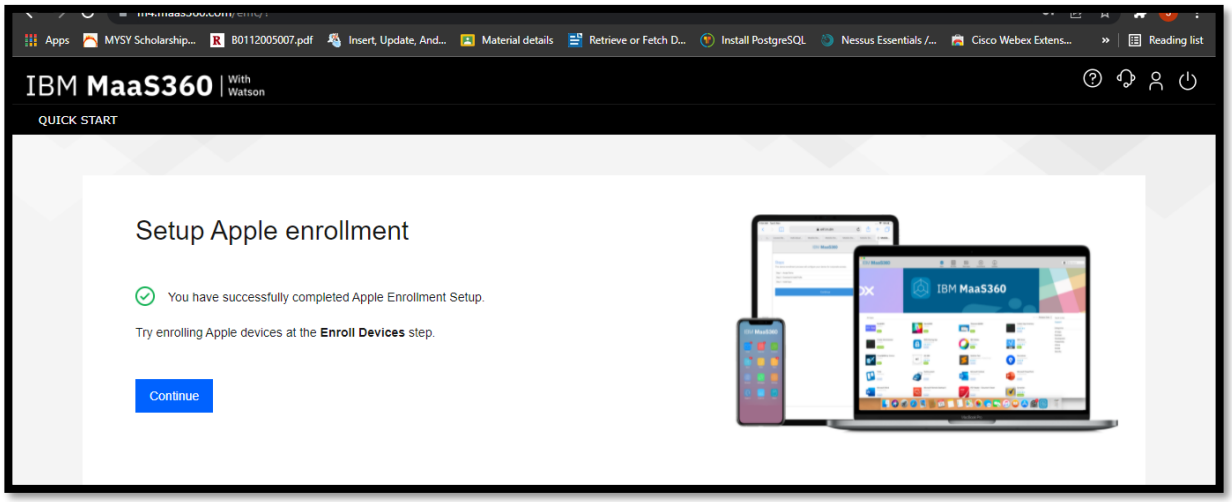



8. Click OK to save the PEM file to your Downloads folder, and then click Next.
9. Click Browse to upload the certificate to MaaS360.

10. Locate the MDM_Fiberlink_Communications.pem file in your Downloads folder, and then click Open.



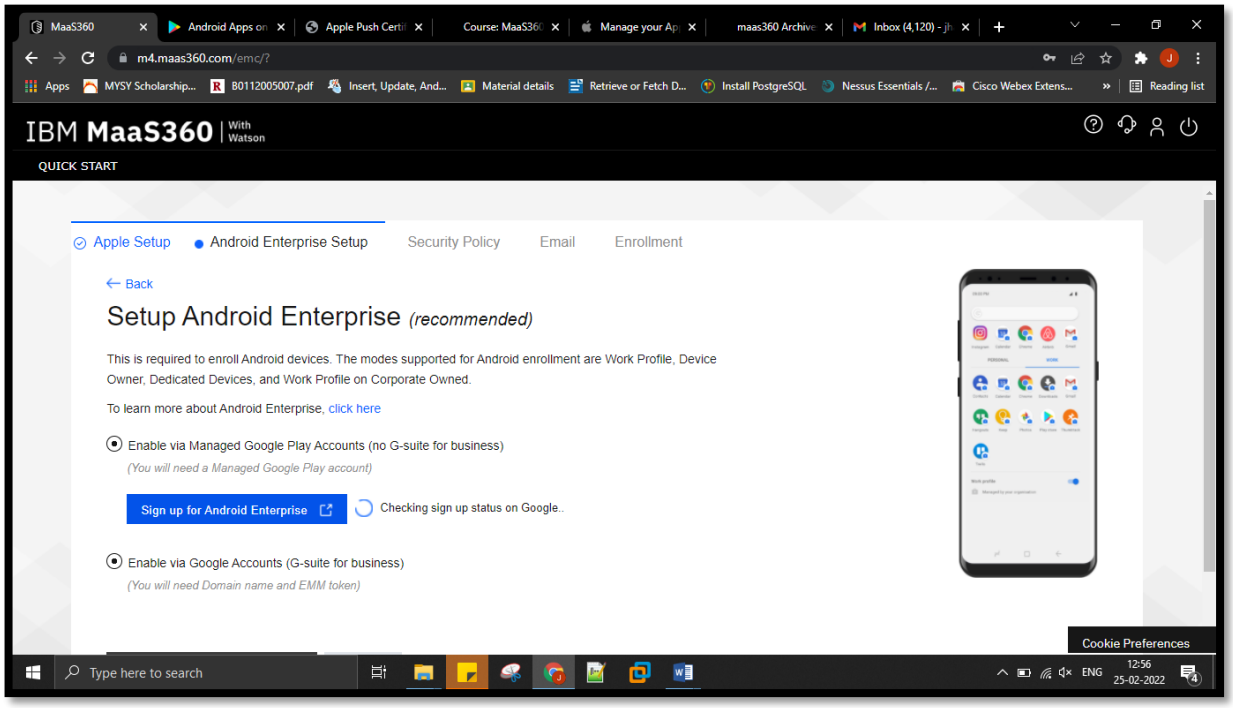

11. Type a password, and then click Upload. Note: This password has no minimum security requirement. To help you remember the password, you might want to use the password that you used for your Apple ID password. The APNs certificate is created.



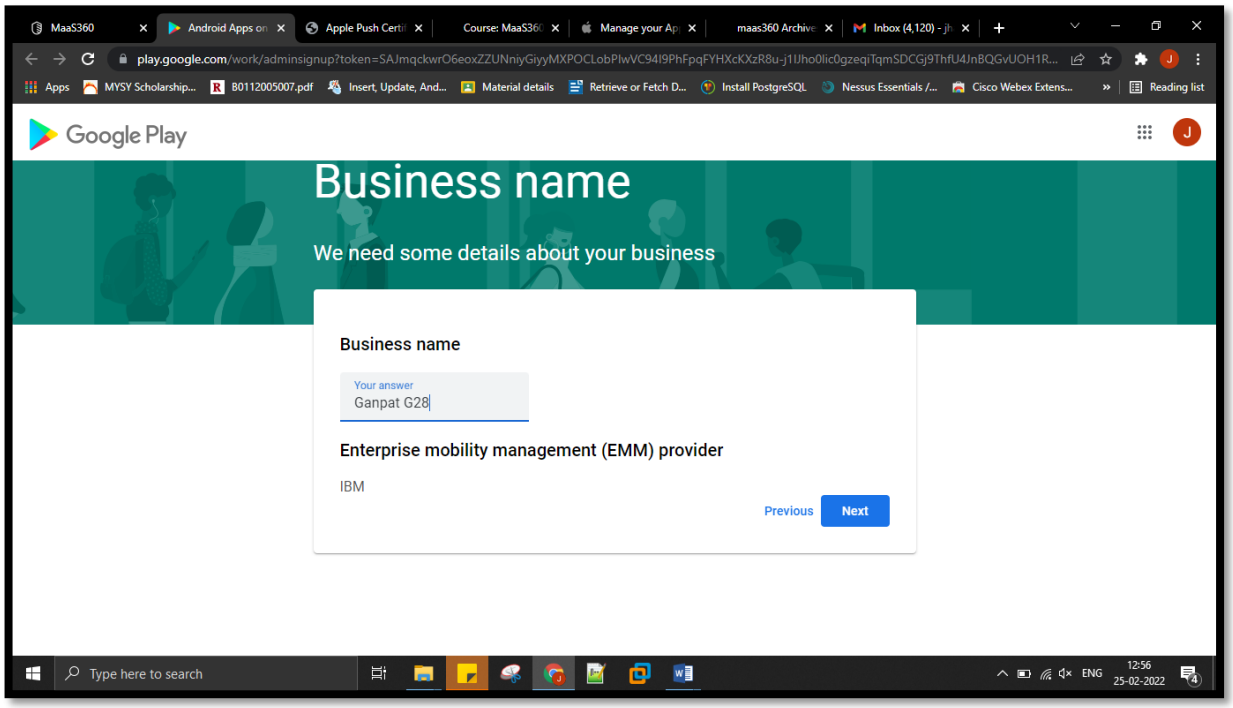

12. Click Close.

### 6.1.2 Android configuration:

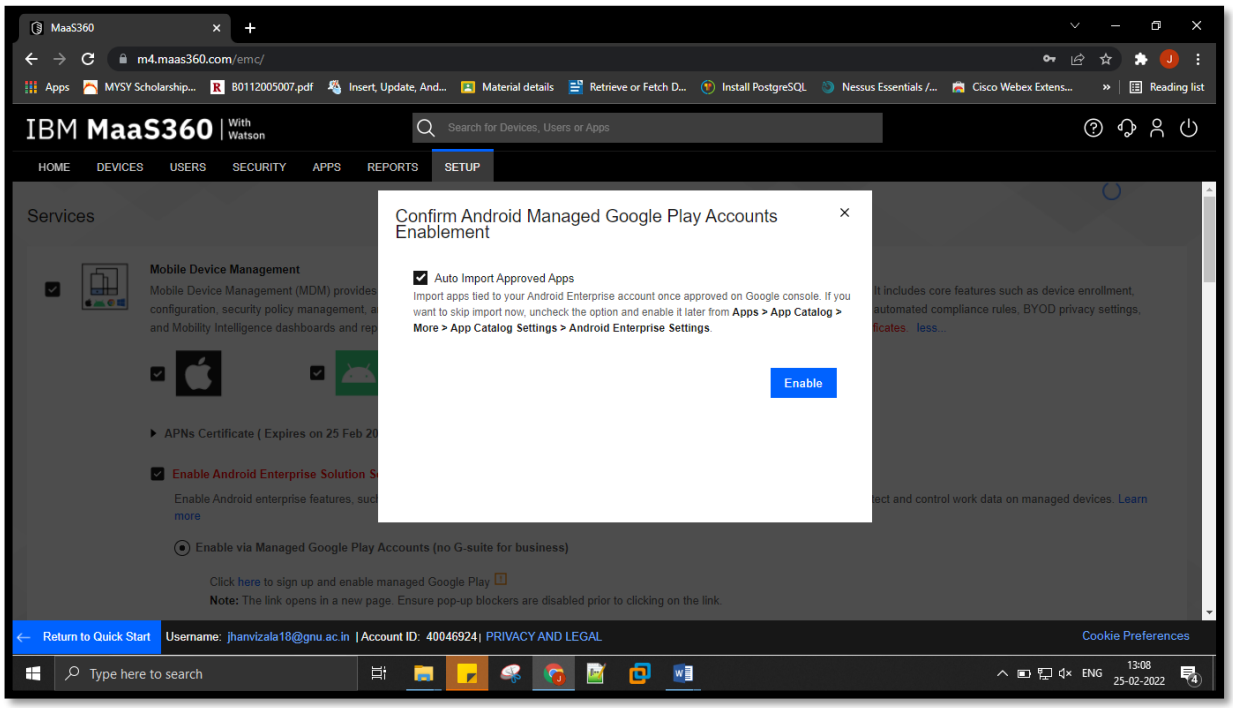
1. To navigate to MDM service. Go to Setup > Services > Mobile Device Management, and then select Enable Android for Work > Enable via Google Accounts.



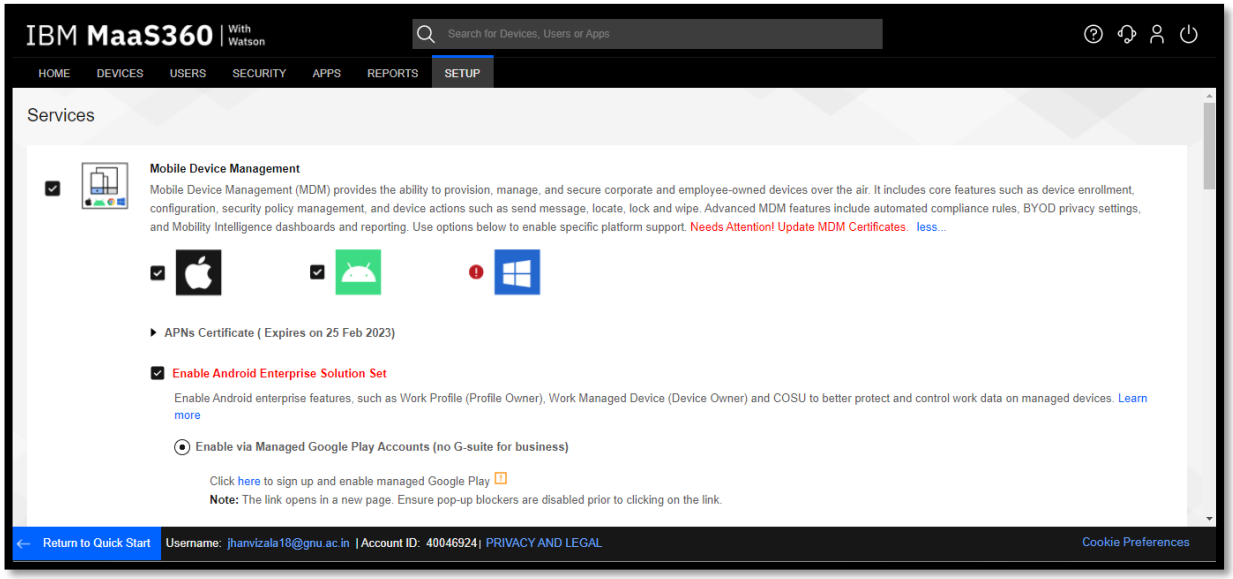

2. Go to the G Suite Admin console (admin.google.com), and then enable the Android Enterprise app (enabled by default in the standalone version of Android Enterprise). You can manage the EMM provider from the Billing subscriptions, which is a free service.



3. Go to Under Security > Show More > Manage EMM Provider for Android, and then click the Generate Token tab.
4. Now for this process we need to generate a token so for that go to Google administration console at https://admin.google.com/AdminHome.
5. Generate a new token or use an current token.




6. In the MaaS360 Portal, enter the domain name, and then copy and paste the token from the G Suite console. 162 IBM MaaS360 Mobile Device Management (SaaS) A message is displayed to indicate that the Android Enterprise integration is successful.



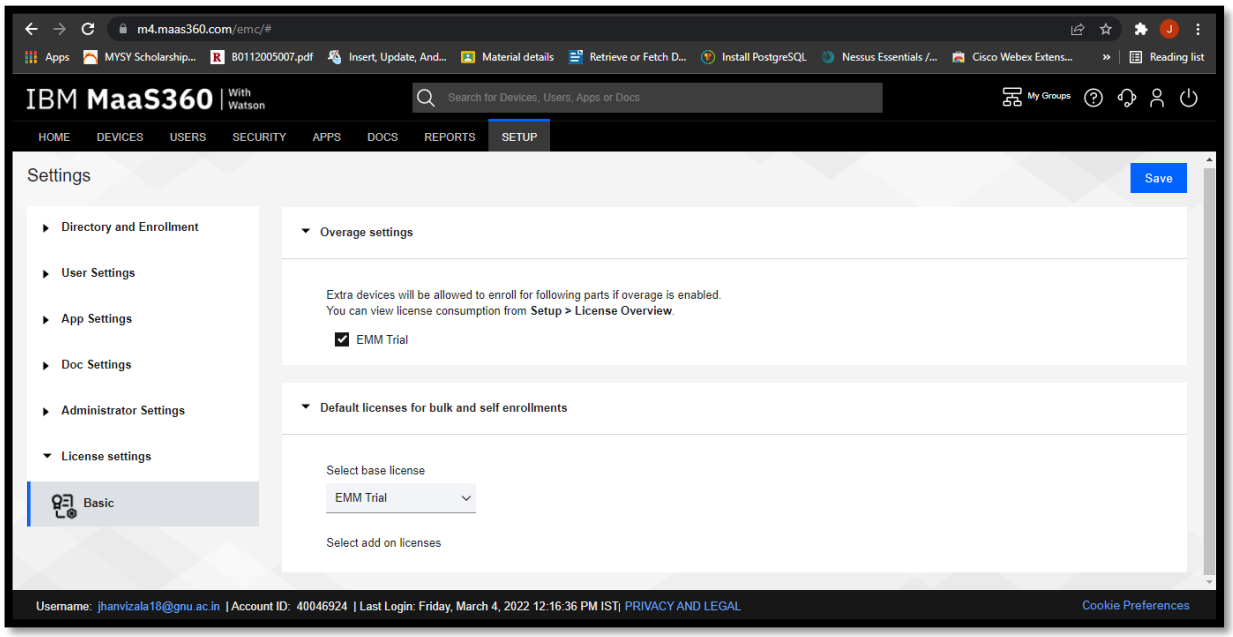
### 6.1.3 License configuration:

As IBM MaaS360 is a paid version. It is having license configuration for organization which is implementing it as it gives administrators rights to setup and manage different modules of Maas360

MaaS360 features are available for customers to enable in the form of services. Customers can turn on these services from the MaaS360 Portal Services section or as settings in MaaS360 policies, depending on their licencing entitlement. To evaluate licence consumption, MaaS360 licence management tracks the activation of various services on devices. The service usage is aggregated for a device or a user depending on whether the license model is per device or per user.

With this feature, administrators can setup license settings, allocate licenses to devices one at a time, and allocate licenses in bulk to devices from a CSV file upload. With the Add Device enrollment request, administrators can specify which licenses are allocated to a device. For self-enrolled devices and bulk enrollment mode, administrators can use the License Settings page to specify which licenses are assigned to a device.

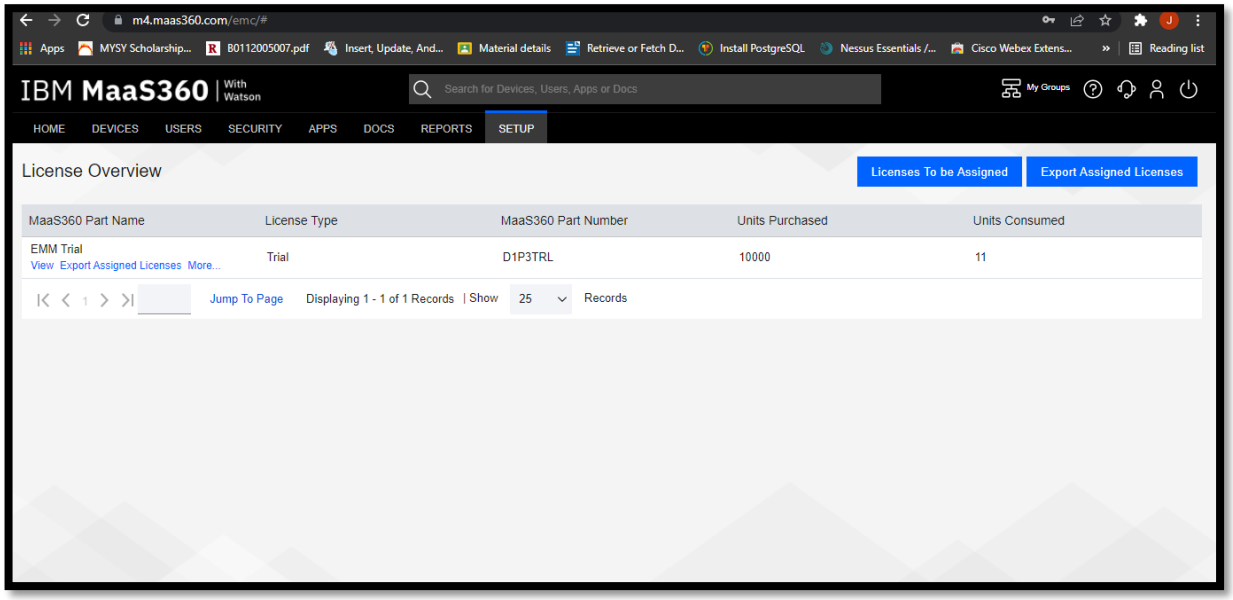
For this go to **Setup->services->license setting**:

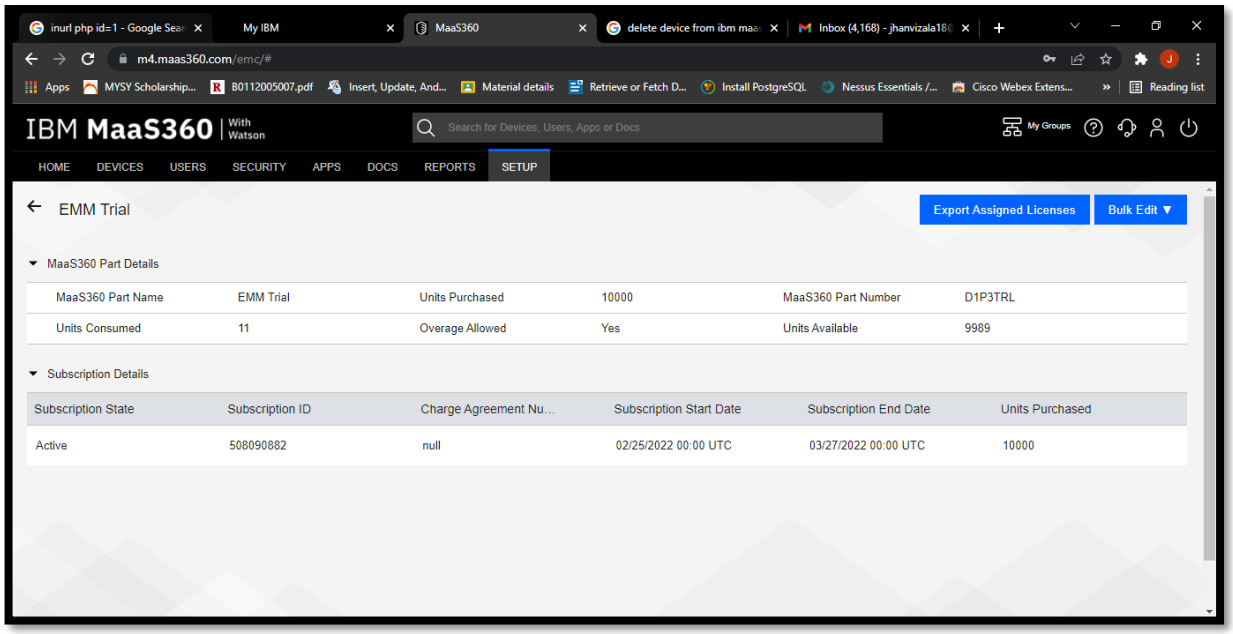


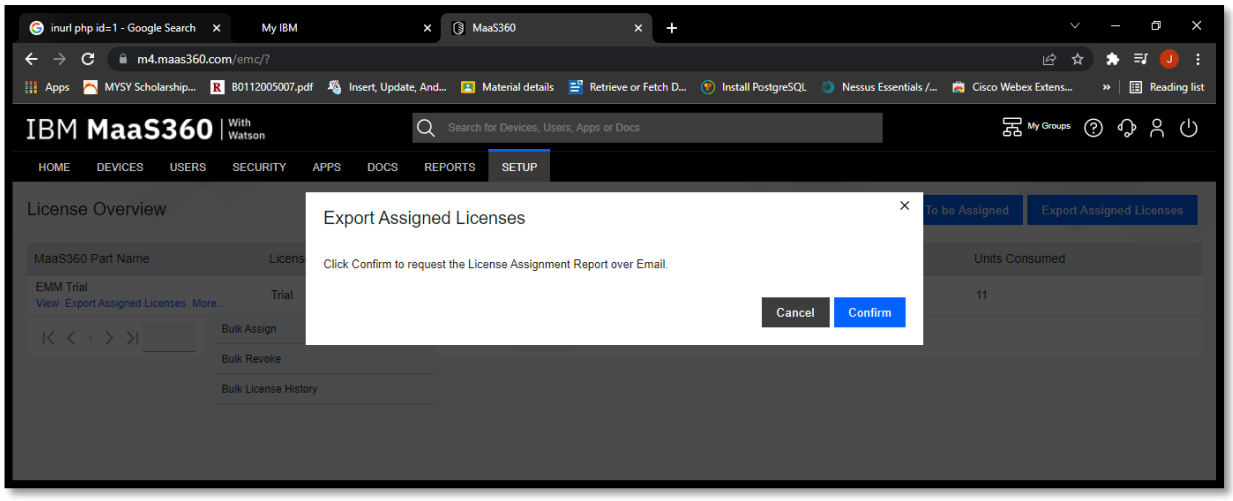

Here we are using EMM trial version.

The License Overview page lists all the licenses that are available for the customer account. For each license, the page displays the type of license, the license part number, and the number of licenses purchased and used by devices. Administrators are having rights to assign licenses to devices and users in bulk

Access the License Overview page at MaaS360 Portal > Setup > License Management.



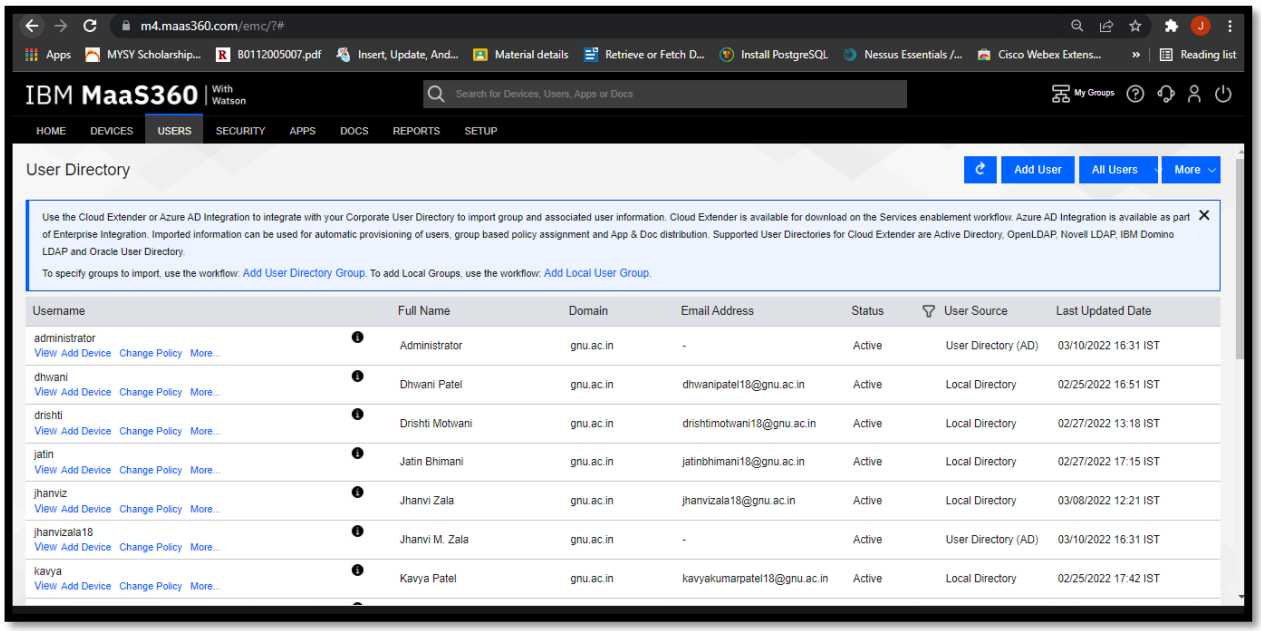



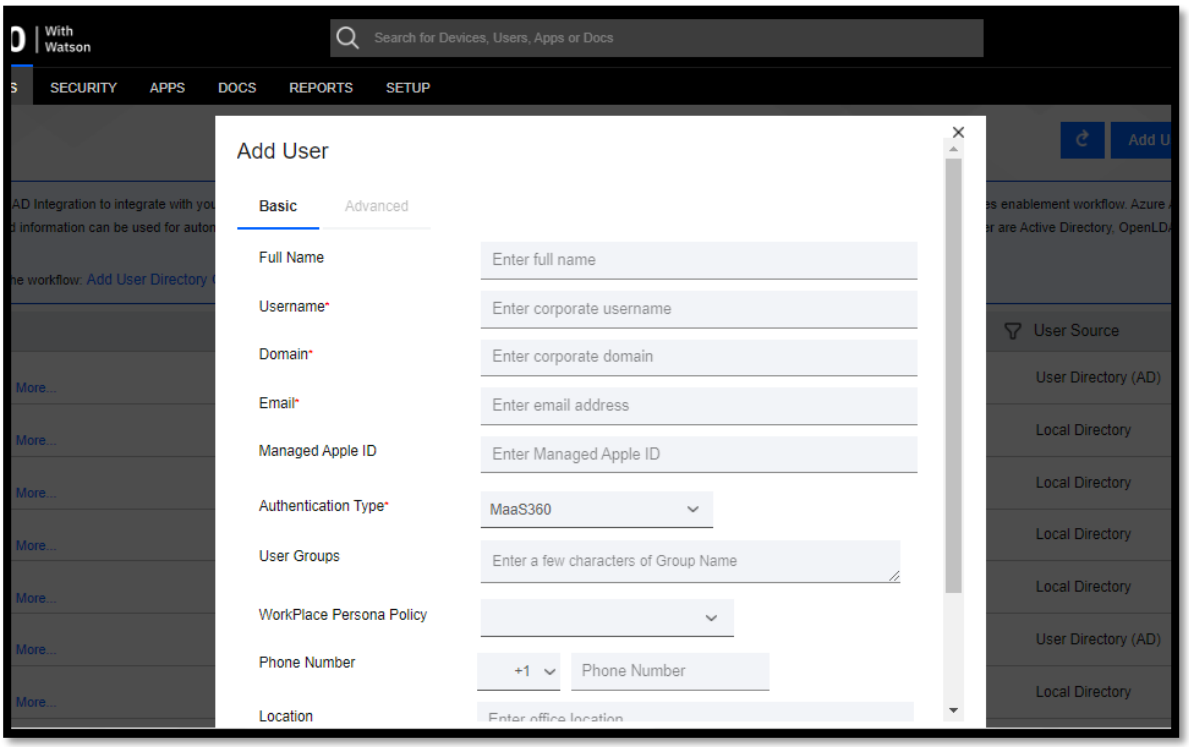
### 6.1.4 Users:

Users which are created in Maas360 are shown in user directory page. From the List view, you can take the following actions on users: filter, sort, search, delete, or export.

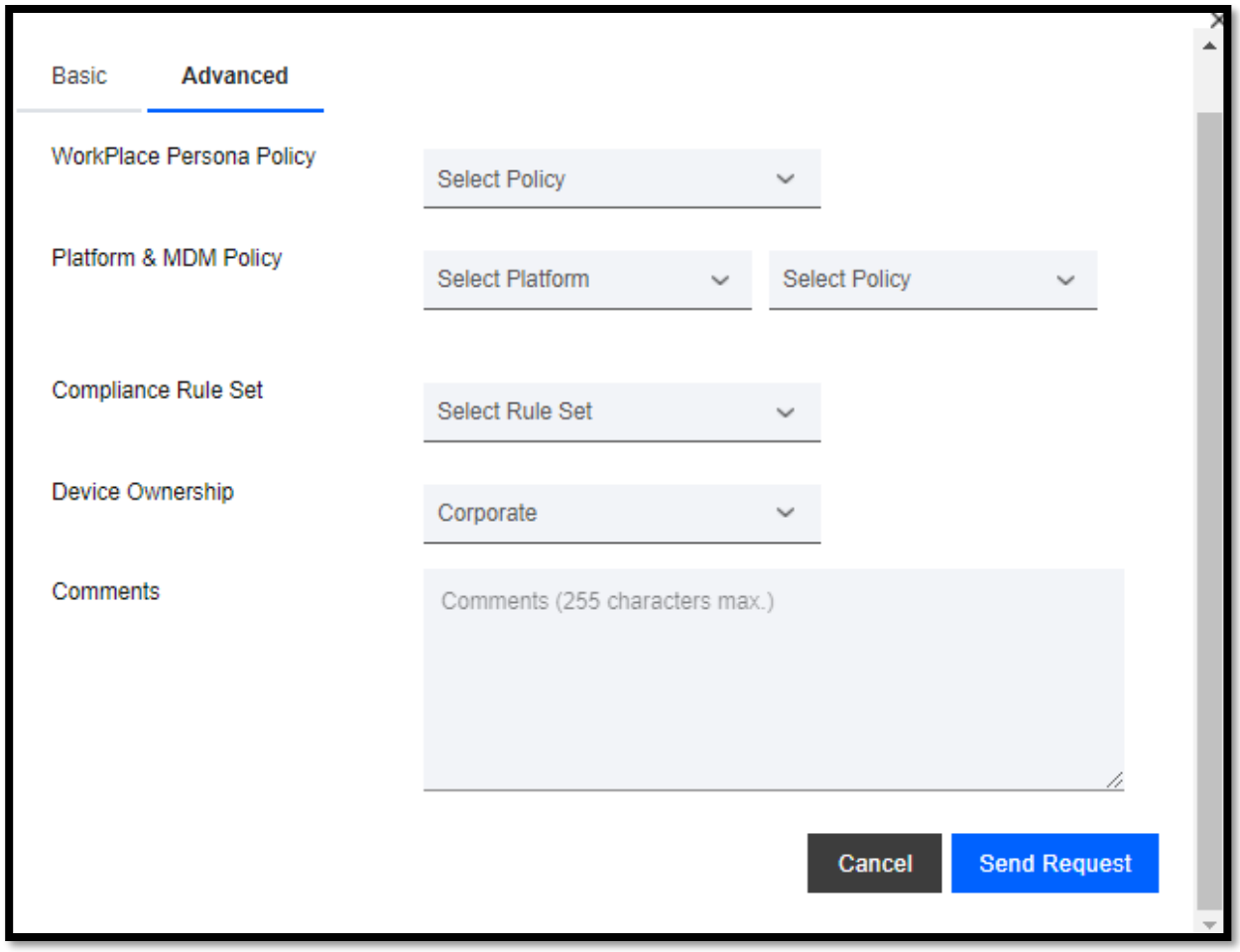
1. To navigate to user directory page. Go to, select Users > Directory. The User Directory page is displayed.




2. Click on Add User to add a user administrator. A pop-up window will appear, asking for basic user information. Select the basic tab and fill in information such as username, domain used by firm, email, if user has an Apple ID, authentication type, if we need to add user to a certain group directly, user groups, workspace persona policy, and phone number to contact user.



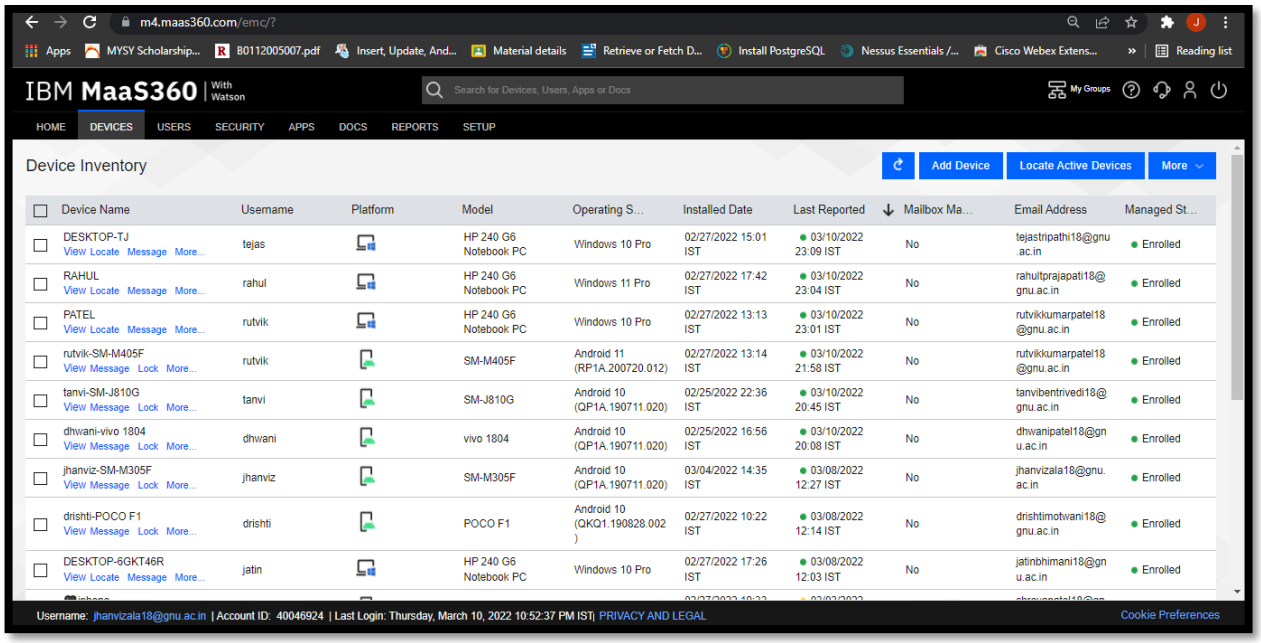
3. Now click on advanced tab. In this we have to give name of policy, platform and MDM policy, compliance rule set, device ownership and all information to configure user.



### 6.1.5 Devices:

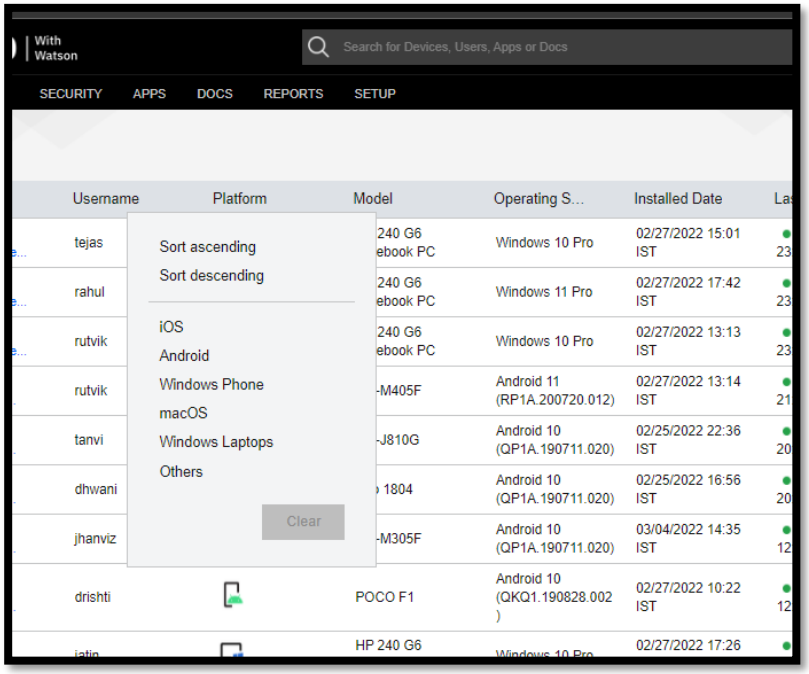
The Device Inventory page in the MaaS360 Portal lists all the devices added to MaaS360. List displayed here includes devices which are already registered or not registered in this portal. This list also includes devices which does not have user control, active or inactive devices.

1. To navigate to Device inventory, go to, select Devices > Inventory. The Device Inventory window is displayed. The page includes a device grid that displays device details in the respective columns in the grid.

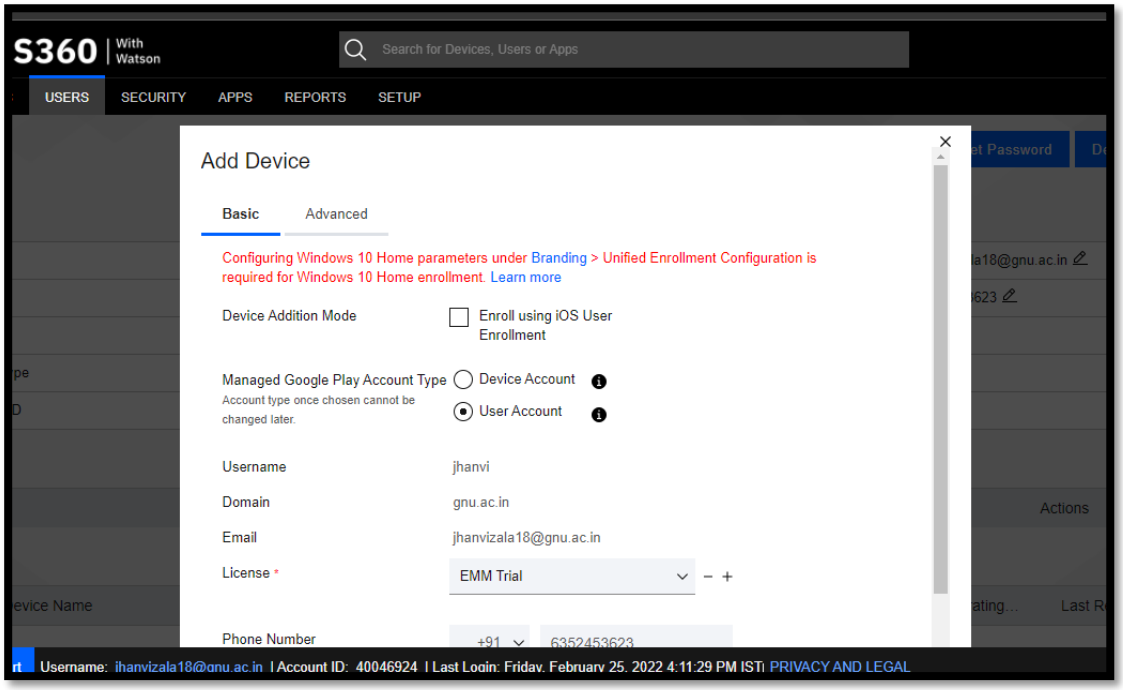



2. Review the list of devices, and choose one of the following options:

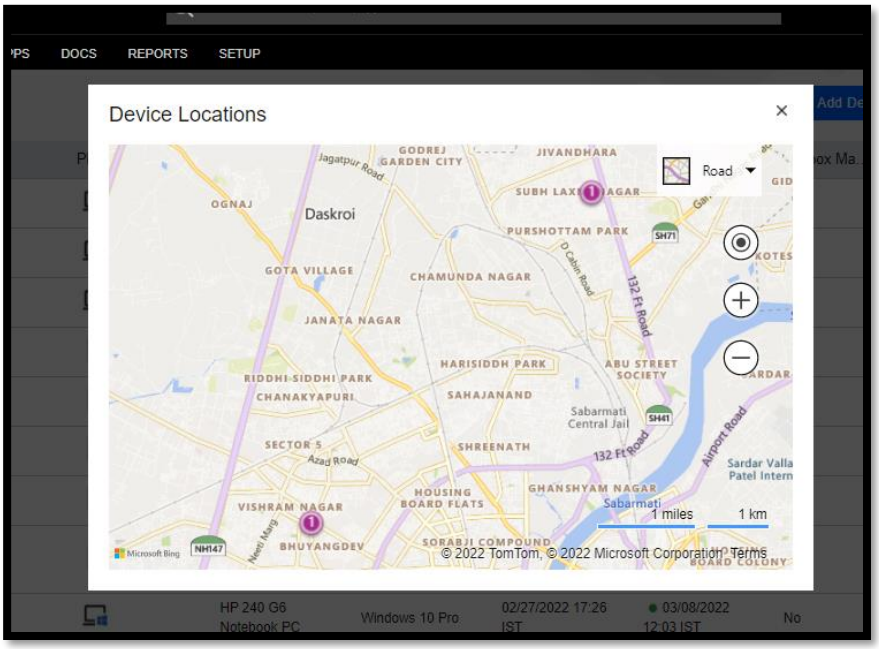
   - Select the column header and filter for a specific type of device. For example, select the Platform column and then sort devices based on the device operating system.



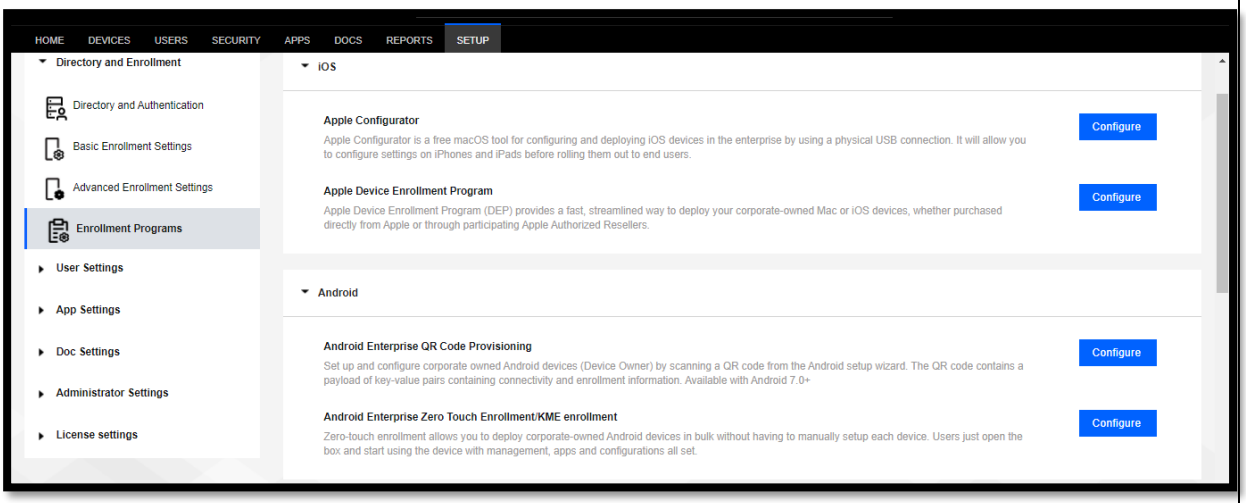
- Click the Refresh icon to refresh the list of devices.
- To add device from device inventory. Click on Add Device to send an enrollment request to a device. For more information about adding devices in MaaS360, see the Adding devices in MaaS360 topic.



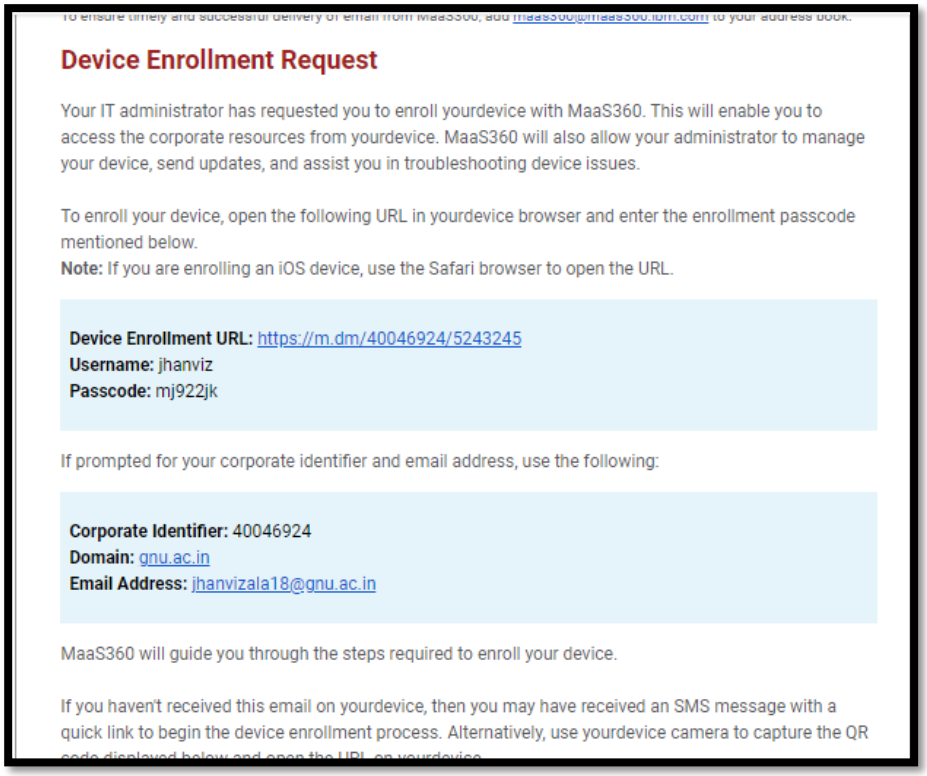

- To locate device, click Locate Active Devices to display it on a map. For more information about locating active devices, see the Locating active devices in the MaaS360 Portal topic.



- Click Delete Device to delete an inactive device.
- Click More > Directory and Enrollment to configure the default authentication mode, unified enrollment settings, advanced management settings, and more enrollment settings for iOS, Android, Windows, and other devices.




3. If we have added an android device. Then configuration of it is as follow:
    - After adding device user will get a passcode and URL to download IBM Maas360 in user email which they provide while creating user:



## Device Enrollment Request

Your IT administrator has requested you to enroll yourdevice with MaaS360. This will enable you to access the corporate resources from yourdevice. MaaS360 will also allow your administrator to manage your device, send updates, and assist you in troubleshooting device issues.

To enroll your device, open the following URL in yourdevice browser and enter the enrollment passcode mentioned below.
**Note:** If you are enrolling an iOS device, use the Safari browser to open the URL.

**Device Enrollment URL:** https://m.dm/40046924/5243245
**Username:** jhanviz
**Passcode:** mj922jk

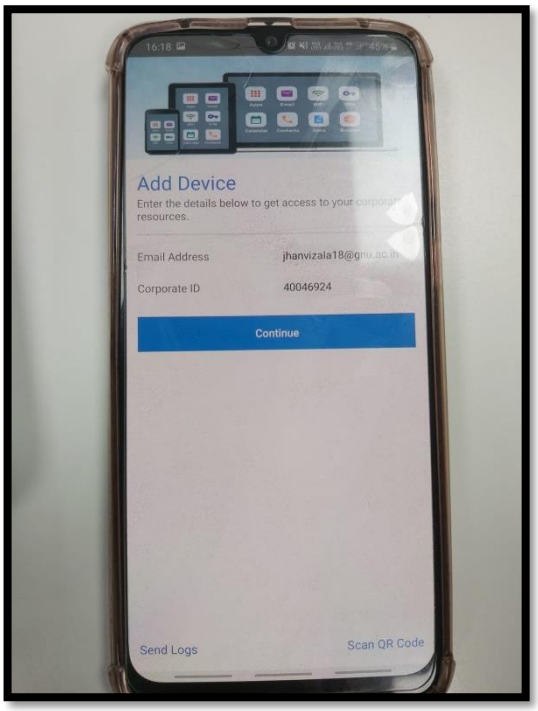
If prompted for your corporate identifier and email address, use the following:

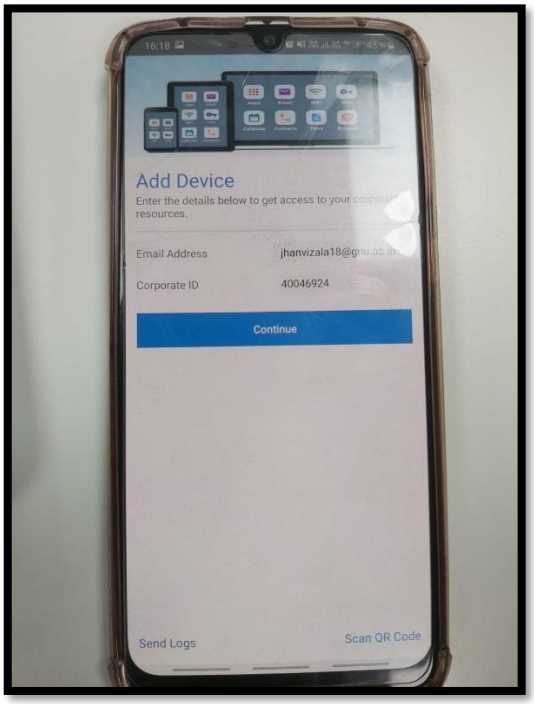
**Corporate Identifier:** 40046924
**Domain:** gnu.ac.in
**Email Address:** jhanvizala18@gnu.ac.in

MaaS360 will guide you through the steps required to enroll your device.

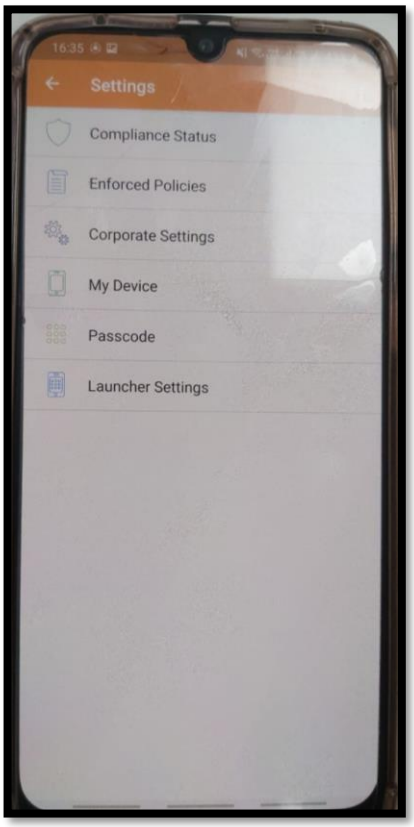
If you haven't received this email on yourdevice, then you may have received an SMS message with a quick link to begin the device enrollment process. Alternatively, use yourdevice camera to capture the QR

- Now after downloading IBM Maas360, while installing application we need to enter passcode and continue



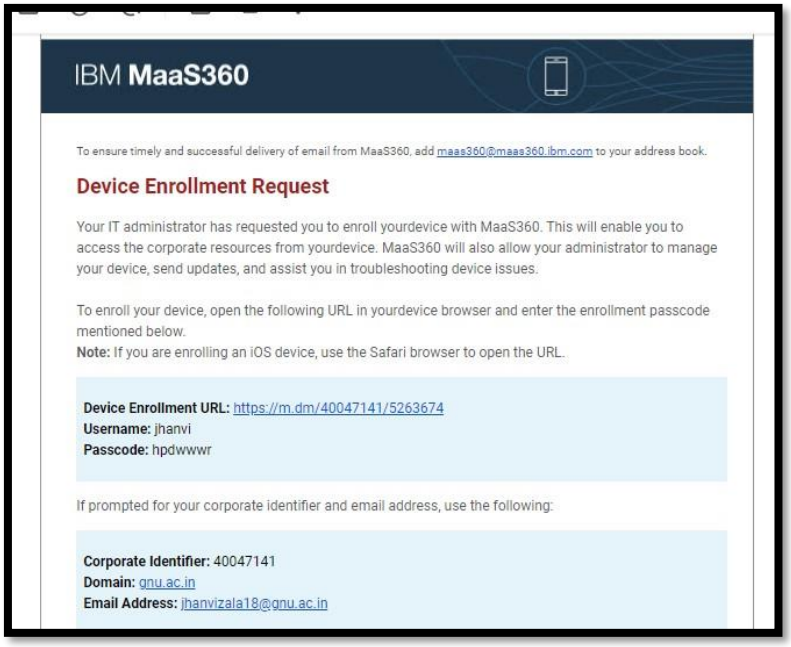




- After installing it we get application of settings and in that we are having compliance status, already enforced policy, corporate settings, my device information, passcode, launcher settings:

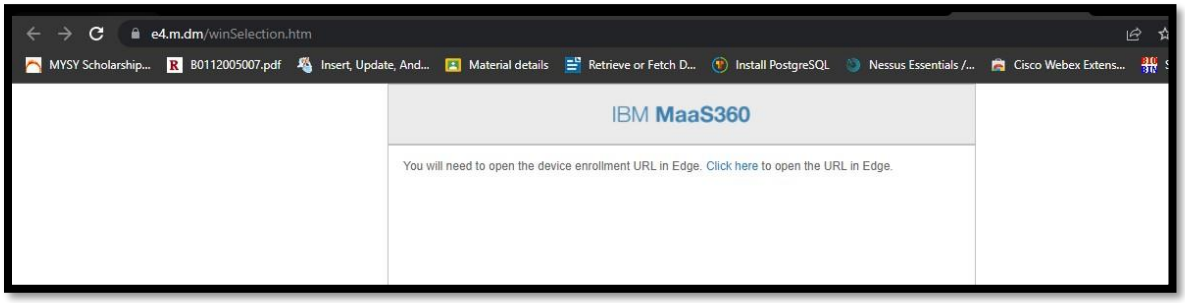




If we have to add device in windows devices. Then configuration is as follow

a. First it will send email to added device user. There it is having a link:




b. Now click on link and it will ask to download application IBM Maas360 from microsoft:




c. After entering passcode and configure it as user:


MaaS360
IBM MaaS360
Browser
App Catalog
Messages
Settings

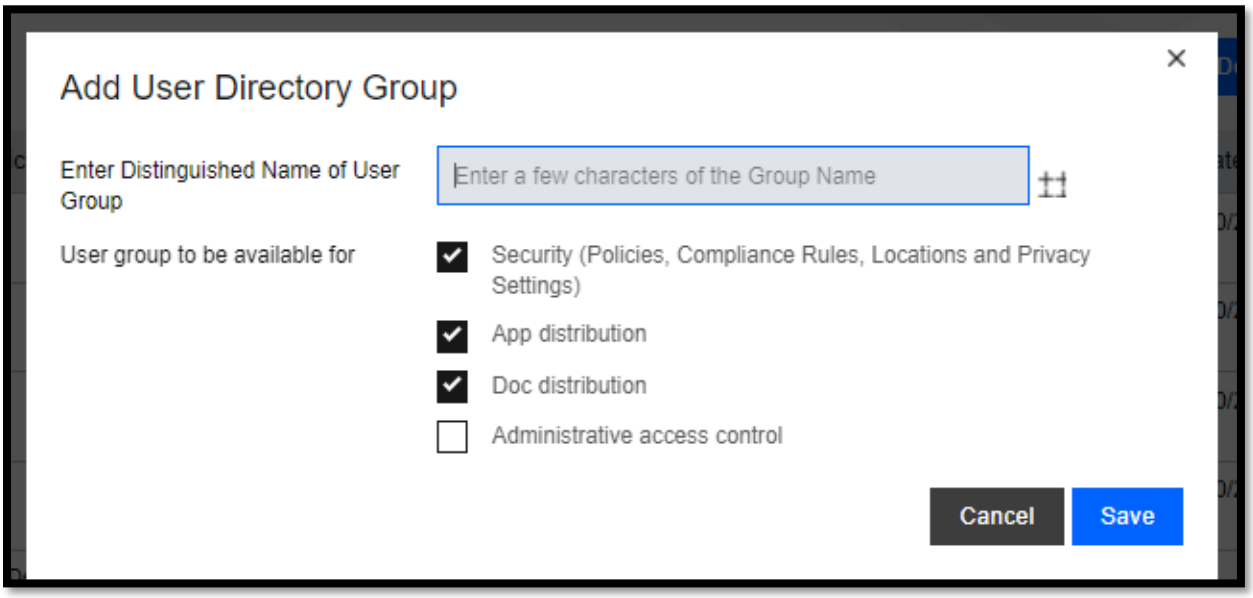
### 6.1.6 Groups:

A group of users is known as user groups and a group of devices is known as device groups. You cannot take all actions on both groups. For example, the Execute Shell Scripts action is available only for a device group. Follow these steps to deploy policies, apps, or documents to a group in the MaaS360 Portal.

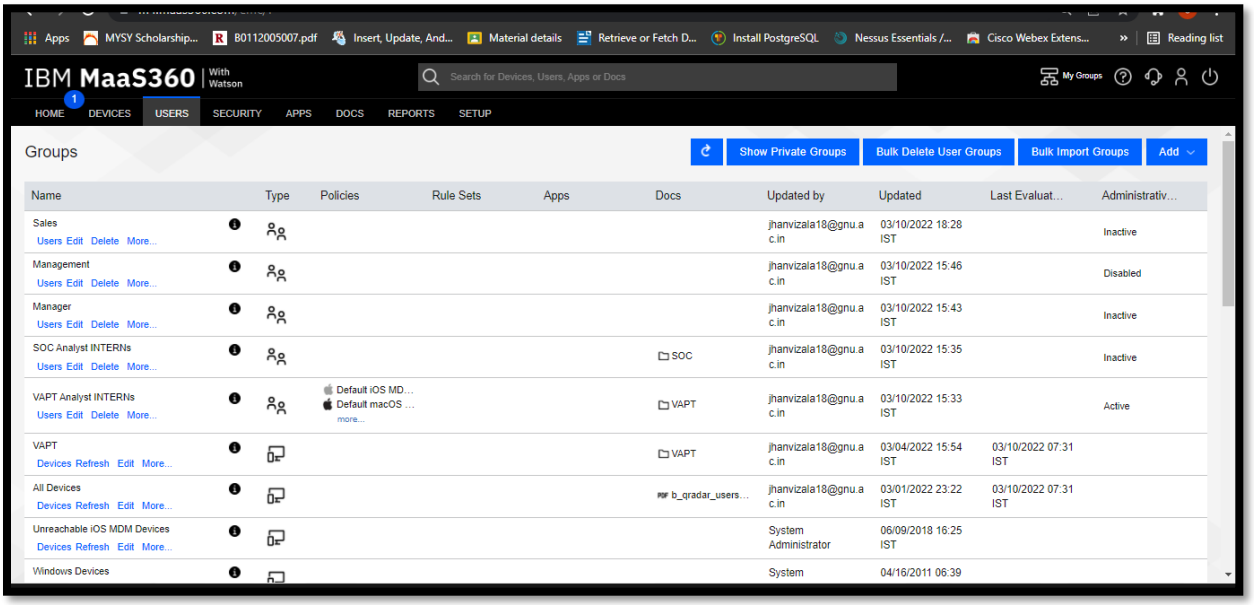
**Adding user directory group:**

For organizations with a large number of users, an administrator can use departmentalization to manage LDAP/AD user groups in MaaS360 and take actions on those user groups. The global administrator manages users in a department, and can also create and maintain departments within the same MaaS360 customer account for other administrators such as the business unit administrator or the portal administrator.

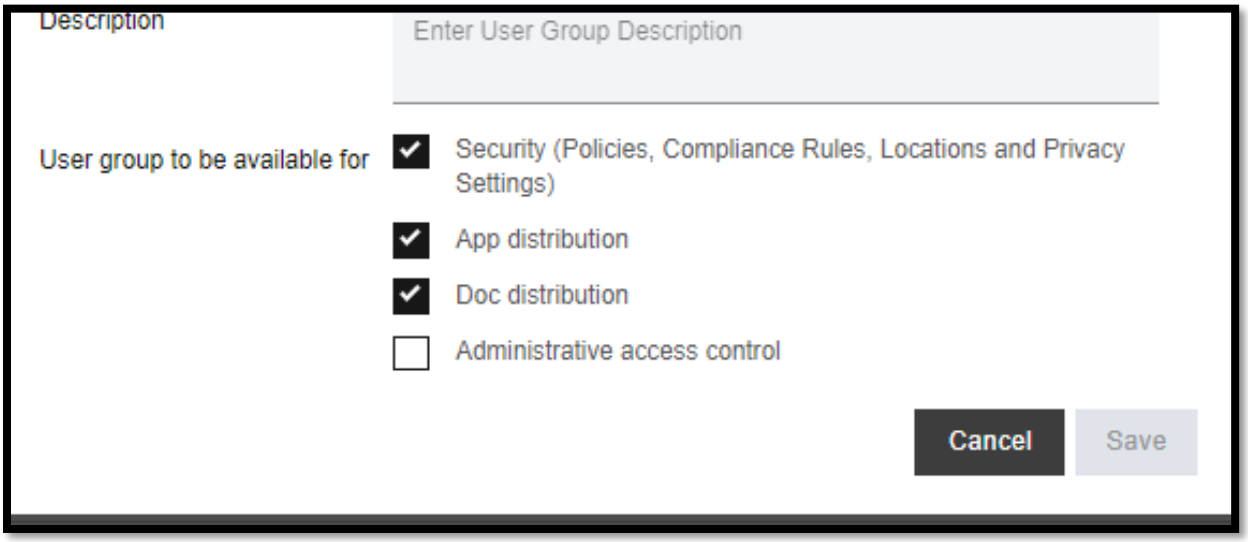
1. From the MaaS360 Portal Home page, choose one of the following methods to add a user directory group:
    a. Select Users > Directory. The User Directory page is displayed.
    b. Click More > Add User Directory Group.
    c. Select Users > Groups. The Groups page is displayed.
    d. Click Add > User Directory Group.
2. Enter the names for the existing user directory groups that you want to import into the MaaS360 Portal.



In this after this we are able to get information in main tab:




So to remove group from disabled setting we need to give administrative access control:

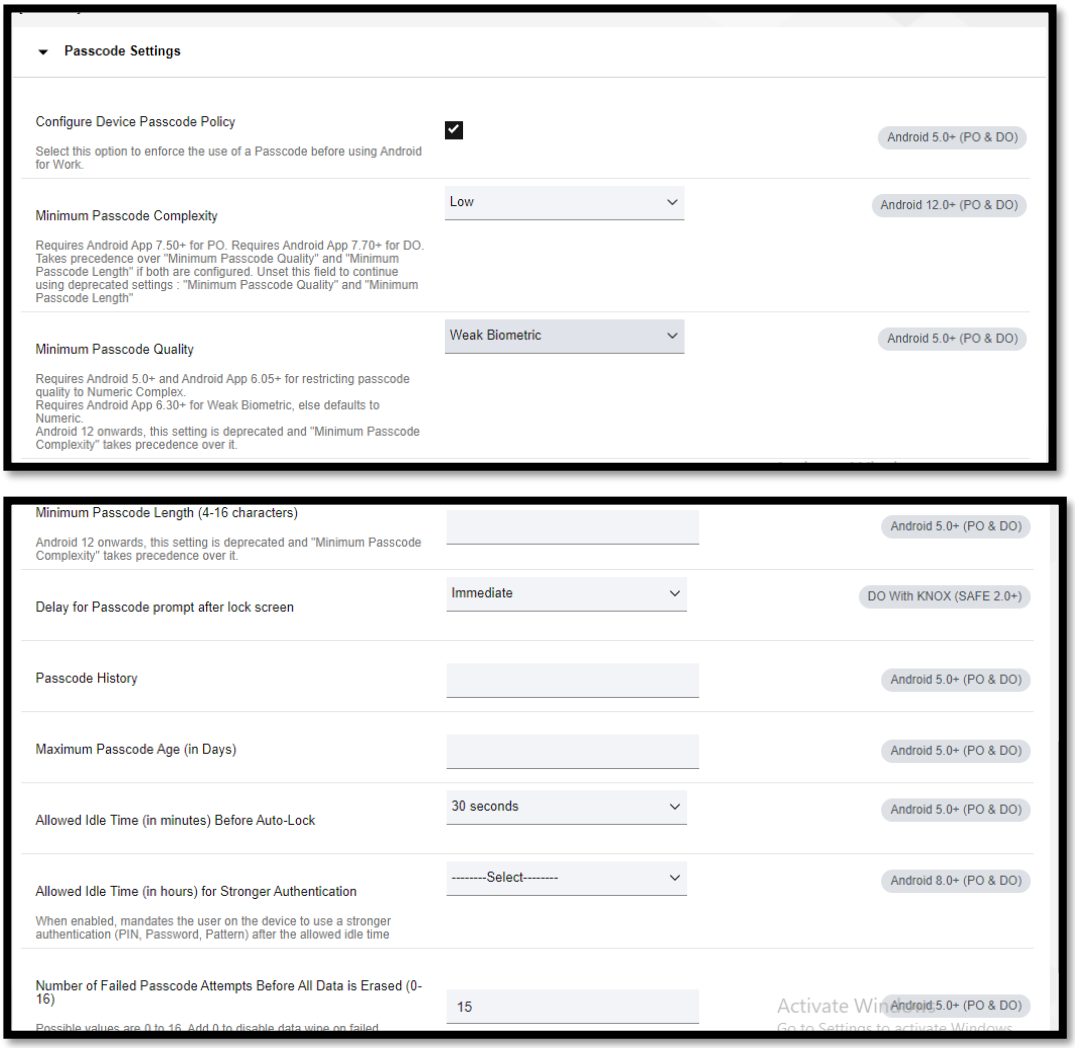



Now to activate group, add one administrator in that group which can check all activities of that group.

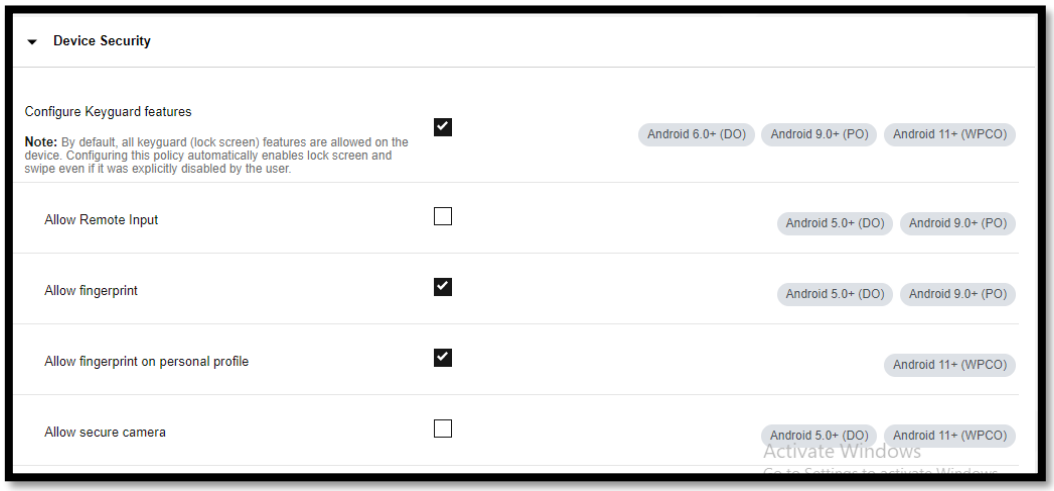
## 6.2 Security

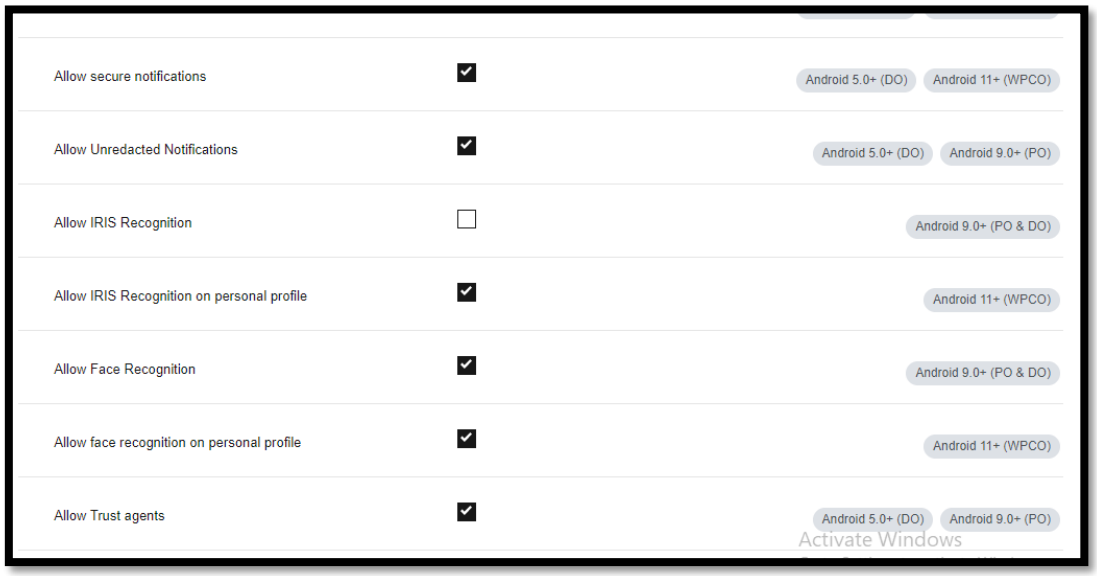
### 6.2.1 Policies: Configuring Android MDM Policy for VAPT users

1. We will start with Passcode settings.
    - Configure Device Passcode Policy: Enable
    - Minimum passcode complexity: Low
    - Minimum passcode Quality: Weak Biometric
    - Allowed idle time: 30sec
    - Number of failed passcode attempts allowed: 15

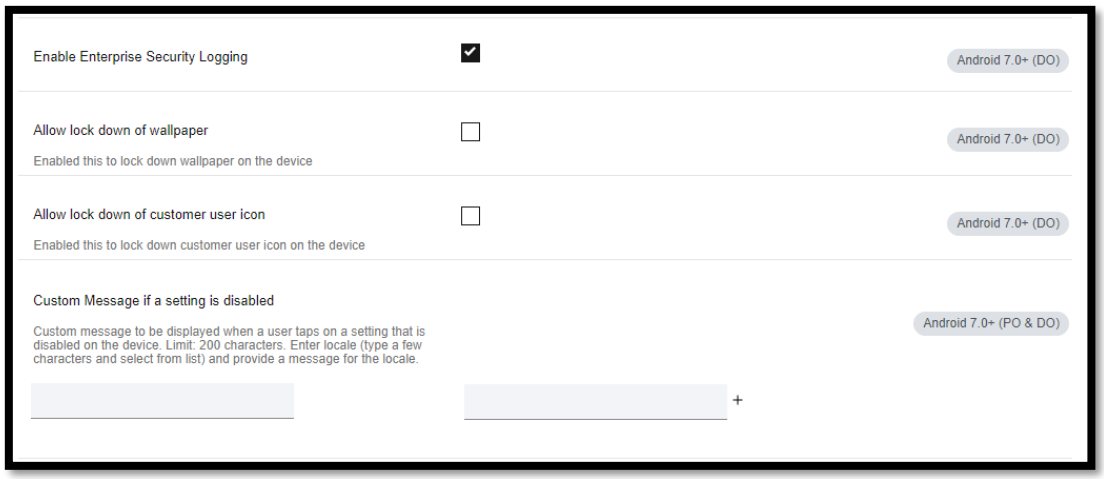


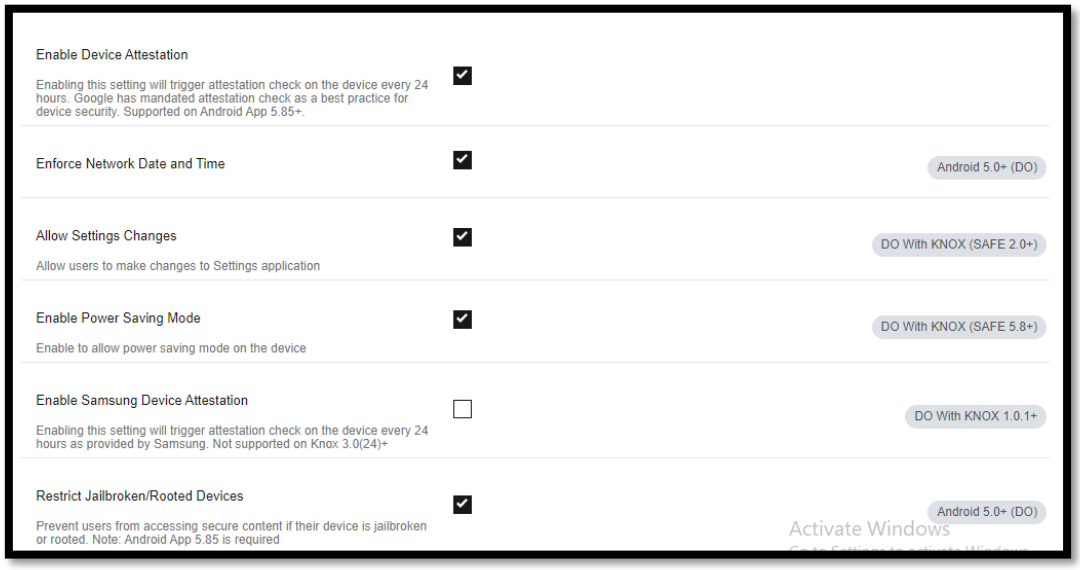
2. Continuing with security settings
   - Configure keyguard features: Enable
   - Allow Remote Input: Disable
   - Allow secure camera: Disable
   - Allow secure notification: Enable
   - Allow IRIS Recognition: Disable
   - Allow removal of user profile: Disable
   - Allow boot of device in safe mode: Disable
   - Enterprise security logging: Enable
   - Restrict Jailbroken/ Rooted Device: Enable
   - Mark device as non-compliant if location permissions are not given: Enable
   - USB Transfer: Disable
   - USB Debugging: Disable
   - Mounting of physical media: Disable
   - Allow screen capture on personal profile: Disable
   - Allow Share List" Disable
   - Allow clipboard sharing: Within work profile
   - Allow work events on personal calendar: Do not allow

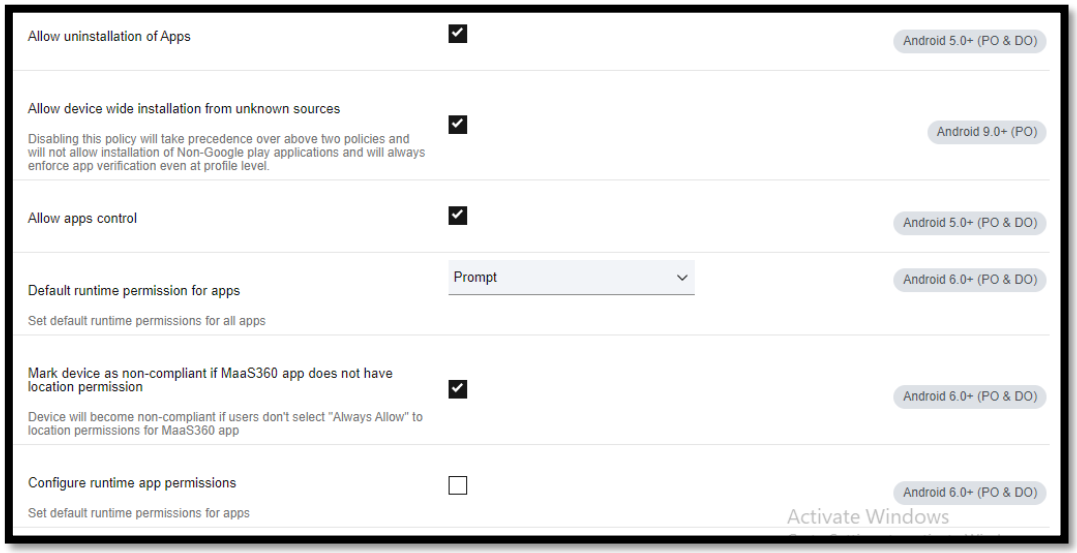


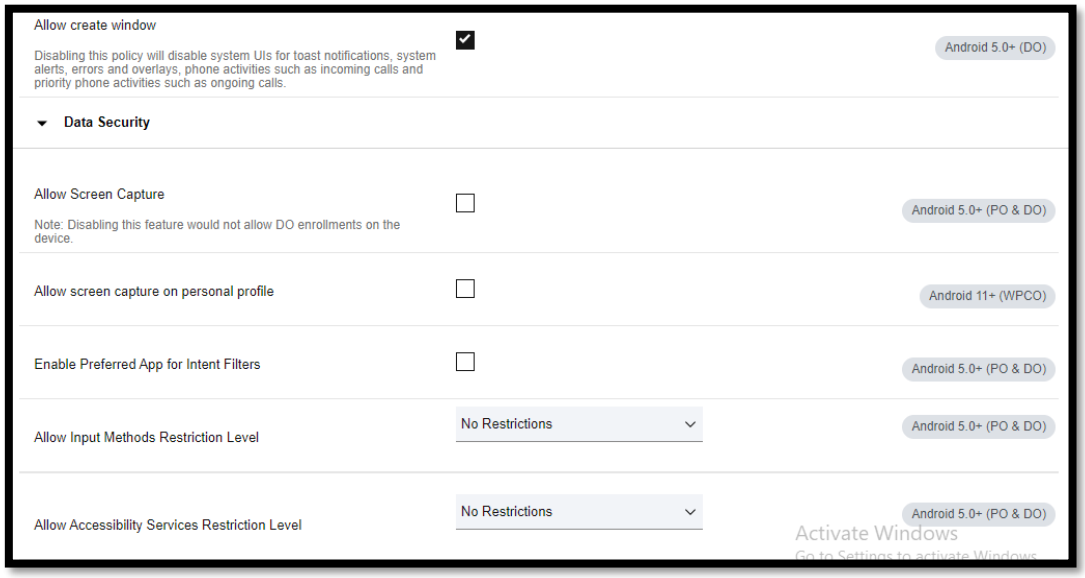

Allow trust agents on personal profile
Android 11+ (WPCO)
Allow boot of device in Safe mode
Android 6.0+ (DO)
Allow Factory reset
Android 5.0+ (DO)
Allow configuration of credentials
Android 5.0+ (DO)
Allow User profile creation
Android 5.0+ (DO)
Allow removal of user profile
Android 5.0+ (DO)
Allow modification of accounts
Android 5.0+ (PO & DO)
Activate Windows

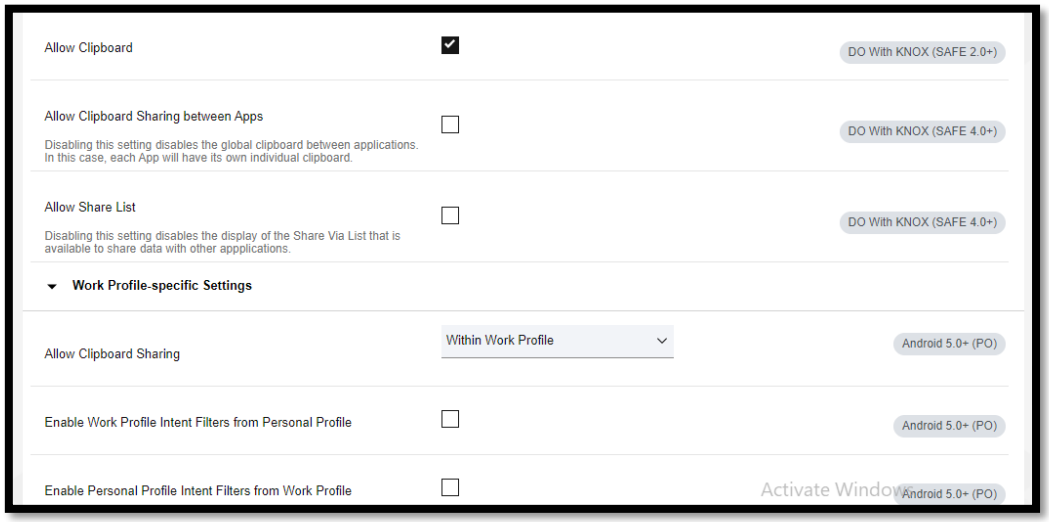

Enable Enterprise Security Logging
Android 7.0+ (DO)
Allow lock down of wallpaper
Enabled this to lock down wallpaper on the device
Android 7.0+ (DO)
Allow lock down of customer user icon
Enabled this to lock down customer user icon on the device
Android 7.0+ (DO)
Custom Message if a setting is disabled
Custom message to be displayed when a user taps on a setting that is disabled on the device. Limit: 200 characters. Enter locale (type a few characters and select from list) and provide a message for the locale.
Android 7.0+ (PO & DO)
+

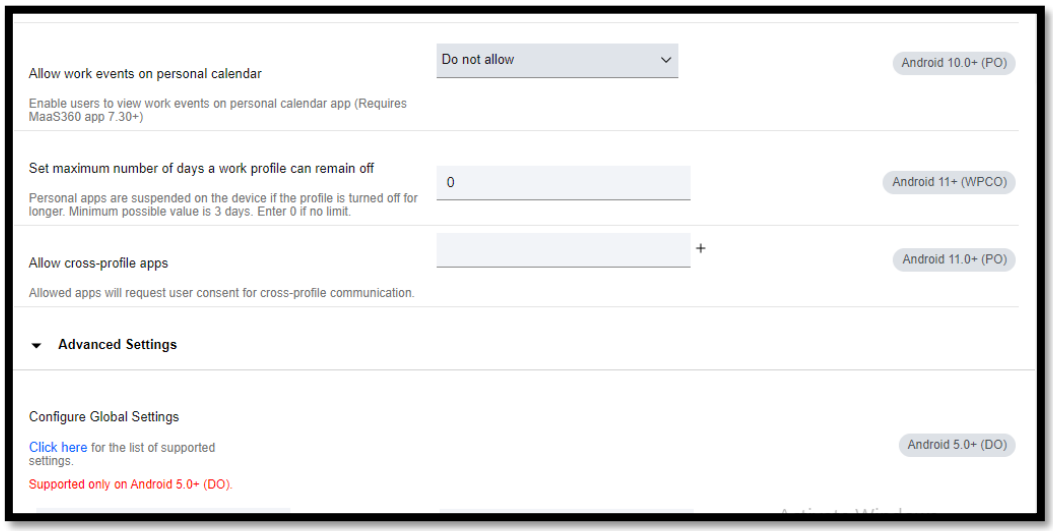

Enable Device Attestation
Enabling this setting will trigger attestation check on the device every 24 hours. Google has mandated attestation check as a best practice for device security. Supported on Android App 5.85+.
Enforce Network Date and Time
Android 5.0+ (DO)
Allow Settings Changes
Allow users to make changes to Settings application
DO With KNOX (SAFE 2.0+)
Enable Power Saving Mode
Enable to allow power saving mode on the device
DO With KNOX (SAFE 5.8+)
Enable Samsung Device Attestation
Enabling this setting will trigger attestation check on the device every 24 hours as provided by Samsung. Not supported on Knox 3.0(24)+
DO With KNOX 1.0.1+
Restrict Jailbroken/Rooted Devices
Prevent users from accessing secure content if their device is jailbroken or rooted. Note: Android App 5.85 is required
Android 5.0+ (DO)
Activate Windows


Allow uninstallation of Apps
Android 5.0+ (PO & DO)
Allow device wide installation from unknown sources
Disabling this policy will take precedence over above two policies and will not allow installation of Non-Google play applications and will always enforce app verification even at profile level.
Android 9.0+ (PO)
Allow apps control
Android 5.0+ (PO & DO)
Default runtime permission for apps
Prompt
Android 6.0+ (PO & DO)
Set default runtime permissions for all apps
Mark device as non-compliant if MaaS360 app does not have location permission
Device will become non-compliant if users don't select "Always Allow" to location permissions for MaaS360 app
Android 6.0+ (PO & DO)
Configure runtime app permissions
Android 6.0+ (PO & DO)
Set default runtime permissions for apps
Activate Windows

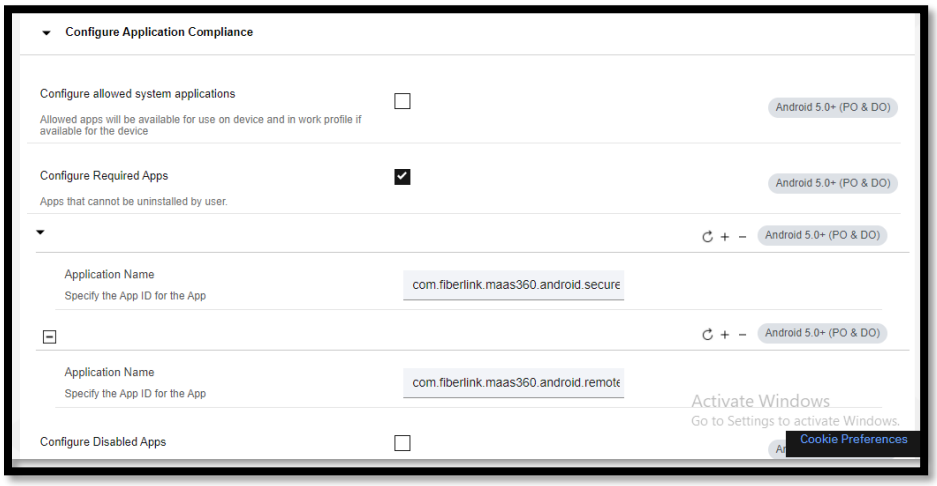

Allow Notifications
DO With KNOX (SAFE 3.0)
Developer Option
Allow USB file transfer
Android 5.0+ (DO)
Android 11+ (WPCO)
Allow USB Debugging
Android 5.0+ (PO & DO)
Allow mounting of physical media
Android 5.0+ (DO)
Android 11+ (WPCO)
Activate Windows

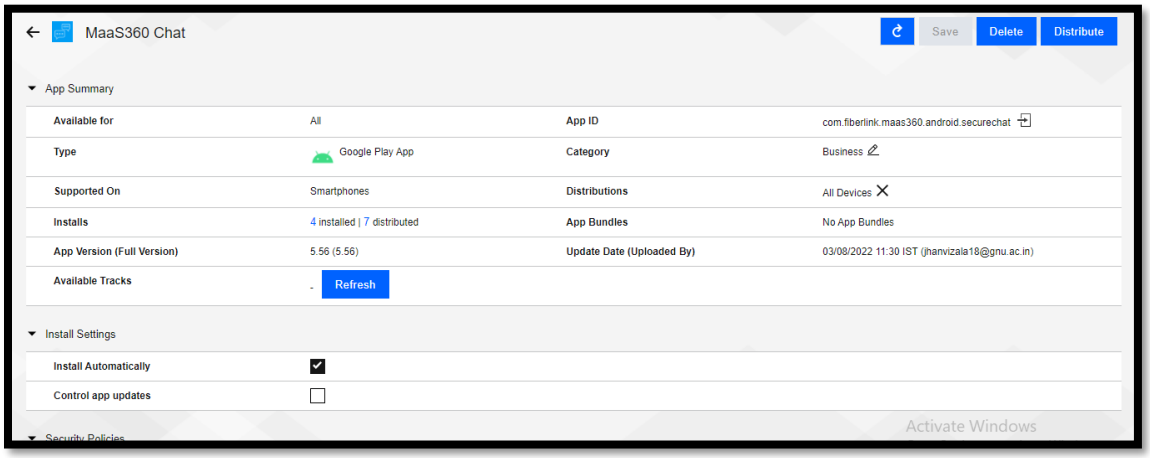

Allow create window
Disabling this policy will disable system UIs for toast notifications, system alerts, errors and overlays, phone activities such as incoming calls and priority phone activities such as ongoing calls.
Android 5.0+ (DO)
Data Security
Allow Screen Capture
Note: Disabling this feature would not allow DO enrollments on the device.
Android 5.0+ (PO & DO)
Allow screen capture on personal profile
Android 11+ (WPCO)
Enable Preferred App for Intent Filters
Android 5.0+ (PO & DO)
Allow Input Methods Restriction Level
No Restrictions
Android 5.0+ (PO & DO)
Allow Accessibility Services Restriction Level
No Restrictions
Android 5.0+ (PO & DO)
Activate Windows

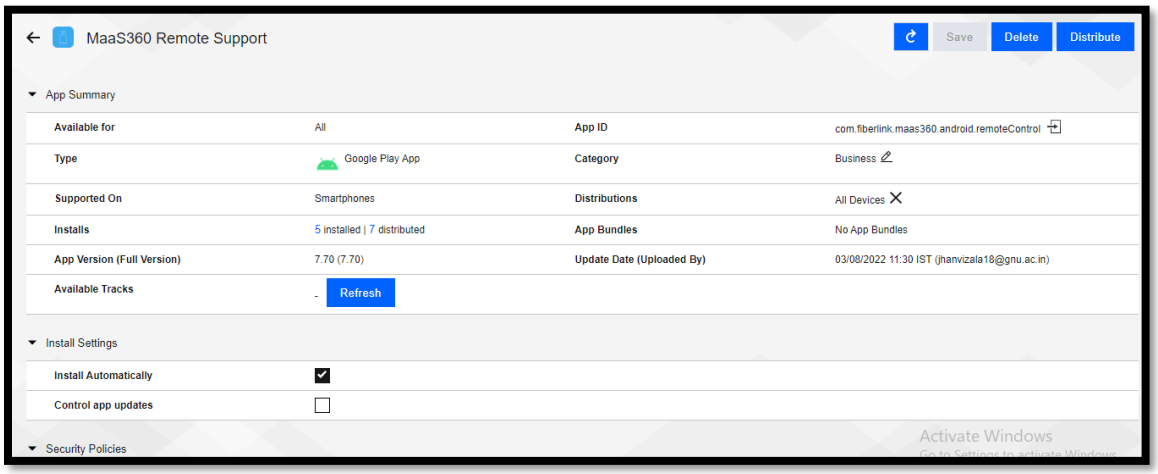


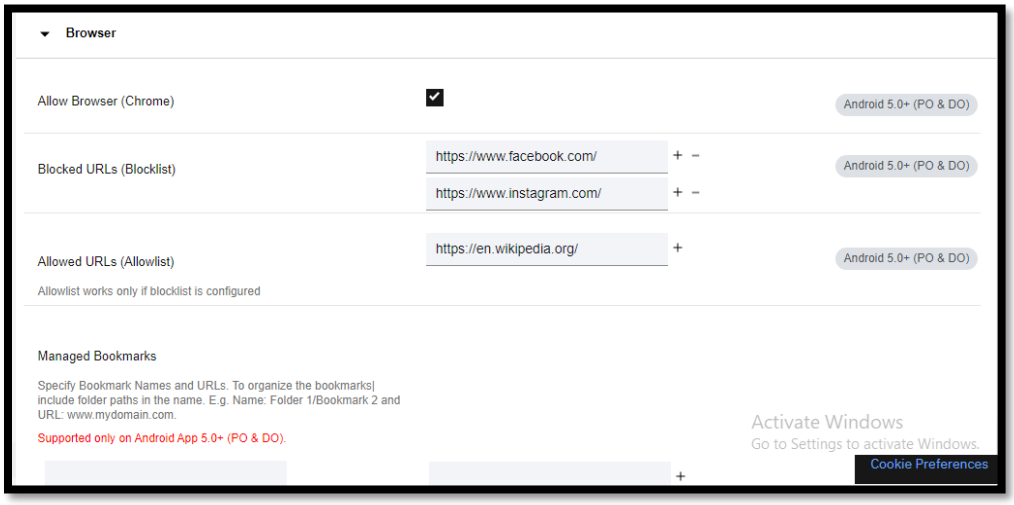

3. Configuring App compliance
    - Configure Required Apps:
        - Maas360 Chat
        - Maas360 Remote Support



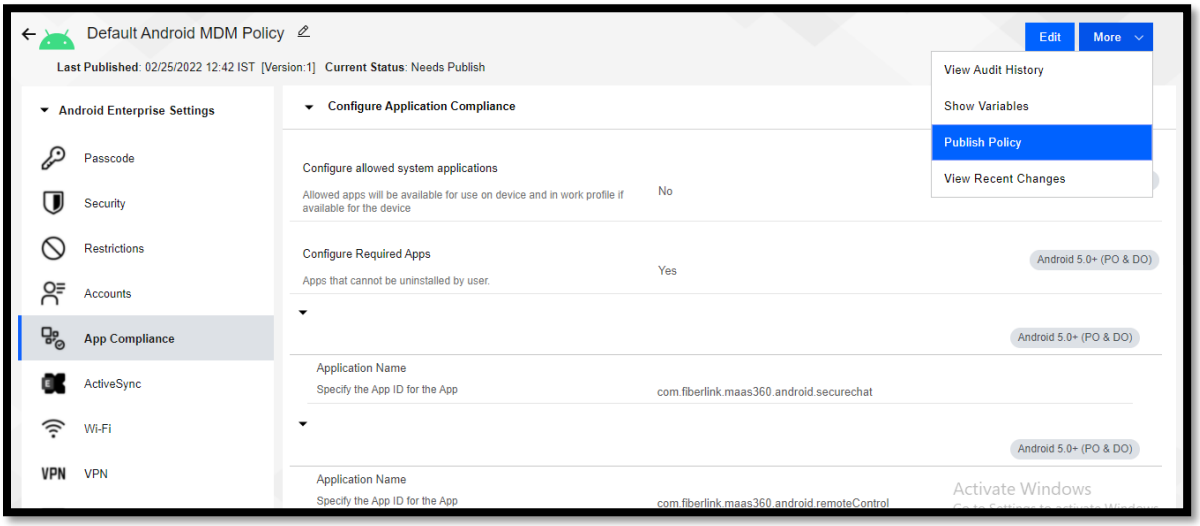


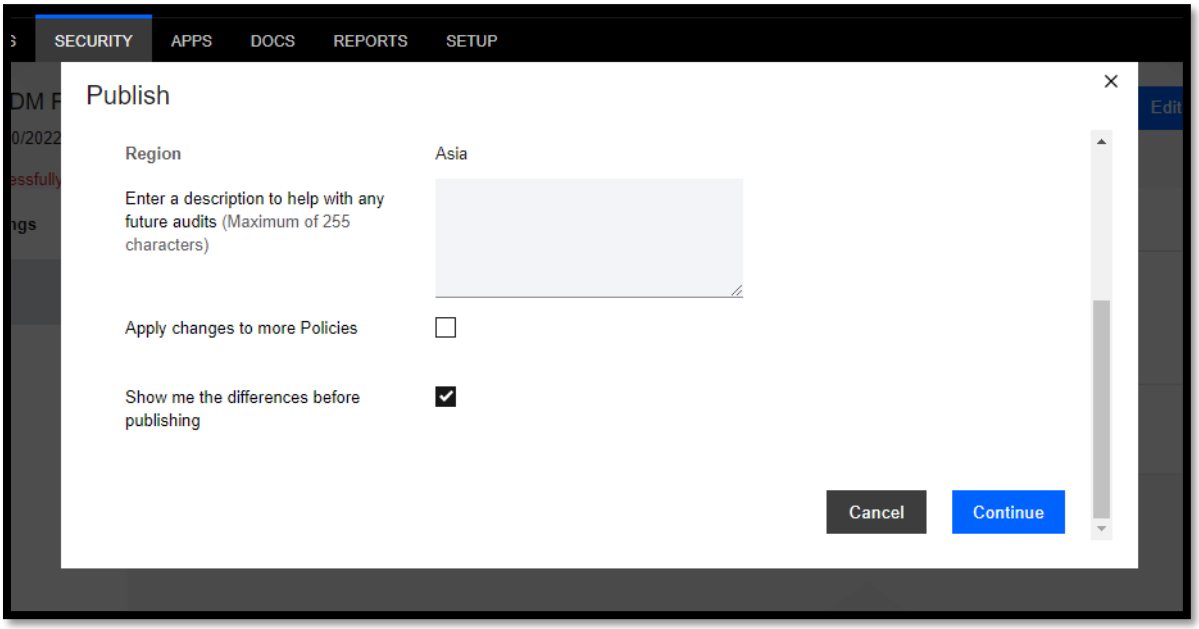




4. Brower Settings
    - Allow Browser (Chrome): Enable
    - Blocked URLs:
        - https://www.facebook.com
        - https://www.instagram.com
    - Allowed URLs:
        - https://en.wikipedia.org/

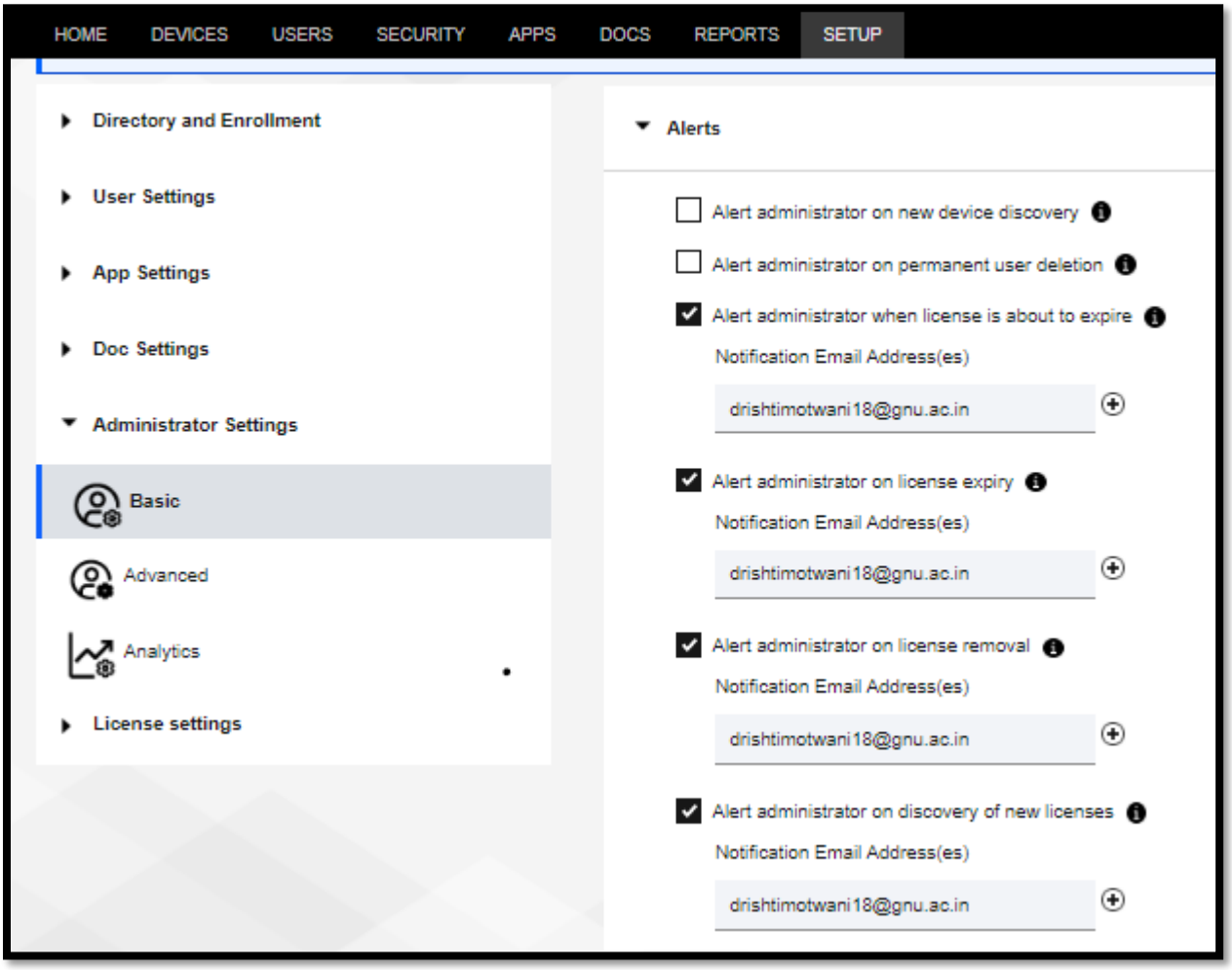


5. Save the policy and publish.



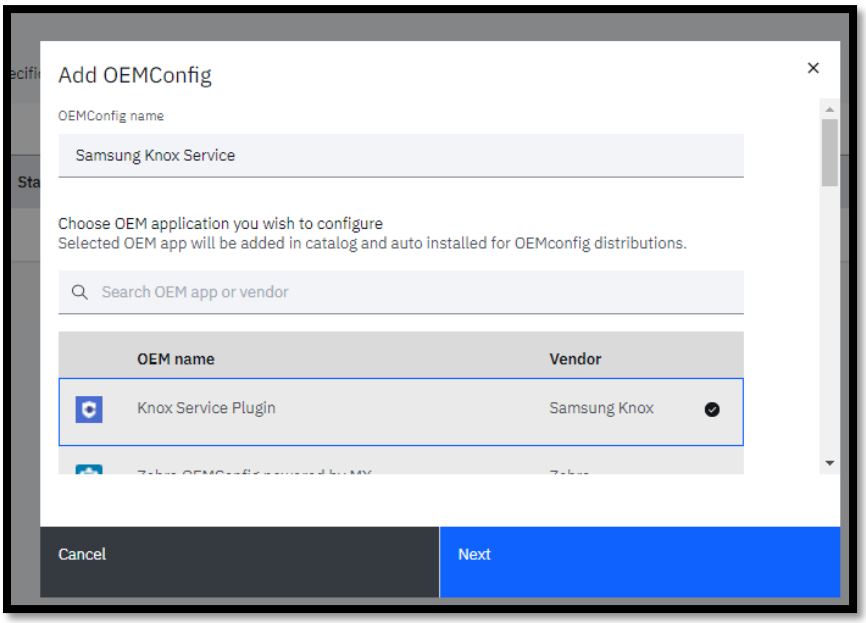



### 6.2.2 Administrative settings:

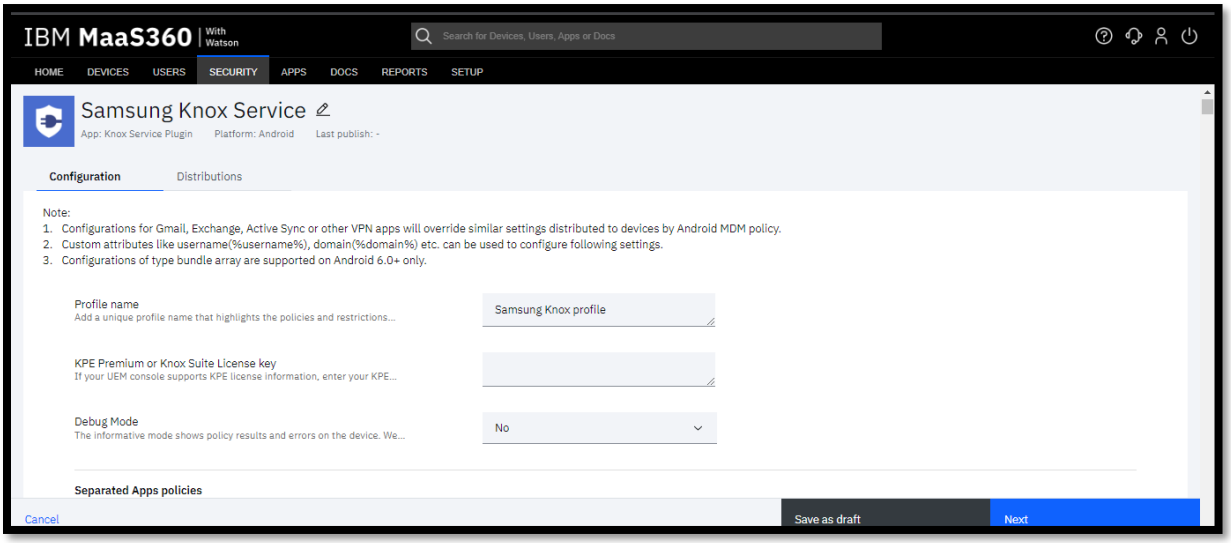


### 6.2.3 Android OEM Config:

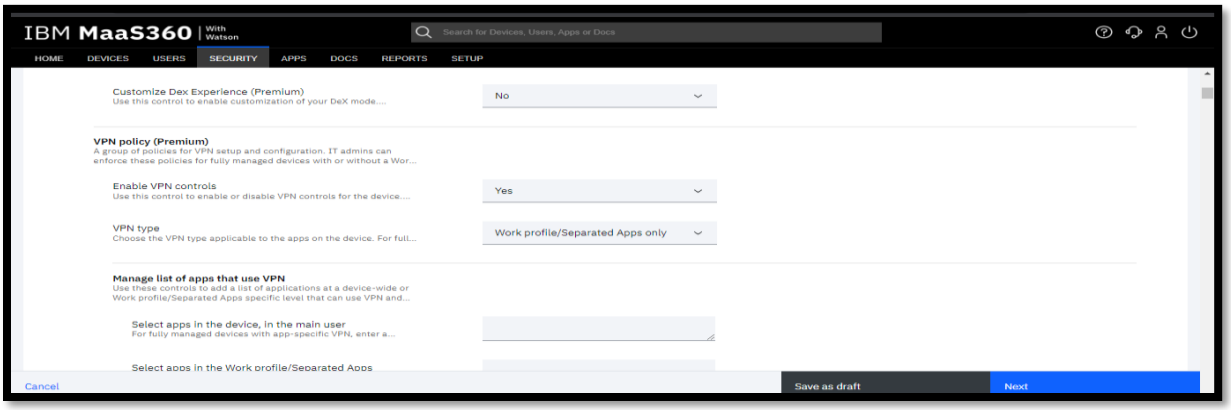
1. Enter the OEM Config name and search for the suitable service name using the OEM name or the vendor's name.



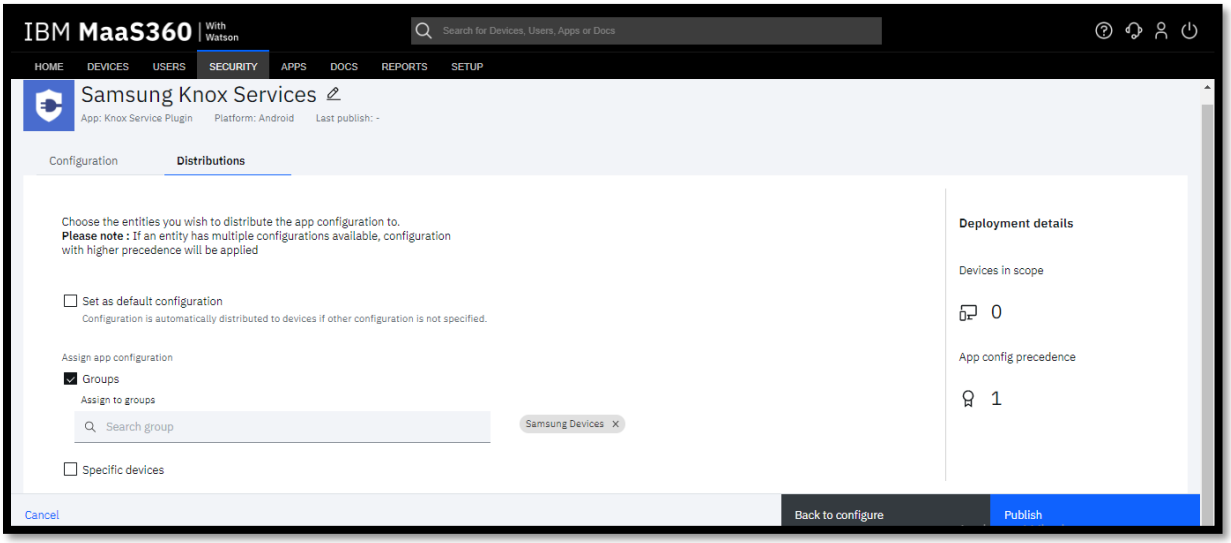

2. Assign profile name.

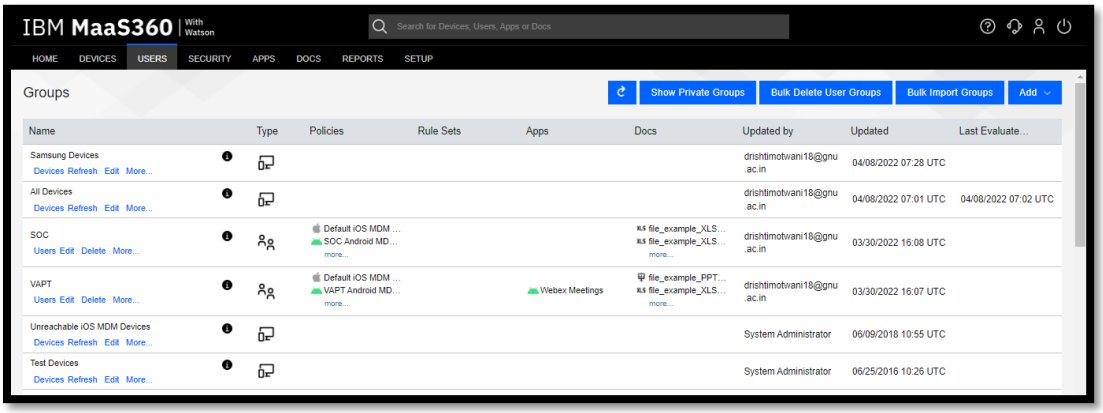



3. Configure settings according to requirement. Here, we enable VPN controls inside work profile.

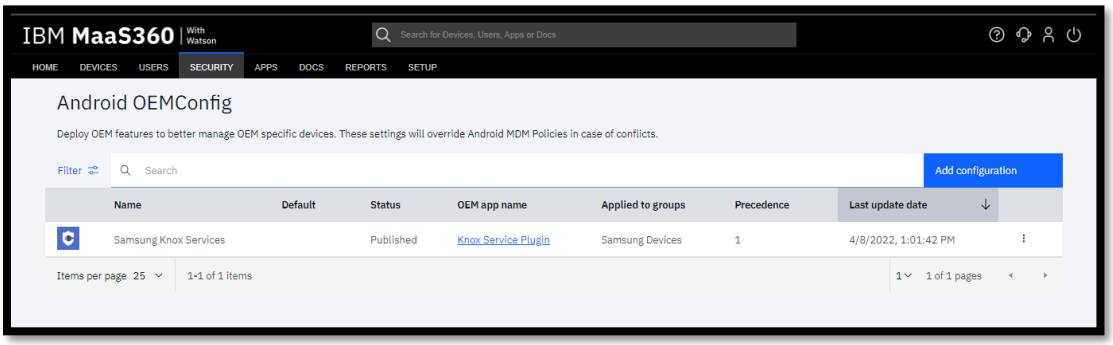


4. Decide and distribute the service among desired group, here we made a group of android Samsung devices and assigned this service to it.



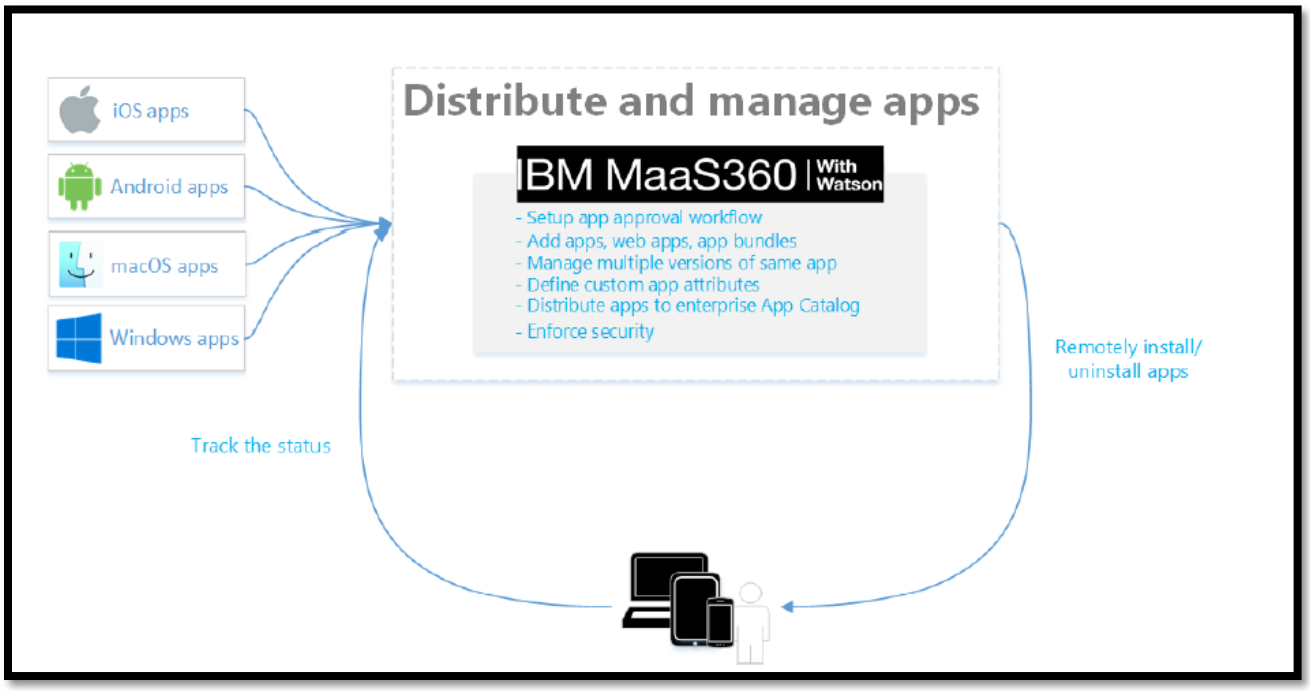




5. Publish the service.

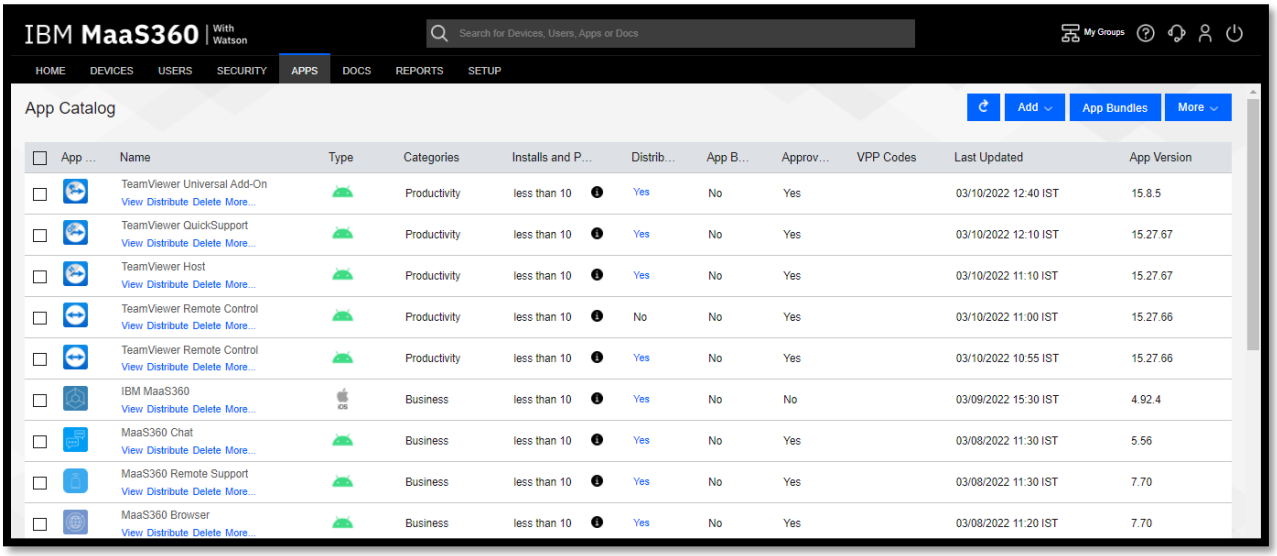


### 6.3 Mobile Application Management:

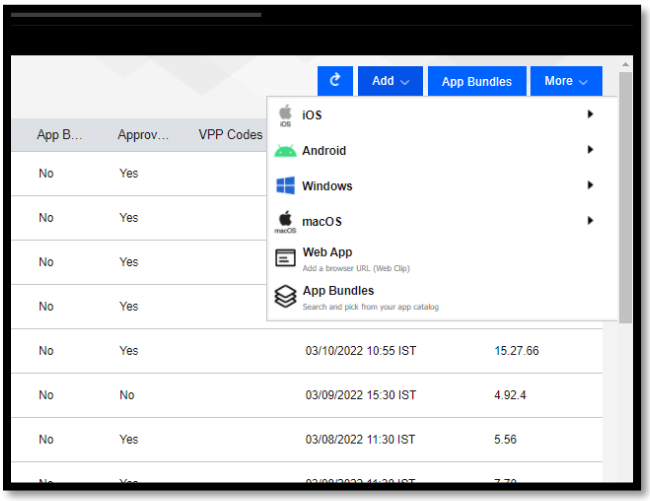
The MaaS360 App Catalog is a collection of public (store) and private (bought) apps, as well as enterprise (custom made) and web apps. For your company workforce, the App Catalog delivers a complete app management lifecycle. The App Catalog can be used to remotely control apps on both personal and business devices. MaaS360 has a number of capabilities that let you add, deploy, upgrade, protect, and manage apps throughout your company.



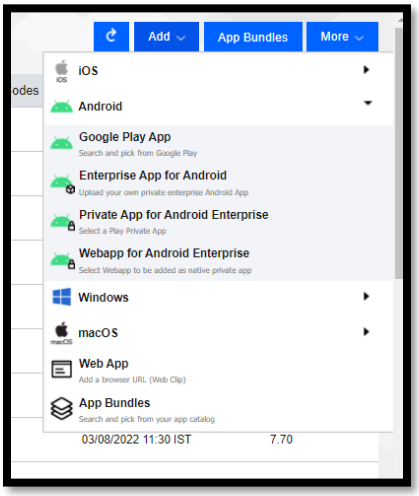

1. From the MaaS360 Portal Home page, select Apps > Catalog.



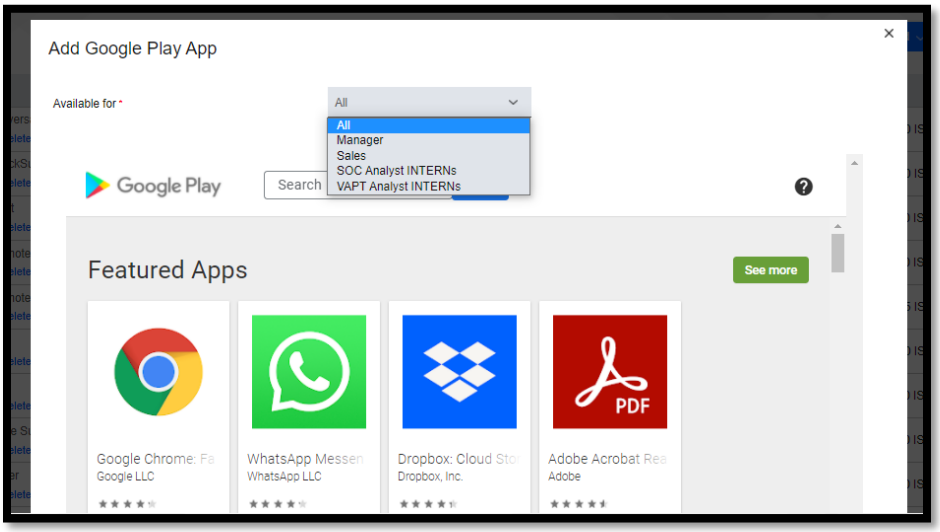
2. To add application click on add. There we are having different section iOS, android, Windows, macOS, web application, app bundles:



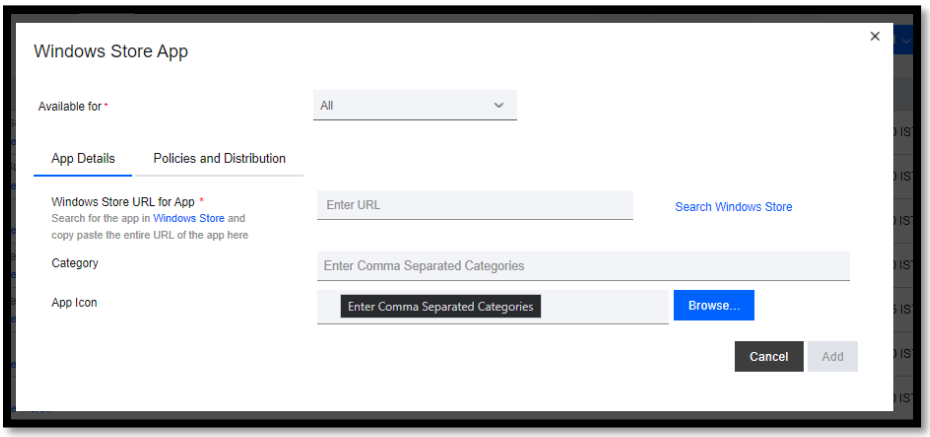

3. Now here, we have added application for android devices. So expand android section. In that add we have options to add application through google app, enterprise application for android, private app for android application, webapp for android enterprise.



4. Now we are adding application from google play app. So in that we have to choose for which group we have to deploy this application:

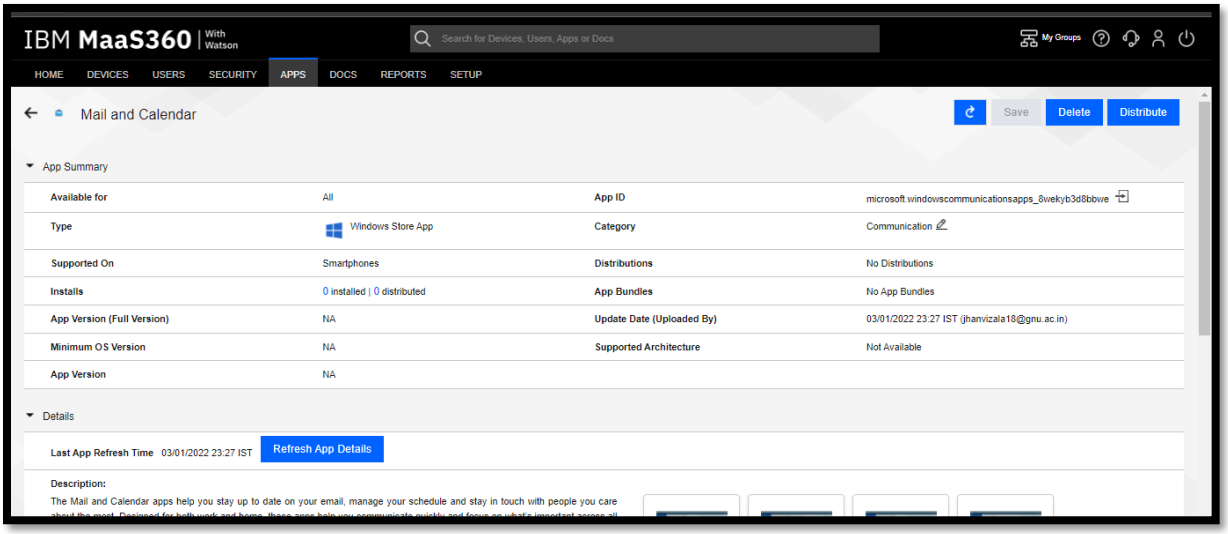



5. To deploy application in windows select windows->windows store app:

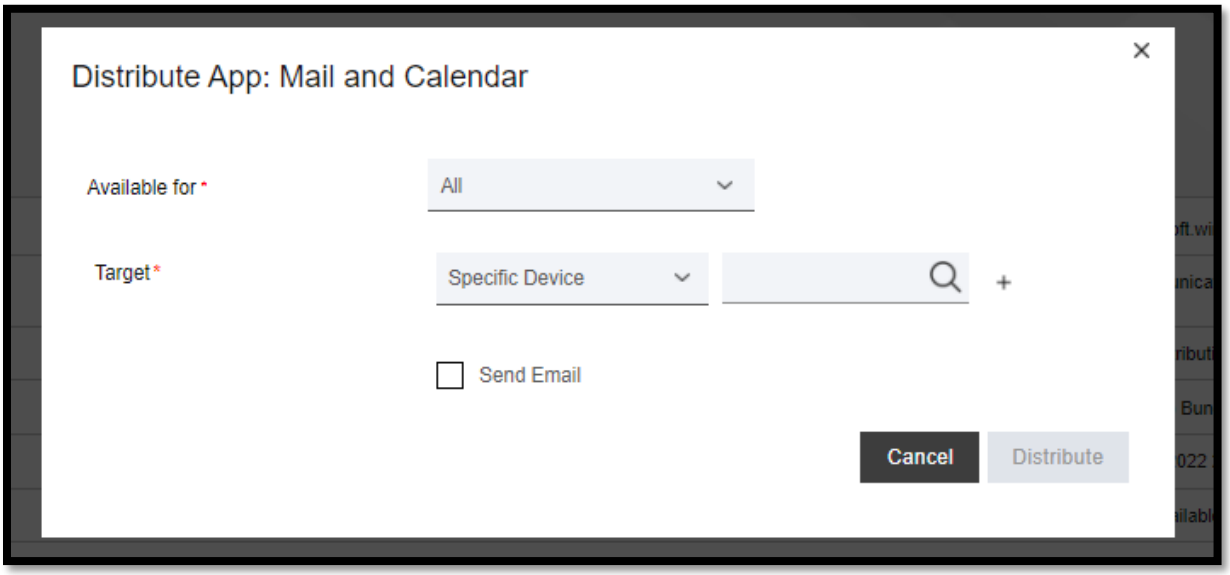


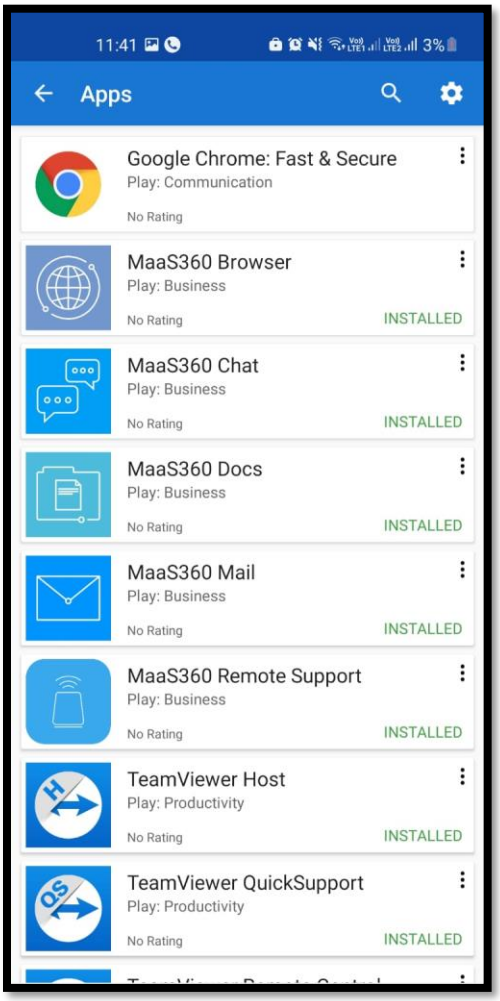

To distribute application which is added throught above process.

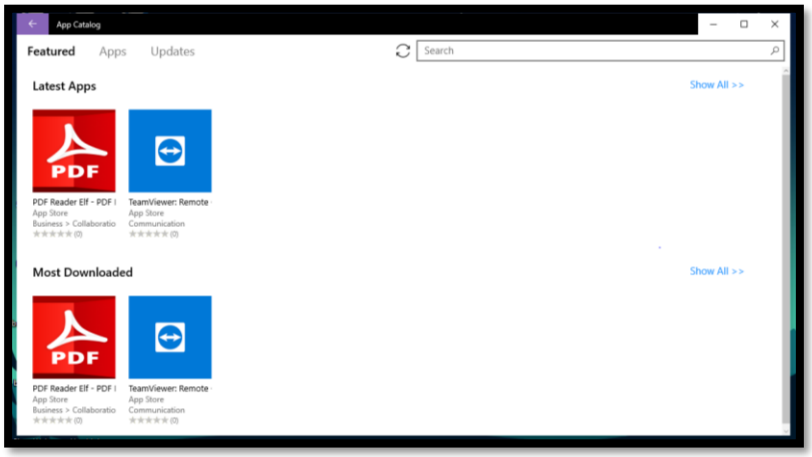
Click on view of that application and then click on distribute button:




Here after clicking on distribute it will ask to which group we want to distribute this applciation and also to which particular device or group we want to distribute:




11:41
3%
Apps
Google Chrome: Fast & Secure
Play: Communication
No Rating
MaaS360 Browser
Play: Business
No Rating
INSTALLED
MaaS360 Chat
Play: Business
No Rating
INSTALLED
MaaS360 Docs
Play: Business
No Rating
INSTALLED
MaaS360 Mail
Play: Business
No Rating
INSTALLED
MaaS360 Remote Support
Play: Business
No Rating
INSTALLED
TeamViewer Host
Play: Productivity
No Rating
INSTALLED
TeamViewer QuickSupport
Play: Productivity
No Rating
INSTALLED


App Catalog
Featured
Apps
Updates
Search
Latest Apps
Show All >>
PDF Reader Elf - PDF I
App Store
Business > Collaboratio
TeamViewer: Remote
App Store
Communication
Most Downloaded
Show All >>
PDF Reader Elf - PDF I
App Store
Business > Collaboratio
TeamViewer: Remote
App Store
Communication

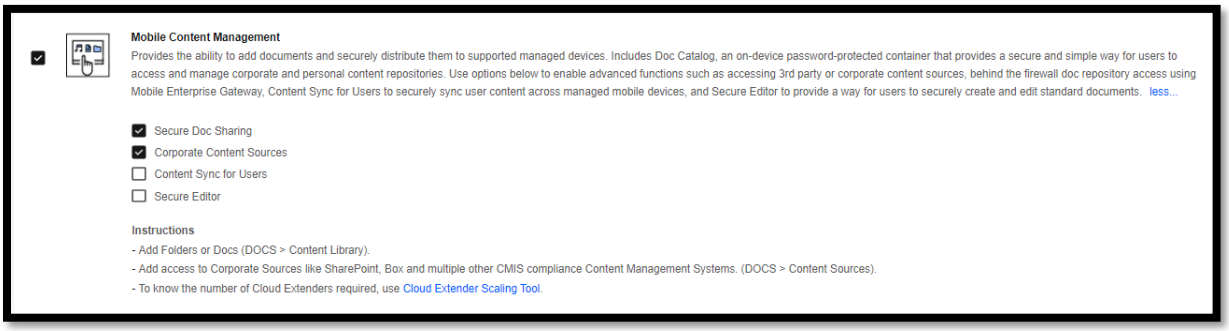
## 6.4 Mobile Content Management:

Users may access corporate documents more securely on their mobile devices with IBM MaaS360 Mobile Content Management, which provides content management and control in an encrypted container.

You may create security controls for documents and distribute them to individuals, groups, or devices using MaaS360 Mobile Content Management. Through data loss prevention (DLP) and other policy settings, documents maintained with this software can be version controlled, audited, and secured.

The following are some of the capabilities and benefits of MaaS360 Mobile Content Management:

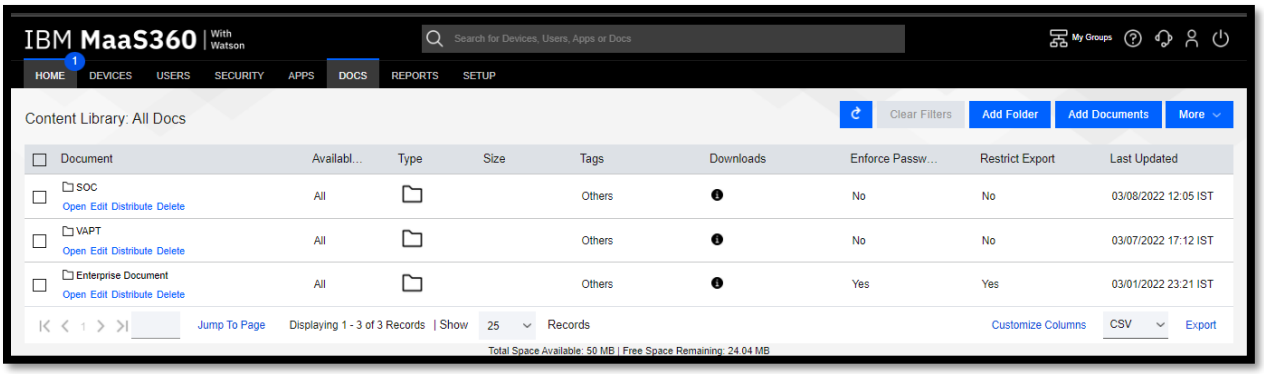
- Enterprise document catalogue to allow users to access and read documents on mobile devices in a secure manner.
- Document lifecycle management to help streamline and standardise workflows.
- Document and file protection and data leakage prevention through compliance and enforcement.



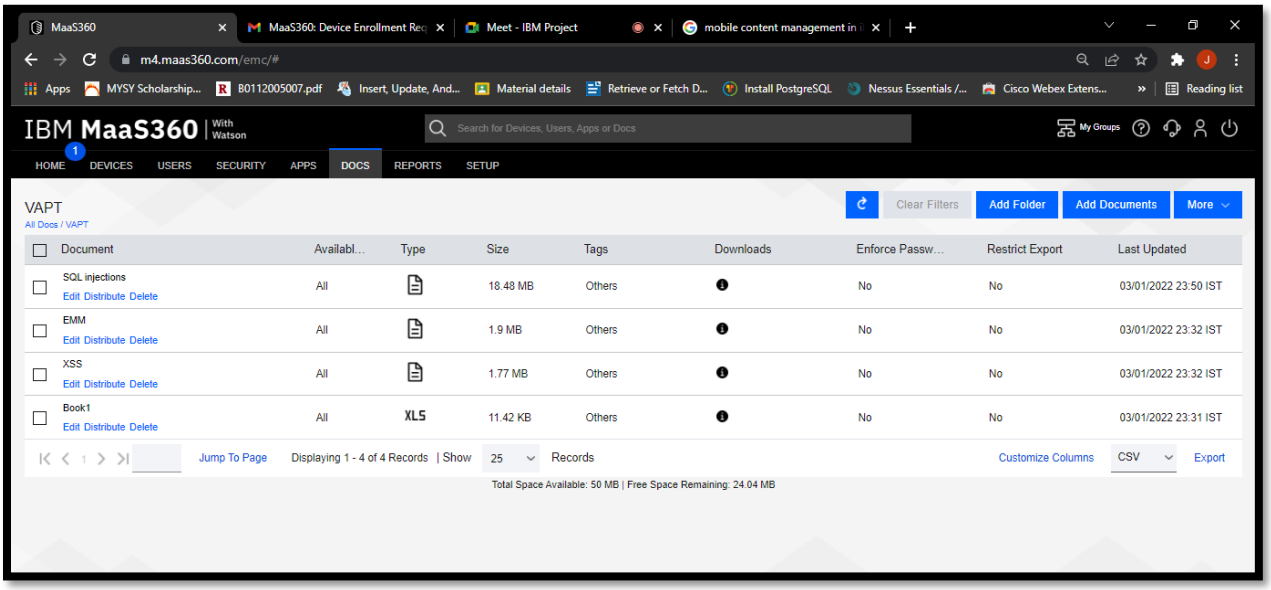
### 6.4.1 **Content library:**

The Content Library uses the MaaS360 Content Distribution Network to distribute content to managed devices from the cloud. You can also host and distribute content from a source other than MaaS360.

1. From the MaaS360 Portal Home page, select Docs > Content Library. The Content Library lists your files, provides basic information about those files, and displays folders of documents.



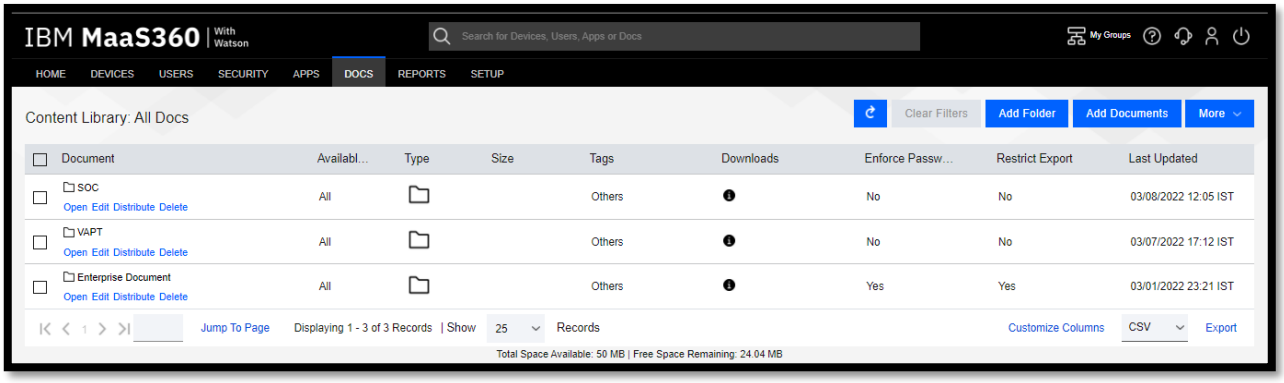

2. Click Open under a folder to display documents or more folders. As you move through the folders, a breadcrumb trail of links is displayed at the top.



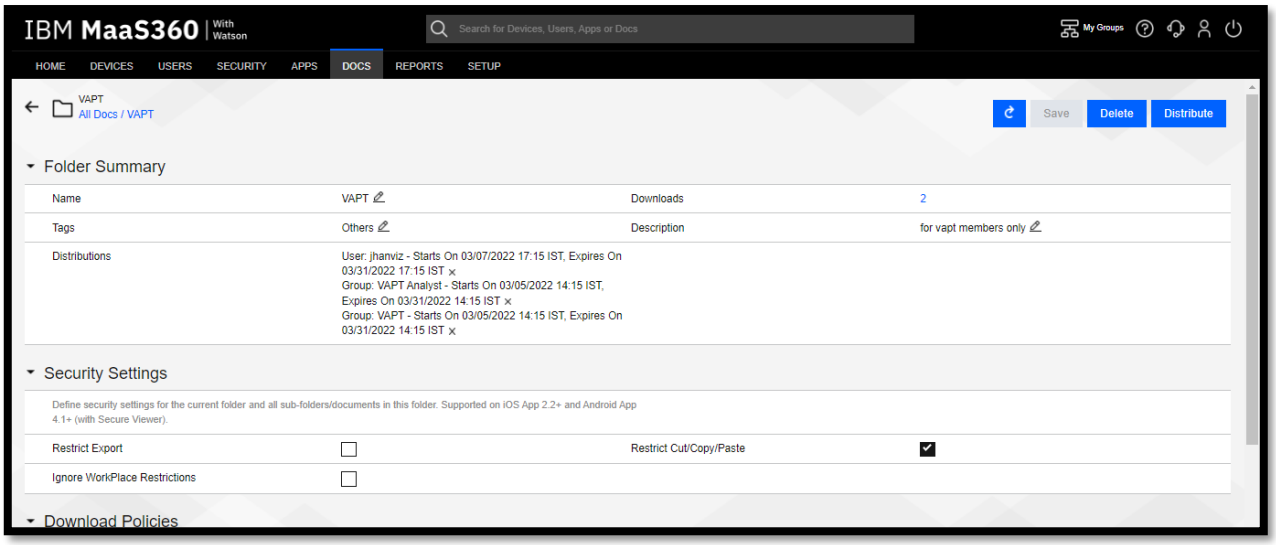

3. Click a column heading to sort and filter files.

### 6.4.2 Managing documents: Content Library:

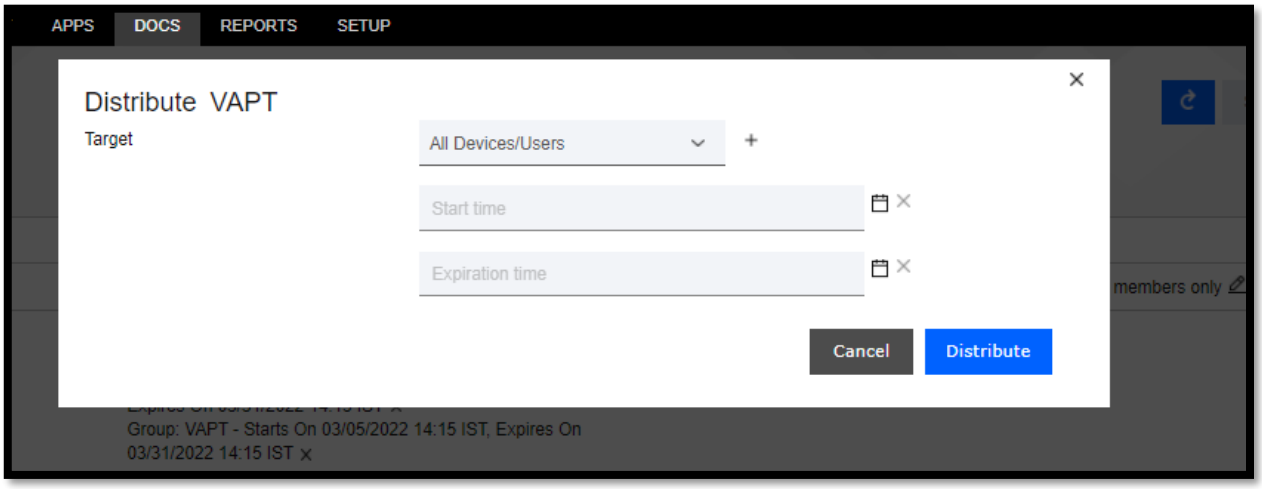
1. To navigate to content library. Go to, select Docs > Content Library.



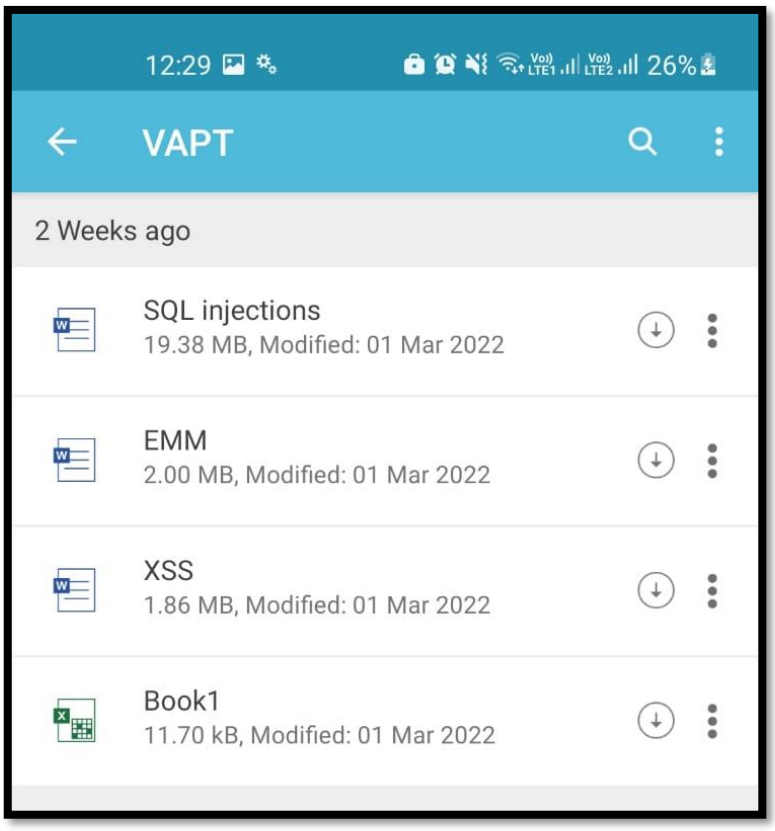

2. Click Edit under the document to view detailed information about the document, including file size, security settings, version history, and download history.




3. Now to distribute this we have to click on distribute. It will ask to which target we want to send this application:

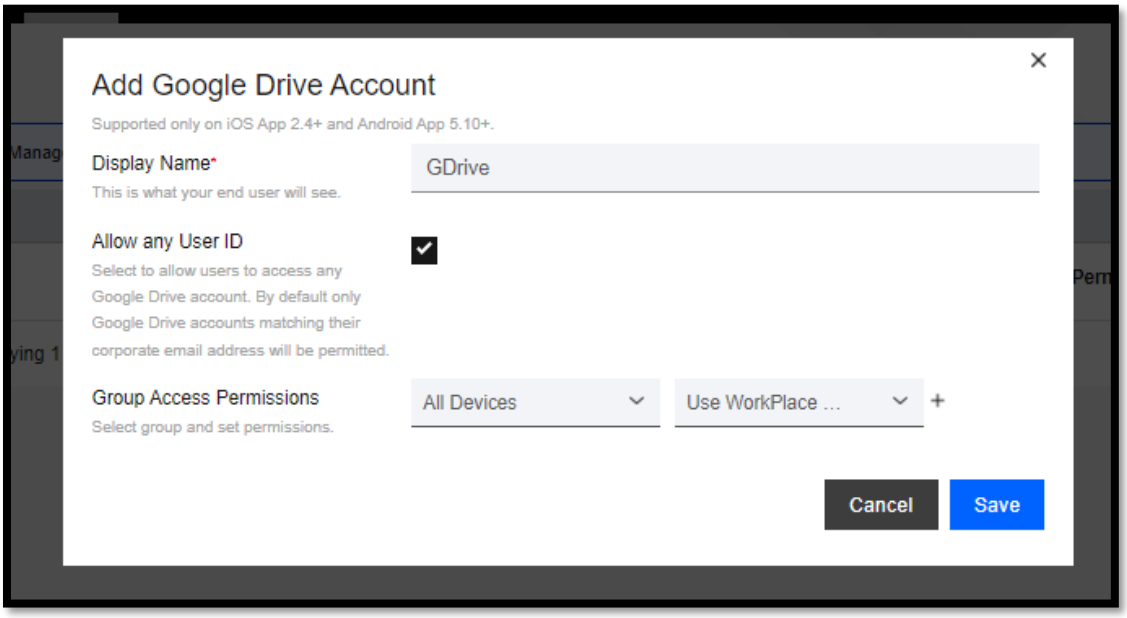



4. Now after distribution in the document section in android device we are able to add that and screen will be like this:

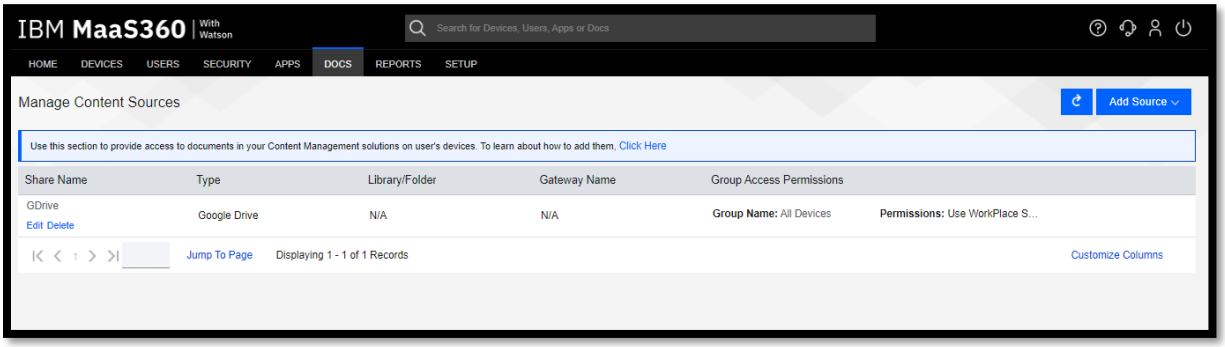



### 6.4.3 GDrive Content Source:

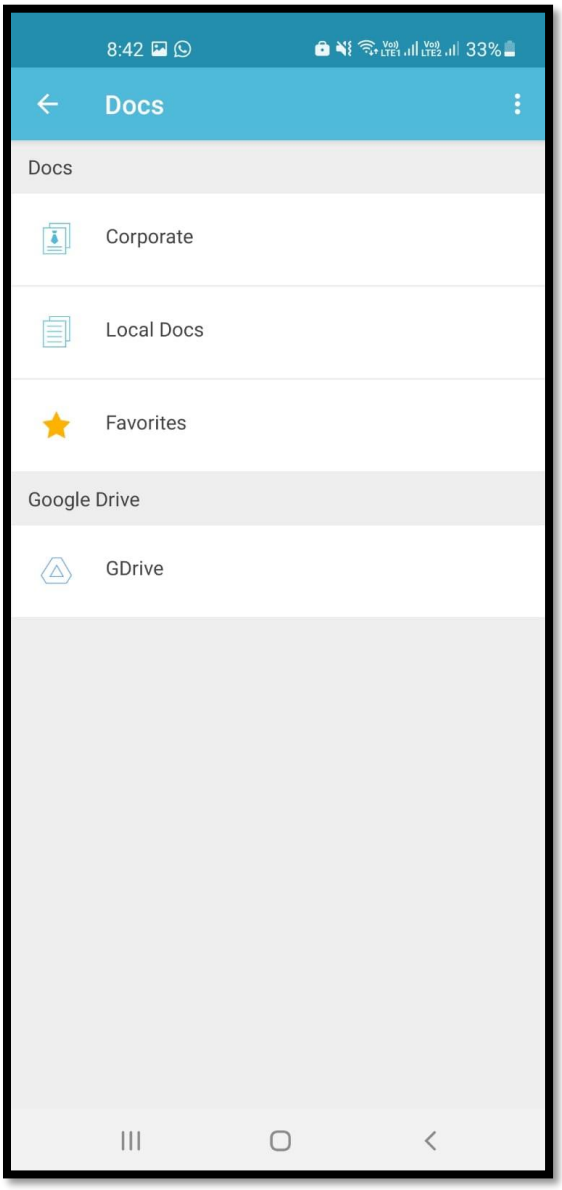
1. To navigate to content source. Go to, select Docs > Content Source.

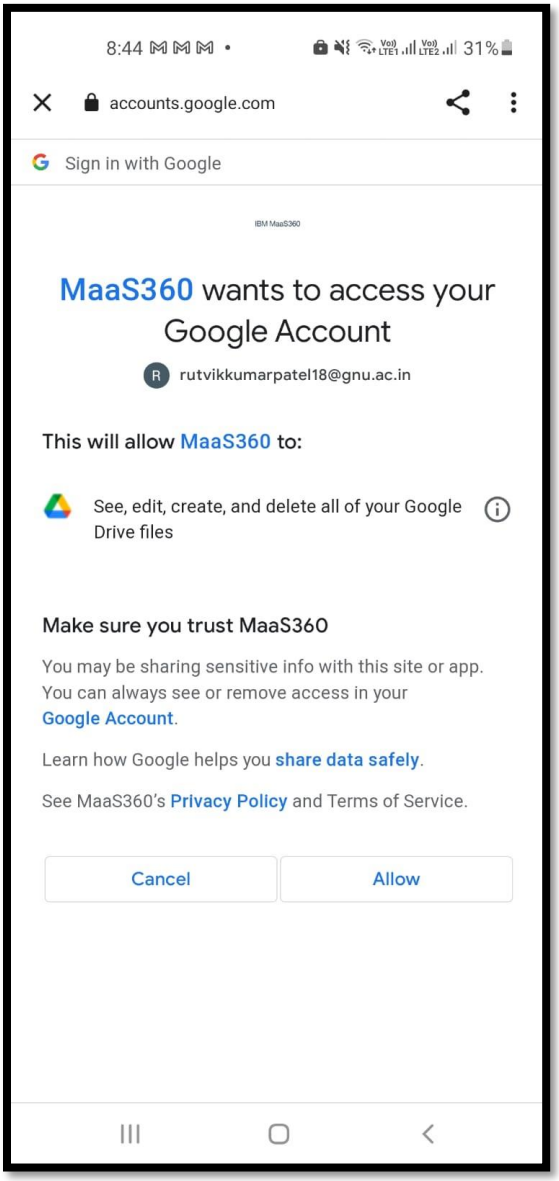



2. Assign name to the source and configure groups access permissions according to the requirements.

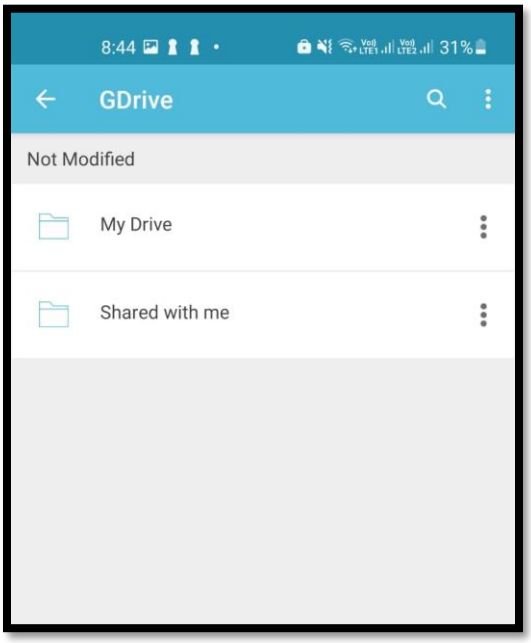



3. Click Save.
4. Now, we can see the added content source,  give access to it.



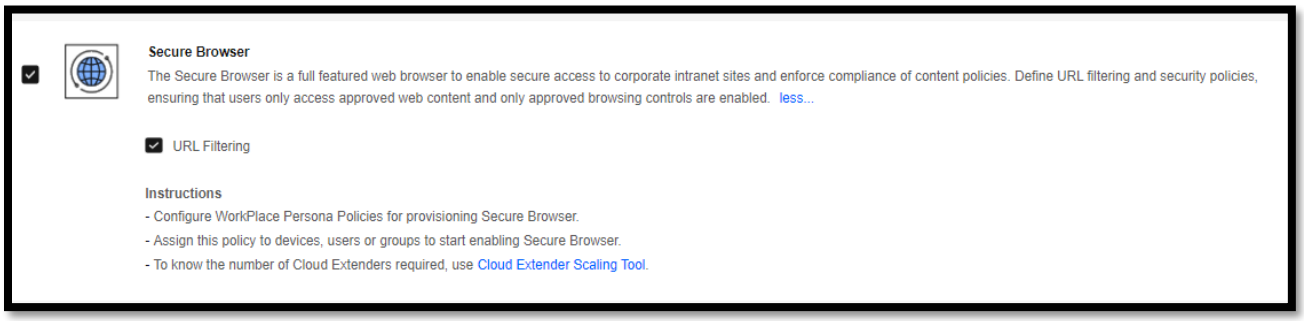

5. Now, we can access our google drive here.




**6.5 Secure browser:**

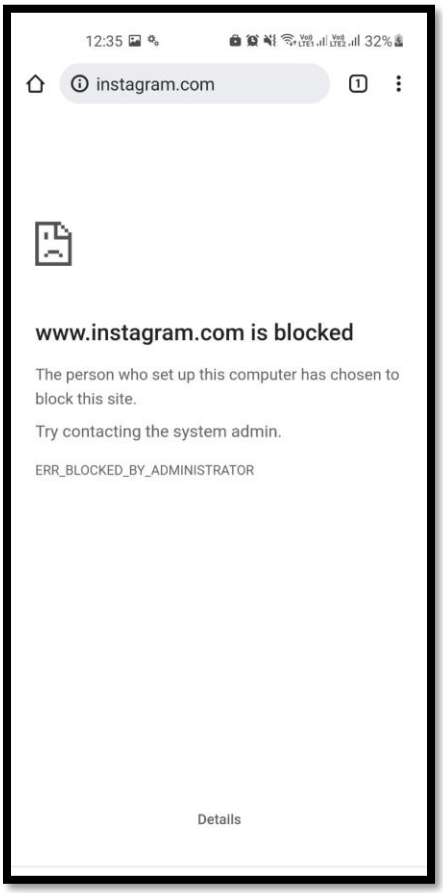
The IBM® MaaS360® Secure Mobile Browser will provide secure access to intranet sites , corporate web apps, and public websites.

The MaaS360 Secure Mobile Browser reduces the risk of accessing websites from your smartphone that may contain malware, violate security policies set by administrators, or otherwise jeopardise device security.




1. After implementing this service get deployed in user devices. Then after creating policy for that which application is allowed and which application is blocked.

   Here in this we have added instagram and facebook application in blocklist. Wikipedia in whitelist. So in browser of user device we are not able to access instagram and facebook.

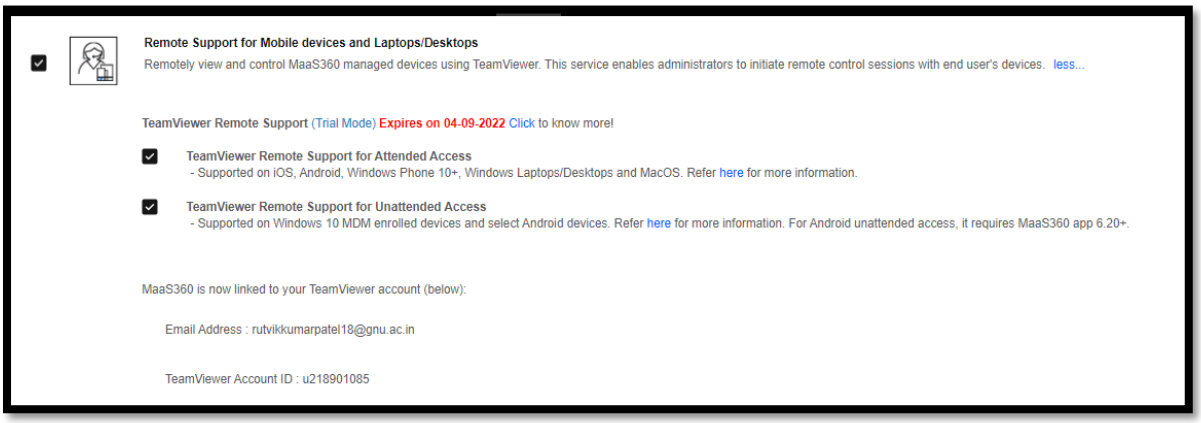



**6.6 Remote support for mobile devices and laptop/desktops:**

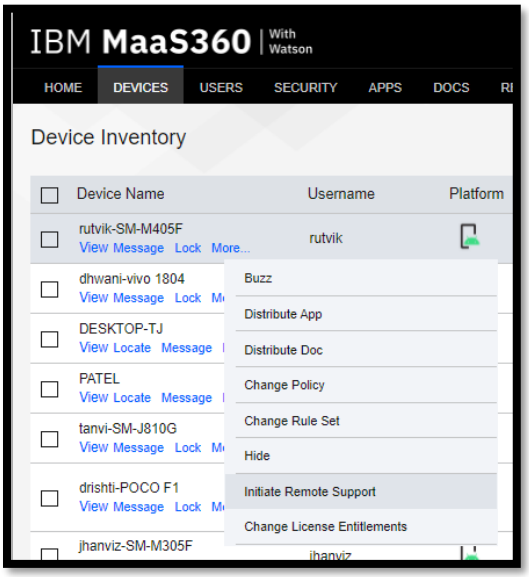
MaaS360 (SaaS) solutions now have a more extensive feature set, with a stronger focus on global online assistance and collaboration, thanks to the inclusion of TeamViewer technology.

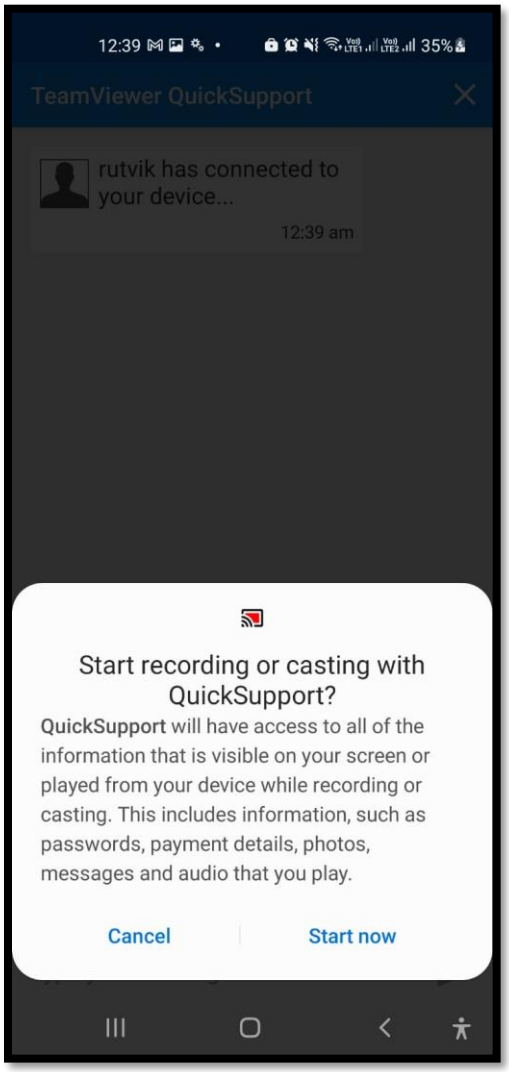
The MaaS360 (SaaS) platform now has TeamViewer Remote Support for MaaS360, which adds the following remote support and functionality:

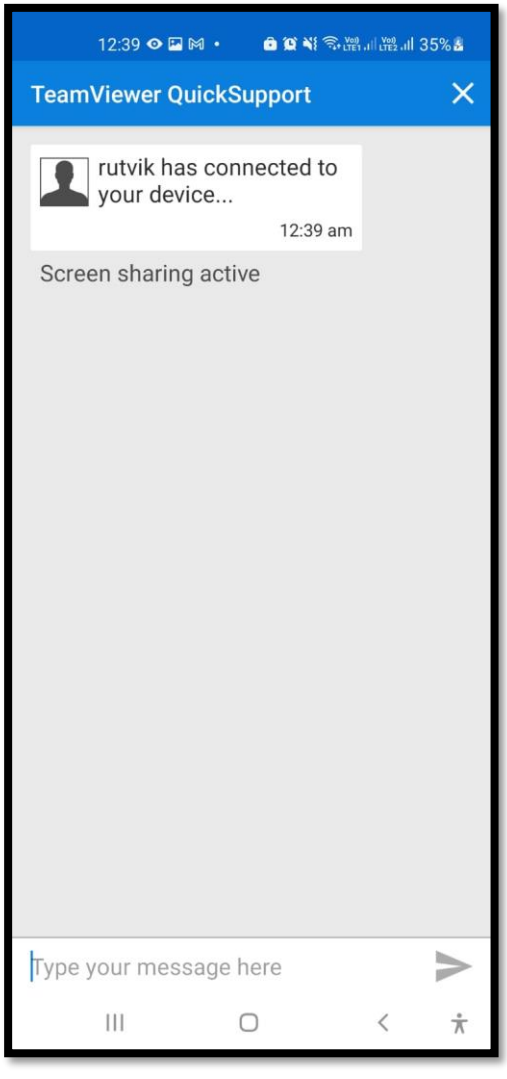
- Fast and reliable way for IT administrators to remotely view and control workstations or mobile devices managed by MaaS360. Users can quickly share the entire screen with IT administrators for troubleshooting issues.
- Remote support for any kind of device operating system or form factor, including Apple iOS, Google Android, and Microsoft™ Windows™ devices.
- During remote sessions, quick-access tools such as chat and file transfer help facilitate the transmission of information between IT and users.
- Additional capabilities such as session recording and connection reports, which enable IT departments to regularly monitor performance and improve the efficacy of remote support in their organisations.

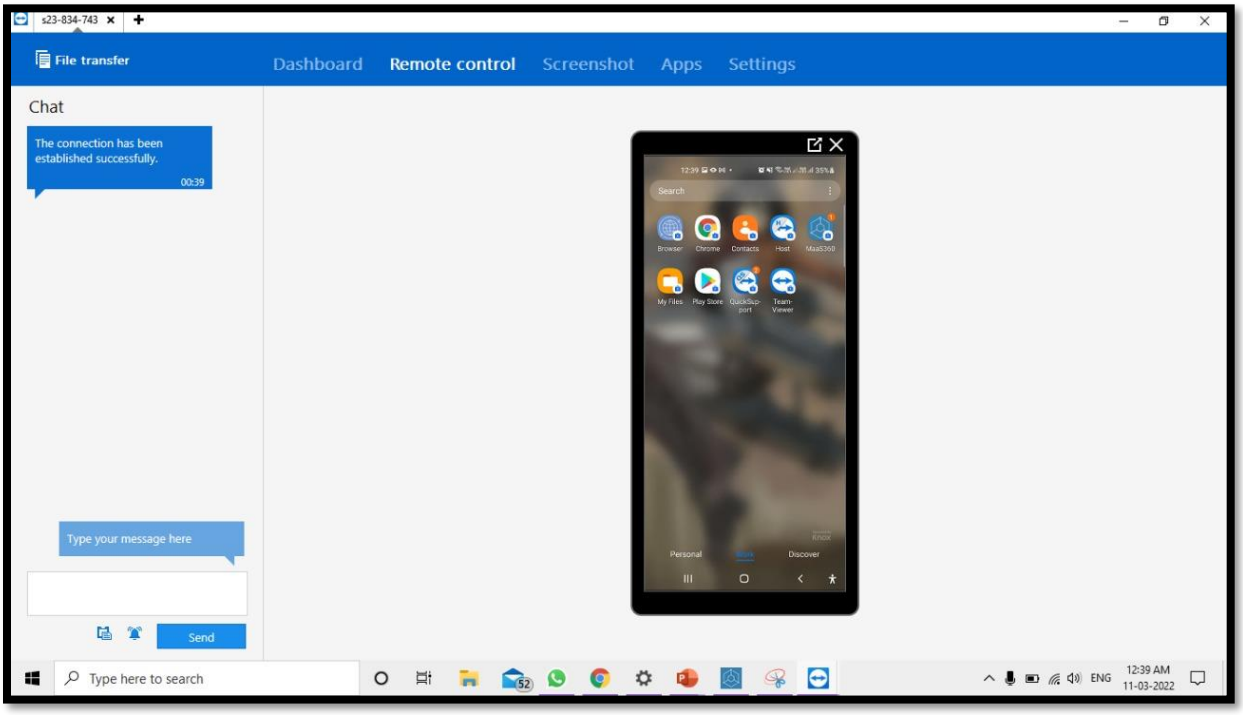



1. After deploying this. In mobile devices we will have team viewer application and messages application. Now while deploying it we will have this steps:



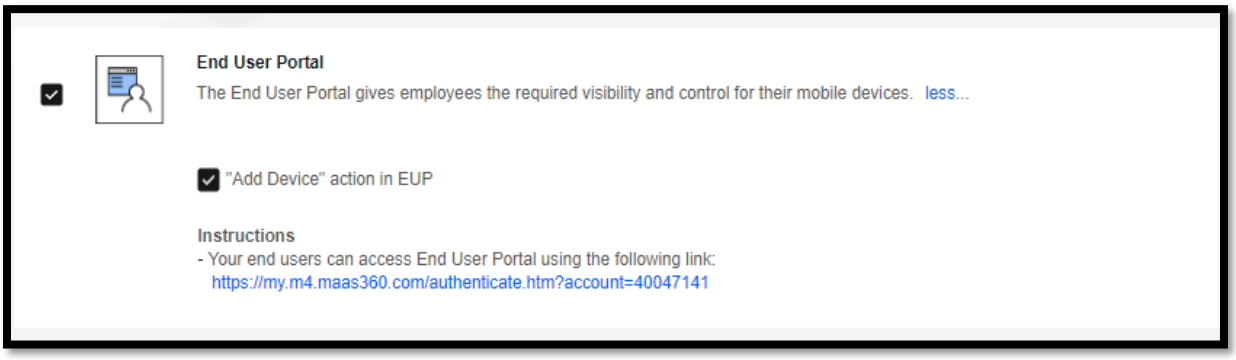

12:39
TeamViewer QuickSupport
rutvik has connected to your device...
12:39 am
Start recording or casting with QuickSupport?
QuickSupport will have access to all of the information that is visible on your screen or played from your device while recording or casting. This includes information, such as passwords, payment details, photos, messages and audio that you play.
Cancel
Start now


12:39
TeamViewer QuickSupport
rutvik has connected to your device...
12:39 am
Screen sharing active
Type your message here

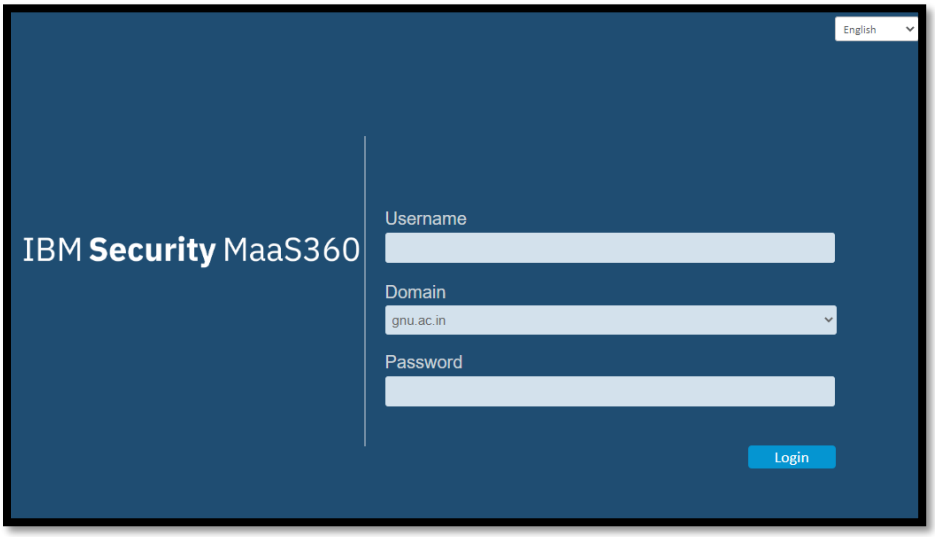

File transfer
Dashboard
Remote control
Screenshot
Apps
Settings
Chat
The connection has been established successfully.
00:39
Type your message here
Send
Type here to search
ENG
12:39 AM
11-03-2022

### 6.7 Configure End user portal:

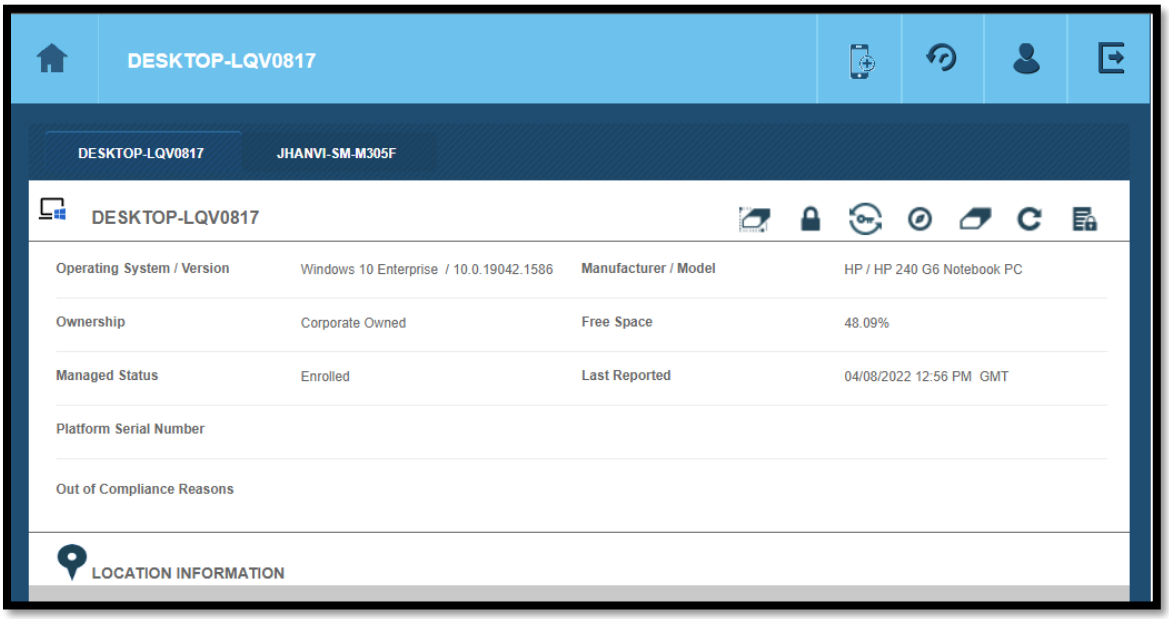
1. Go to setup->services. Enable end user portal:



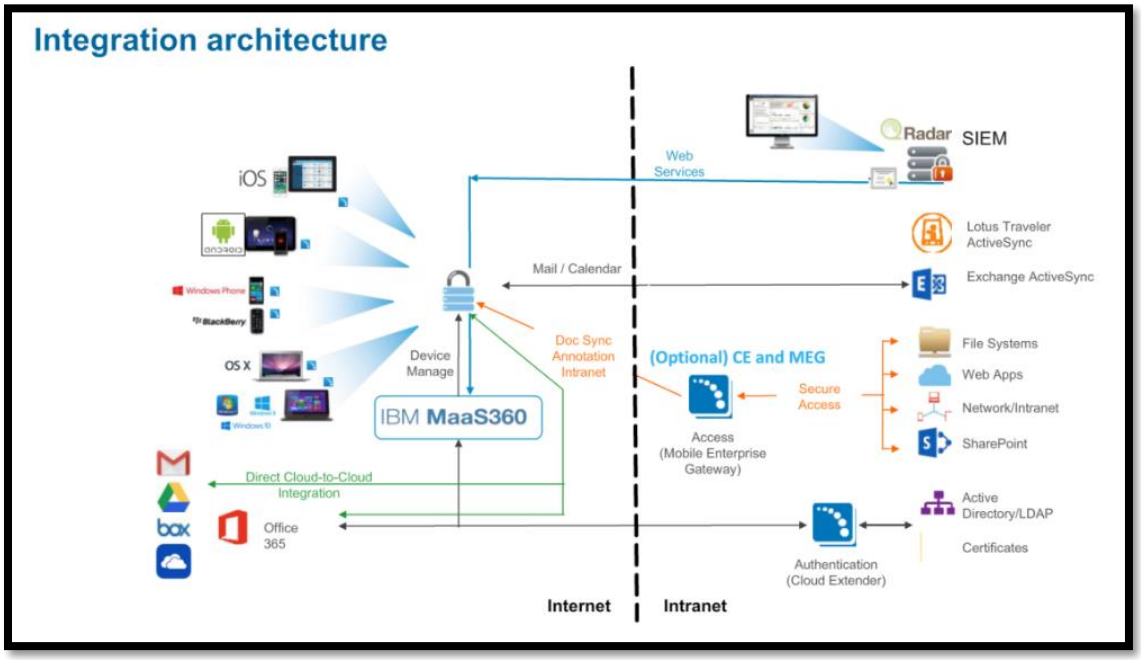

2. Now here click on link given:




3. Login with credential and we are able to get private information of particular user:

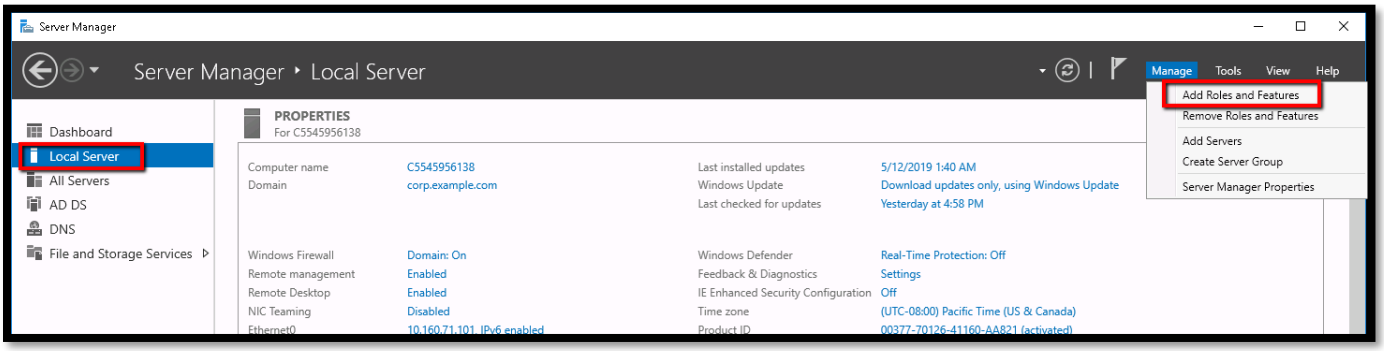



### 6.8 Configuration of server setup:



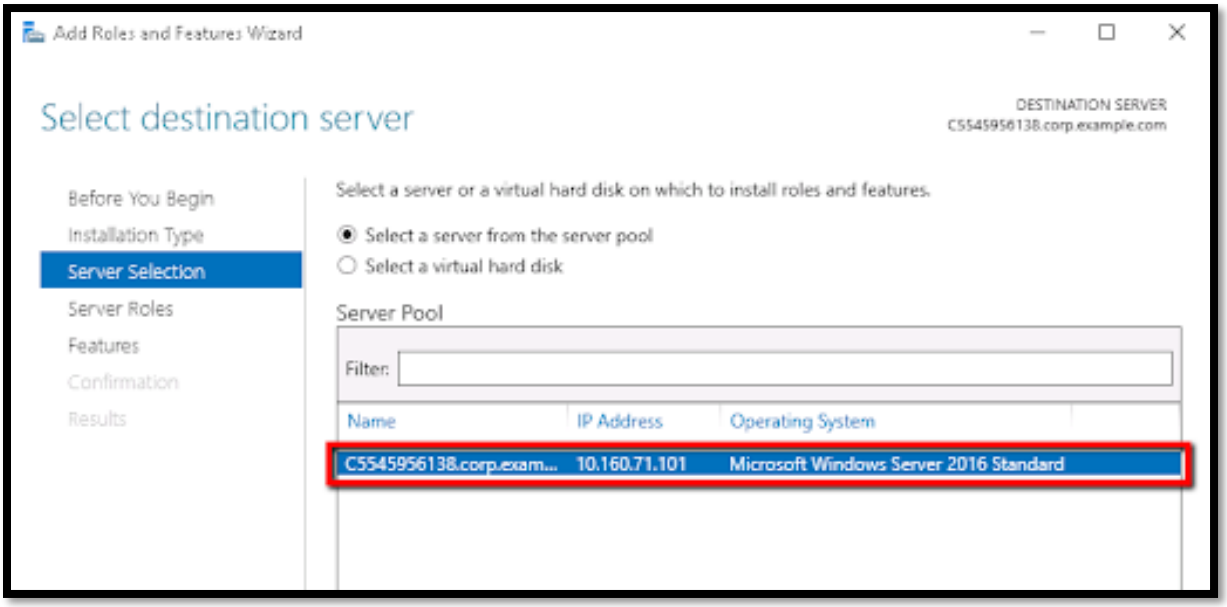

As per requirement to setup cloud extender configuration tool in project. First we need to setup Windows server as a system to donwload:

1. Open the Server Manager by logging in to your Windows Server.
2. Select Manage > Add Roles and Features from the command menu at the top right of the window: 2. Navigate to the Local Server tab and select Manage > Add Roles and Features from the command menu at the top right of the window:

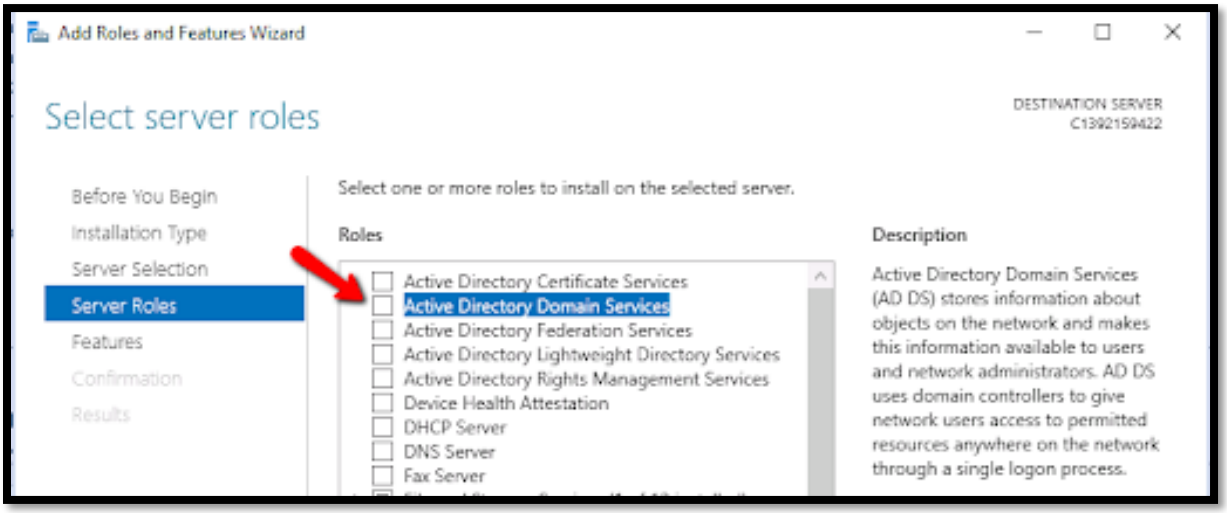



Next should be selected. The Wizard will now move on to the option for Installation Type.

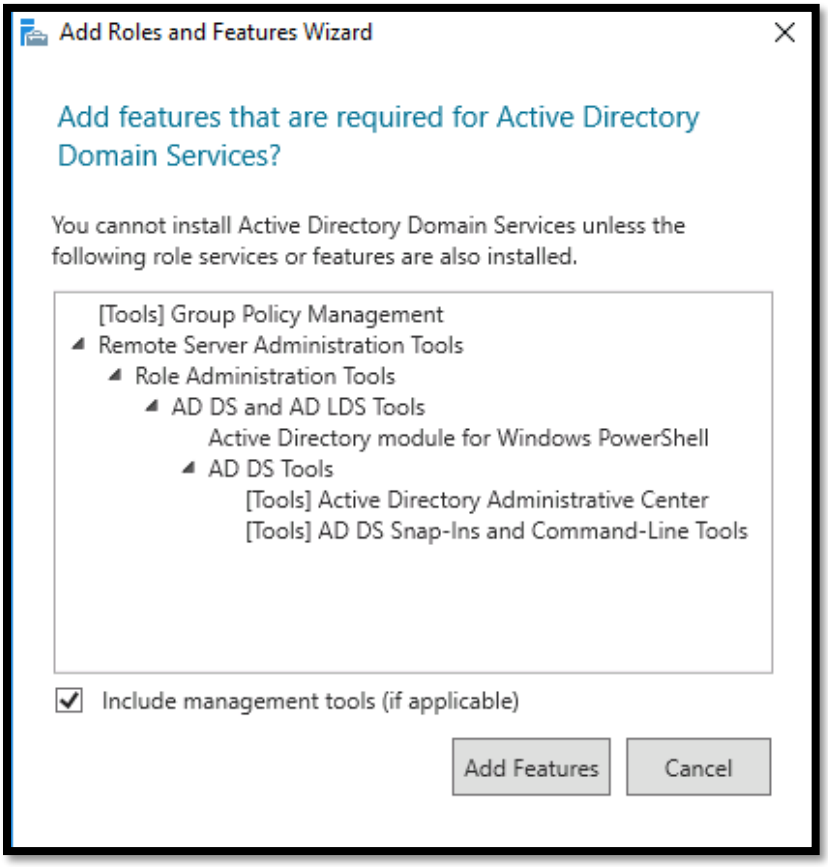
3. Choose between a role-based or feature-based installation.
4. Select Next. The panel Select destination server appears:



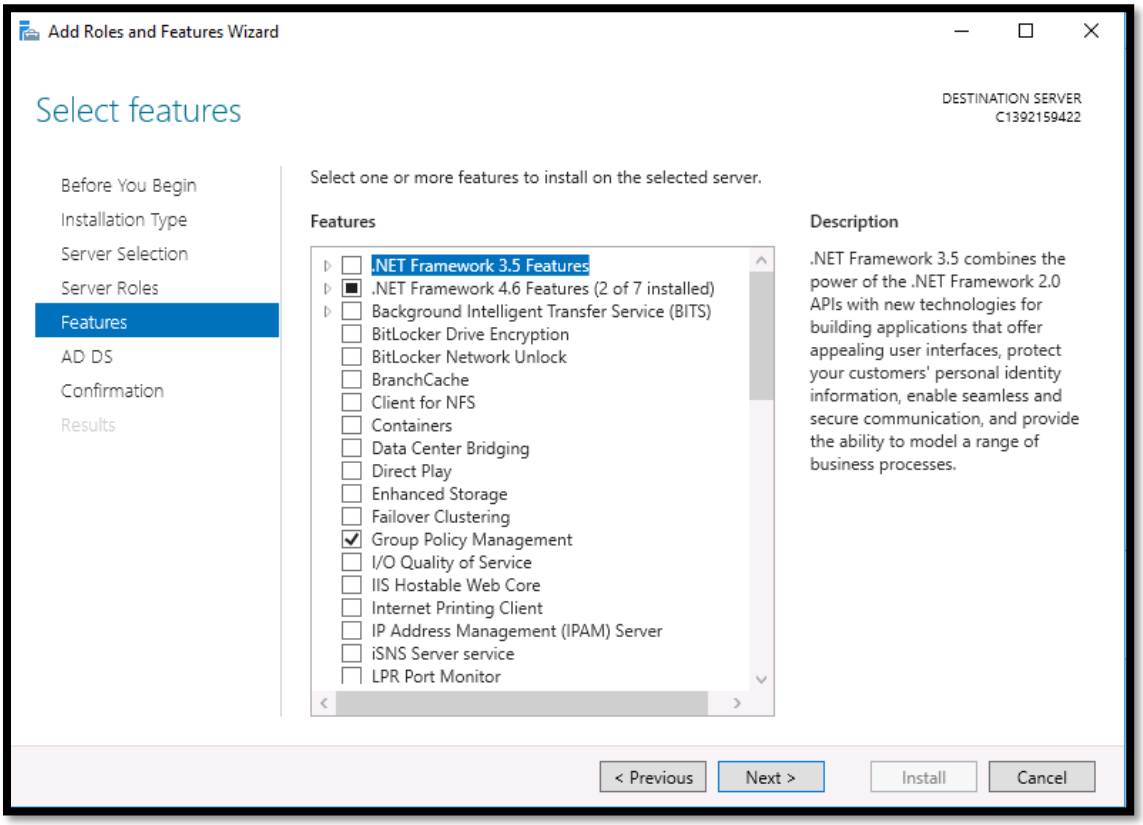

5. The server to which the installation will be applied should be selected by default. Click Next after confirming that the intended server has been picked from the server pool (or selecting the desired server). The Choose Server Roles screen appears:



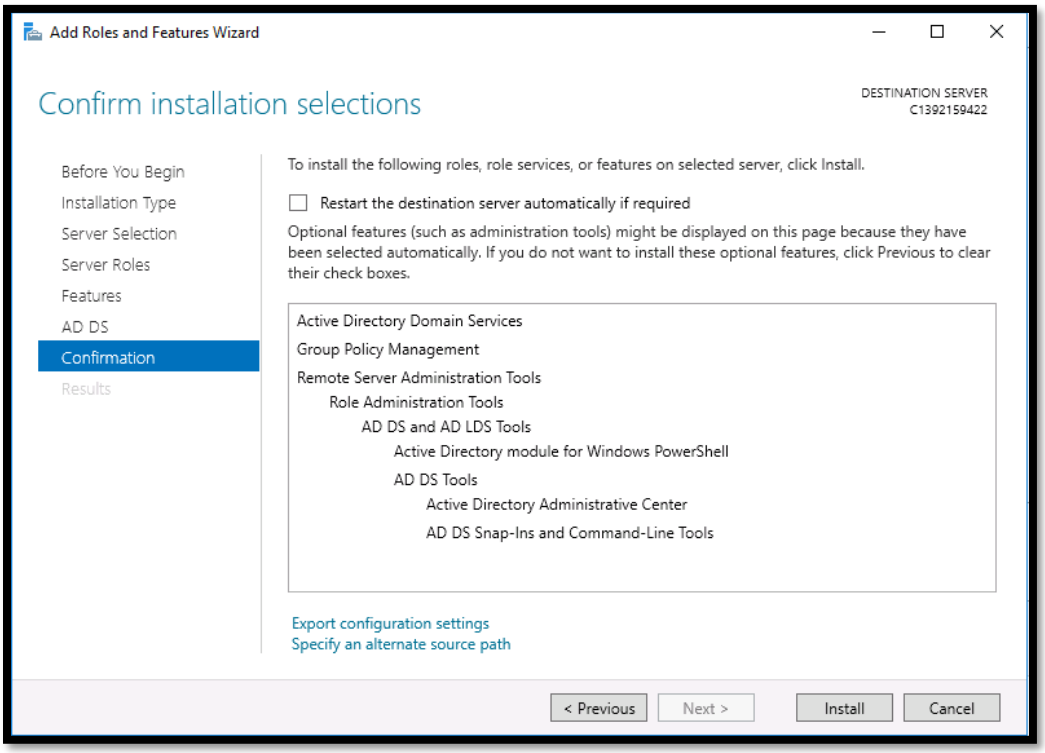
6. To activate user role in server, click on active directory domain services checkbox.
7. Click **Next**. The required features list is displayed:



8. To add required features of the server click on add features options.



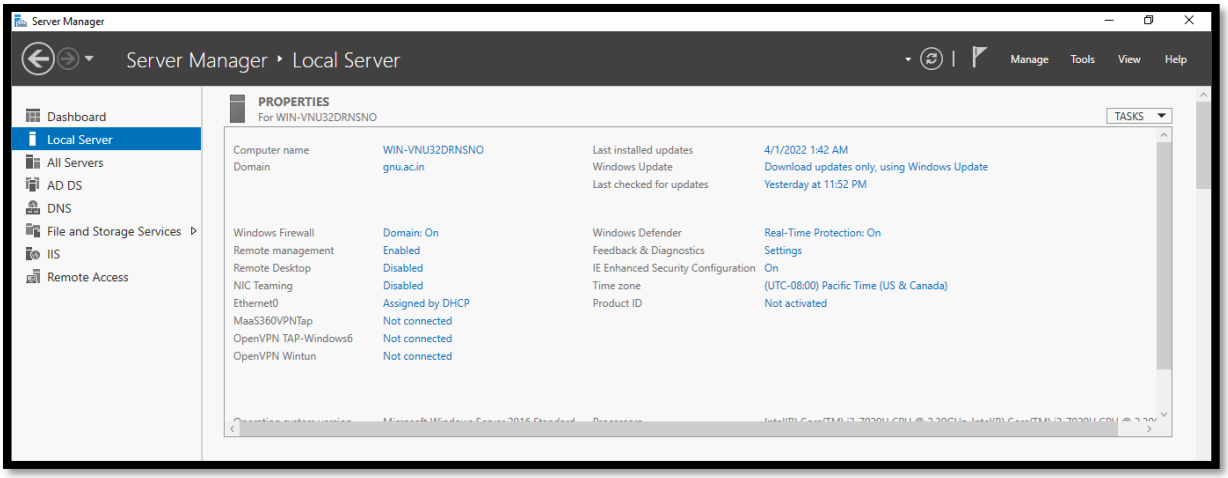

9. After clicking on next we get final option to install the particular update version of server:



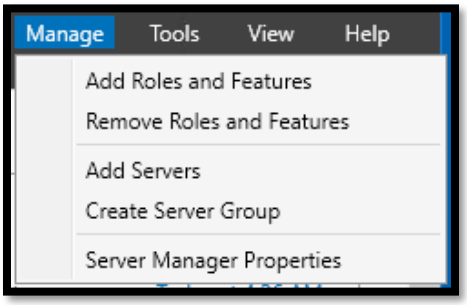

10. If all selections are correct, click **Install**.

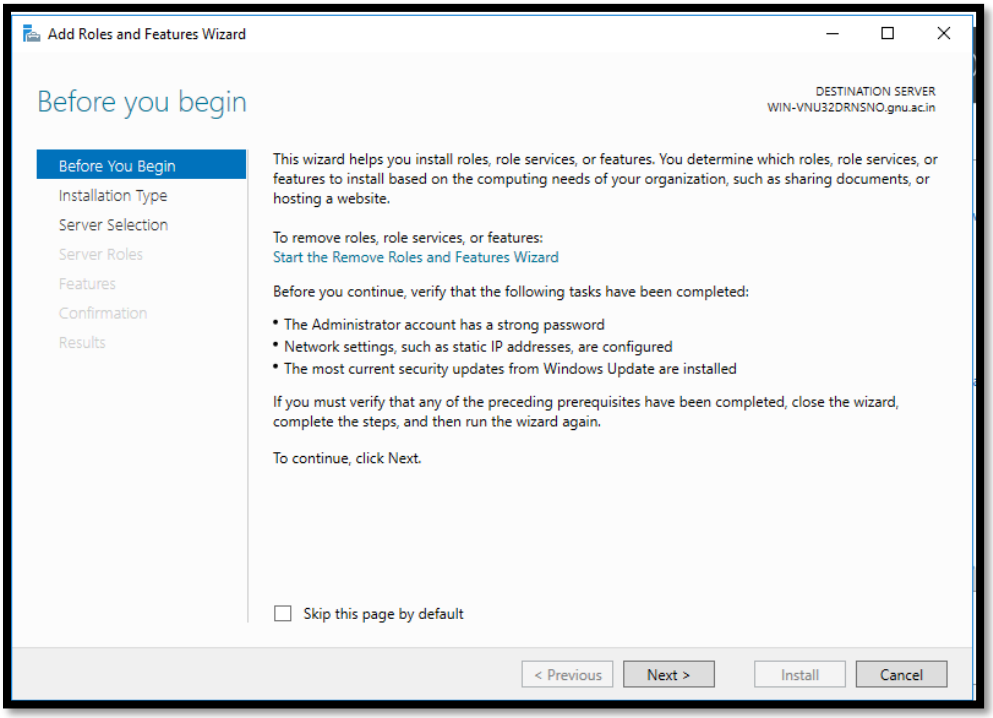
## 6.9 Configure DNS server:

1. To proceed to local server first open the server manager window:

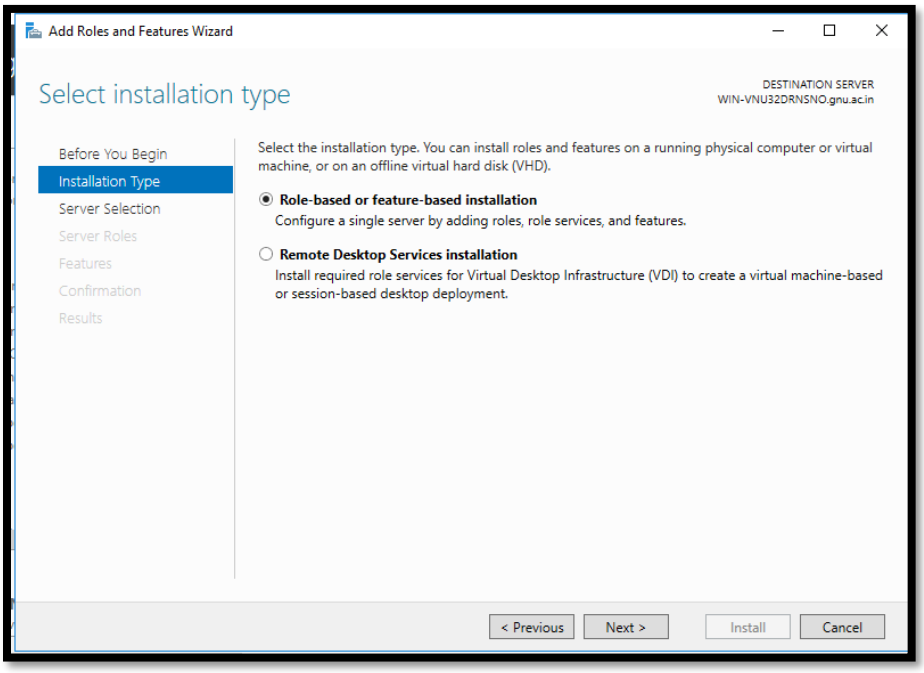



2. To add feature and roles in this click on tools and select add roles and features:

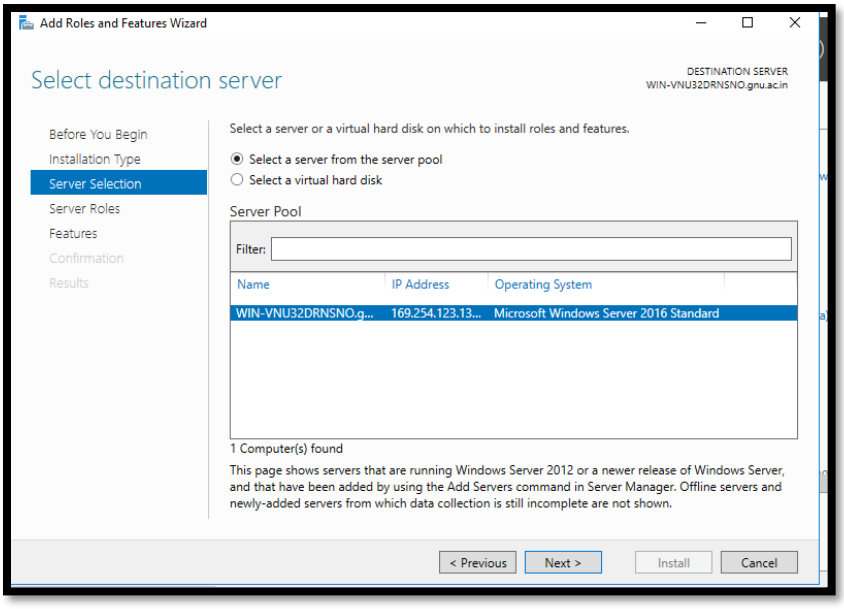


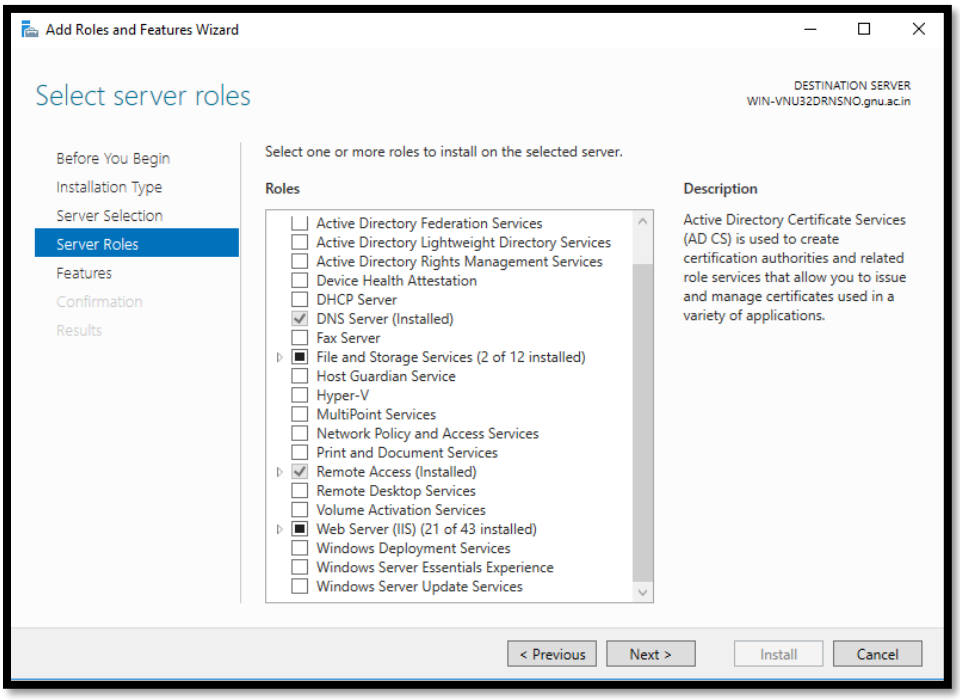
3. If you are using Role-based or Feature-based installation, select the radio button next to it



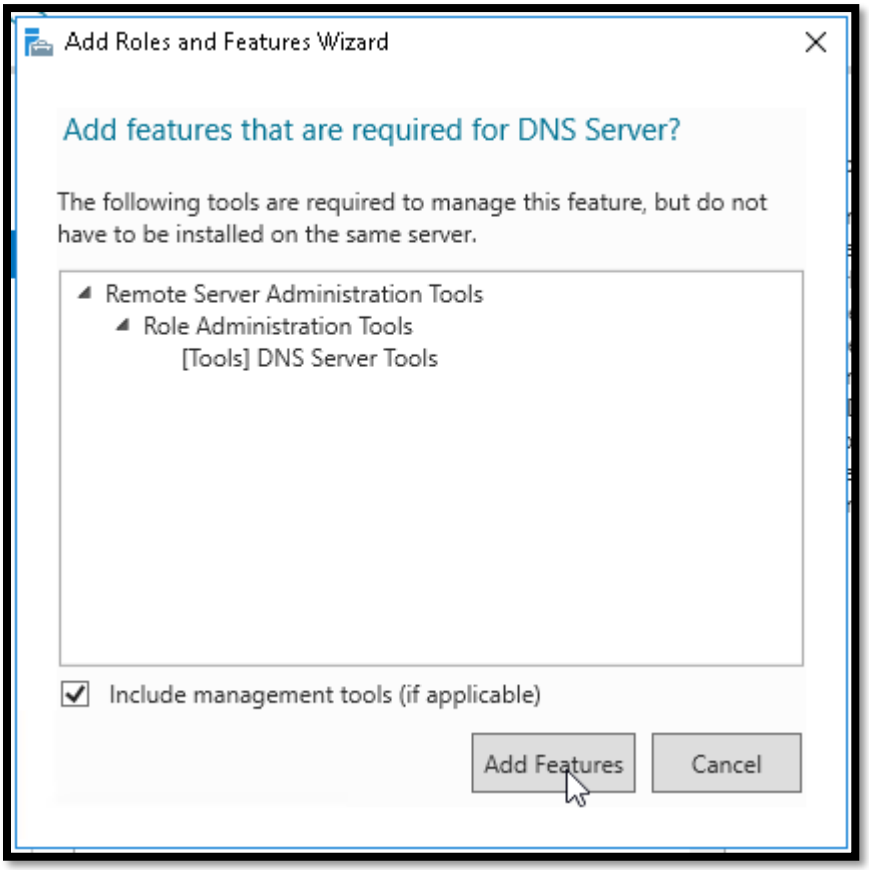

4. Choose the server that will be used for this function. It's usually the same as the machine you're looking at this on for a DNS-Only configuration. However, there is the ability to install the role remotely.



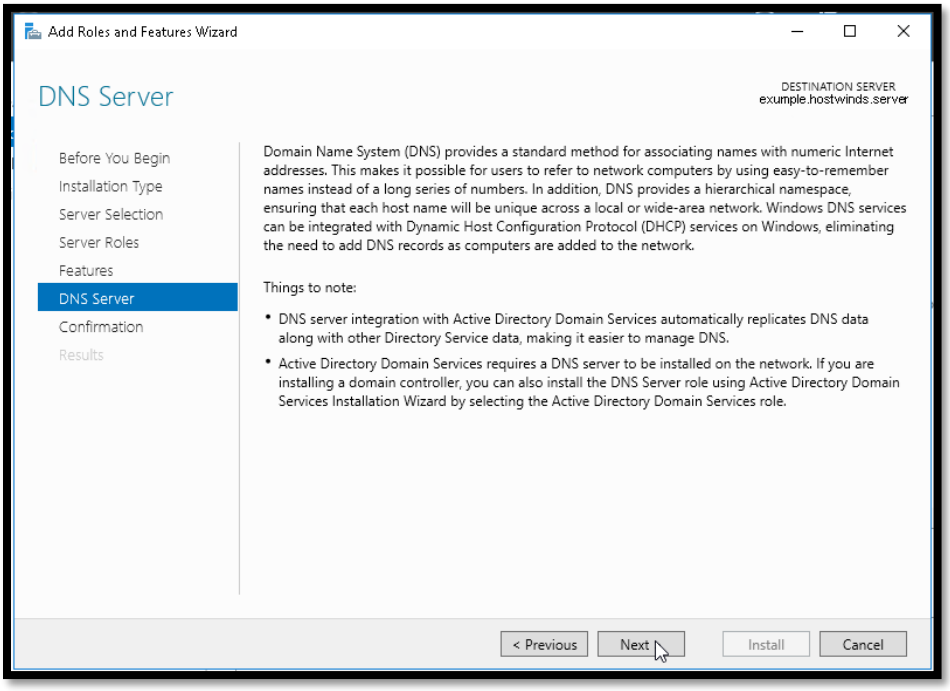
5. Tick mark checkbox of DNS Server.



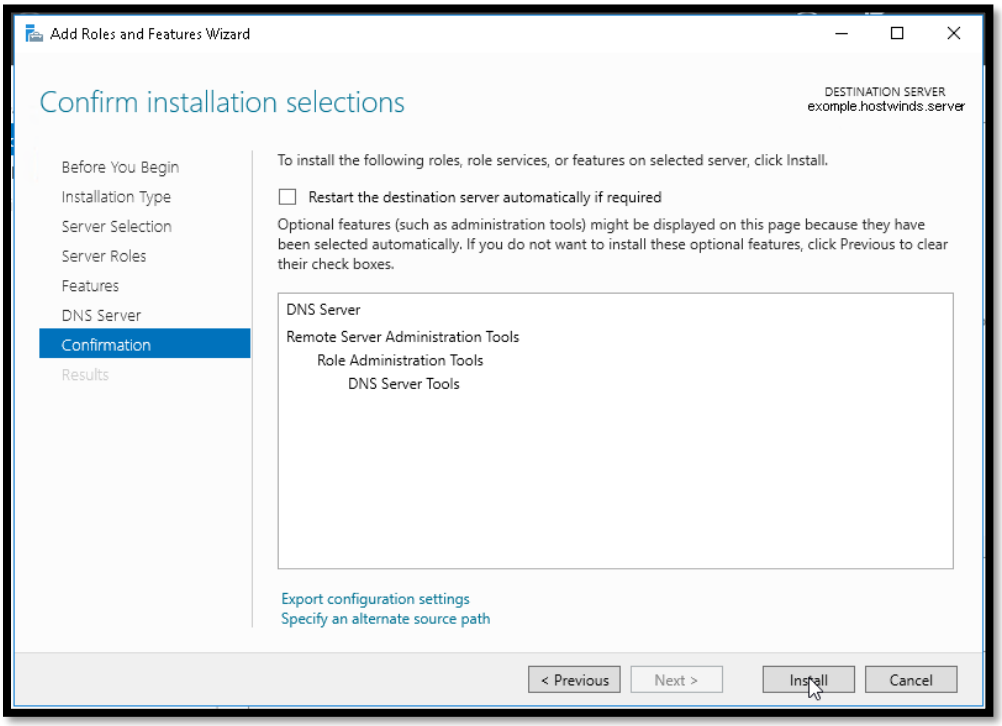

6. A window then asks you to confirm the dependencies (usually just the Administration Tools required for the DNS role) also to be installed. Click Add Features, as this is usually required

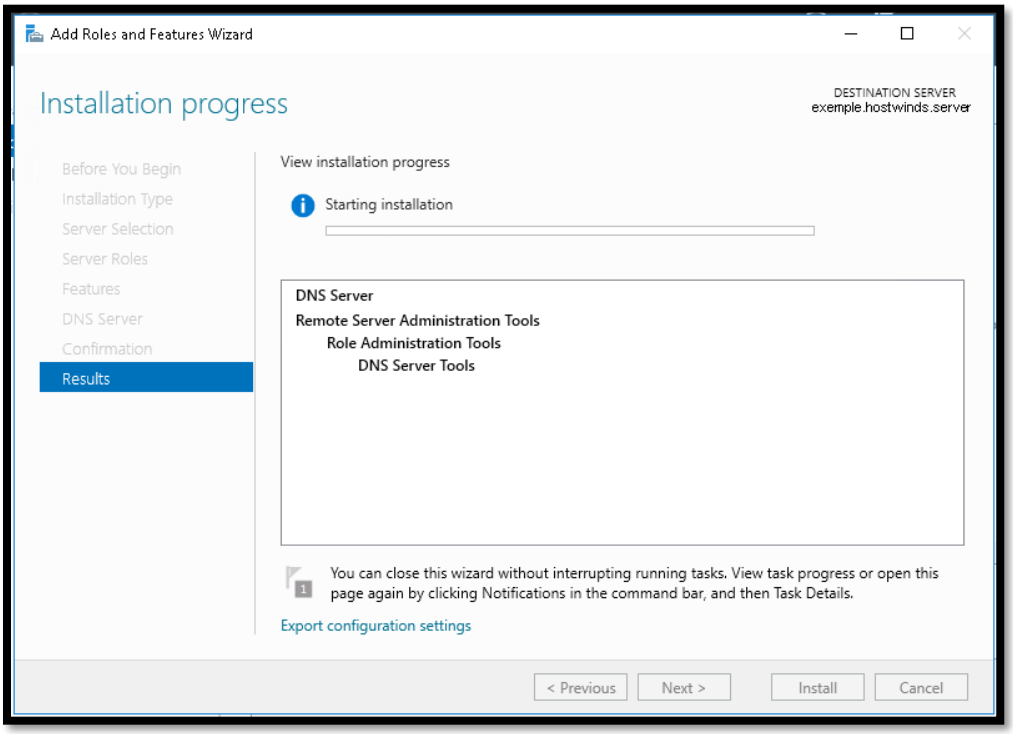


7. A black check icon should be placed next to the check box. This is usually reserved for File & Storage Services by default). Then, to proceed, click Next.
8. In the next box, it offers you a brief description of the services and their tasks, as well as a list of objects that this role may affect or that this role requires installation.




9. The installation's final validation. It then gives you the option to restart the destination server (this is advised for large installations) before returning you to the server manager interface.




Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
exemple.hostwinds.server
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DNS Server
Confirmation
Results
View installation progress
Starting installation
DNS Server
Remote Server Administration Tools
Role Administration Tools
DNS Server Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Install
Cancel

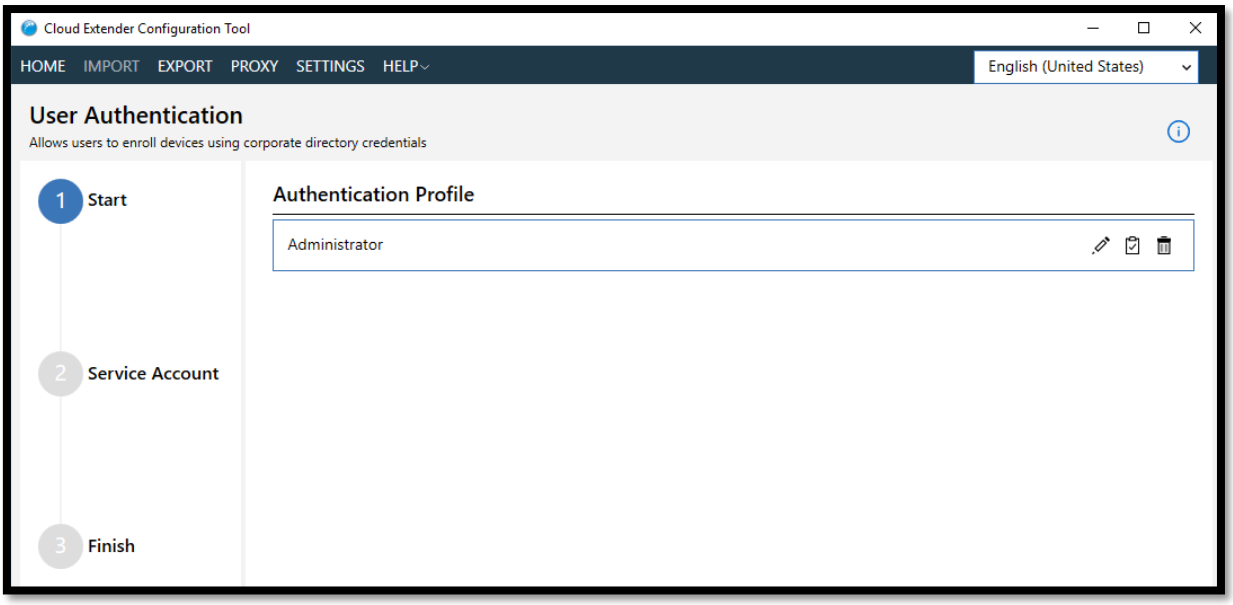
### 6.10 Configuring Cloud extender:

1. Double-click the MaaS360 Cloud Extender Install icon to begin the installation process.
2. To go to the Install Location screen, click Next.
3. Click Next after selecting your destination folder.
4. Enter your Account ID and the licence key number you received in the Welcome email message, then click Next.

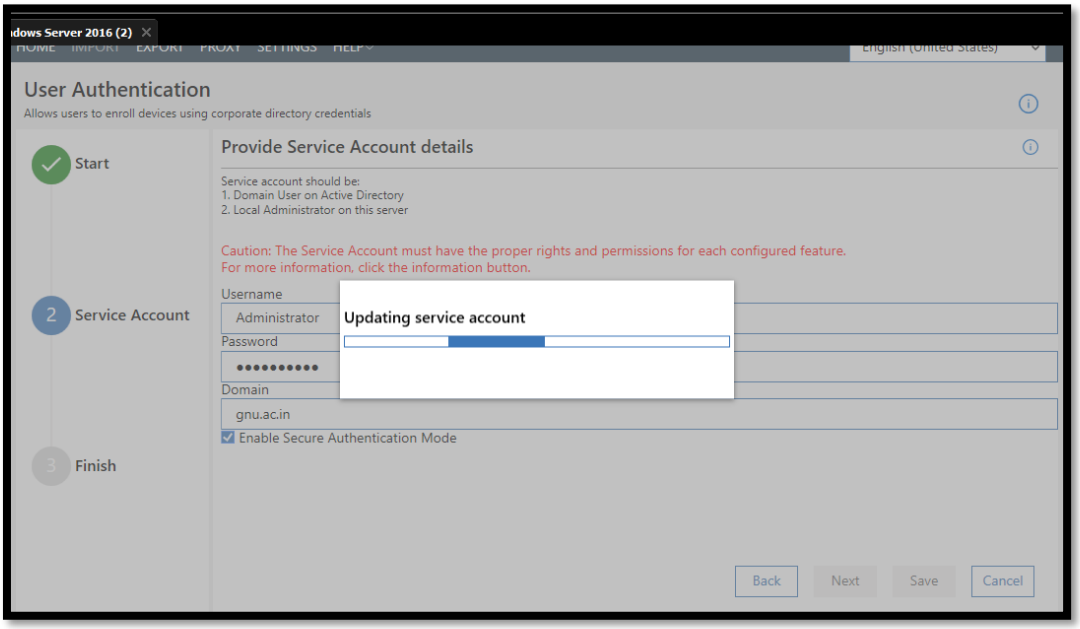
   The Account ID is the same ID as the Billing ID. The installation program compares the Billing ID that is embedded in the license key. If the Billing ID and the Account ID match, the Cloud Extender installation program continues. If the Billing ID and the Account ID do not match, a message box is displayed that informs you that the license key is not valid for the Account ID that you entered.
5. Click Install, and then click Next to continue the installation.
6. When prompted, click Finish to start the Cloud Extender Configuration Tool

### 6.10.1 User authentication:

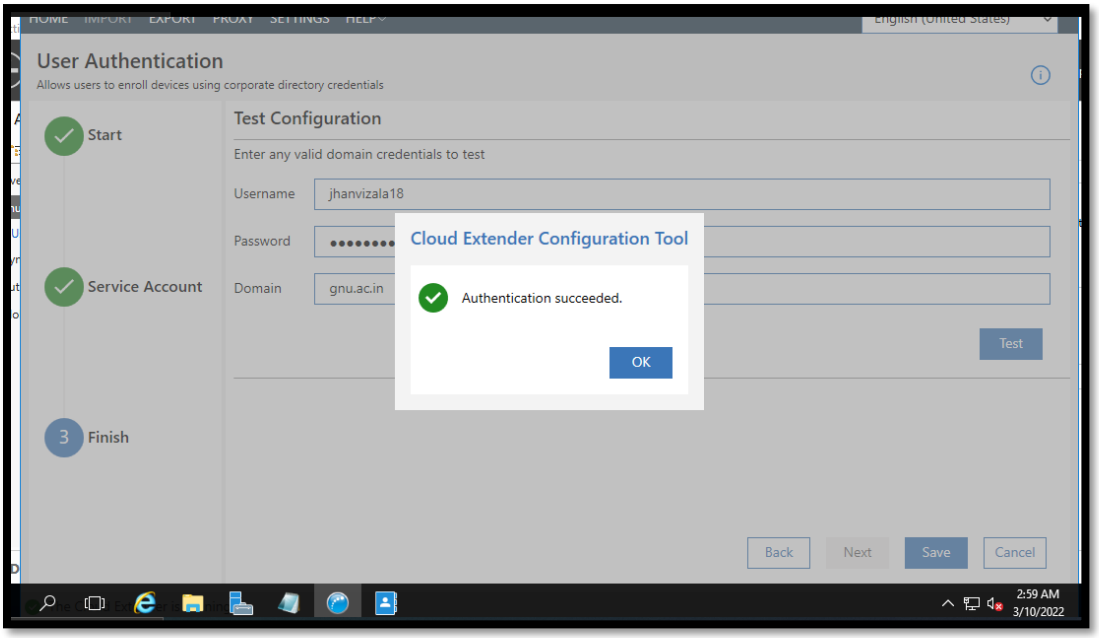
- Select User Authentication in the Cloud Extender Configuration Tool.
- Click Next after selecting the authentication mode you want to configure: Active Directory or LDAP.
- Complete the service account configuration.

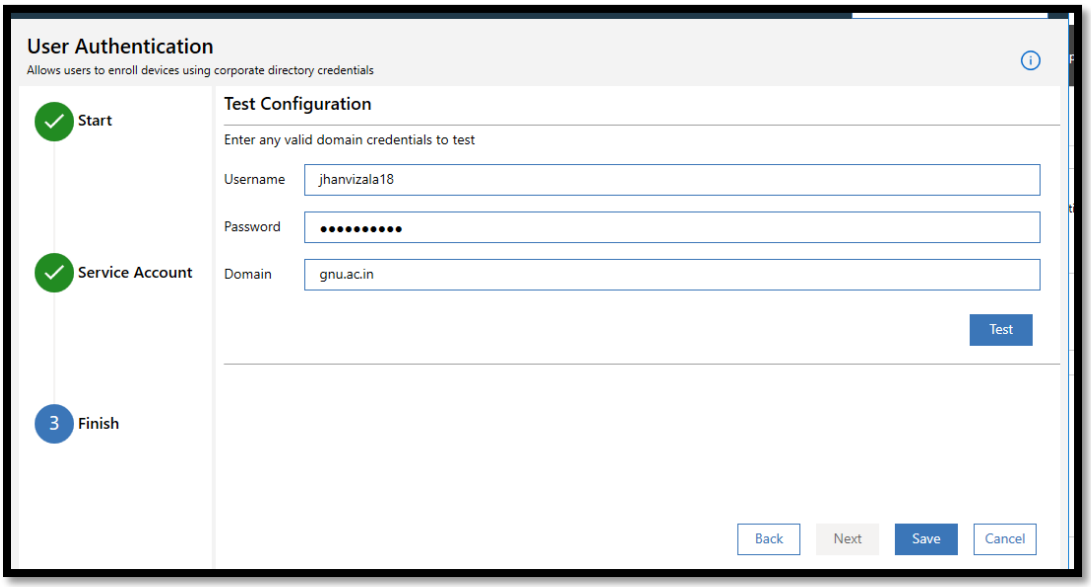



- now after setting up active directory we have username and password. So test this with help of that username and password

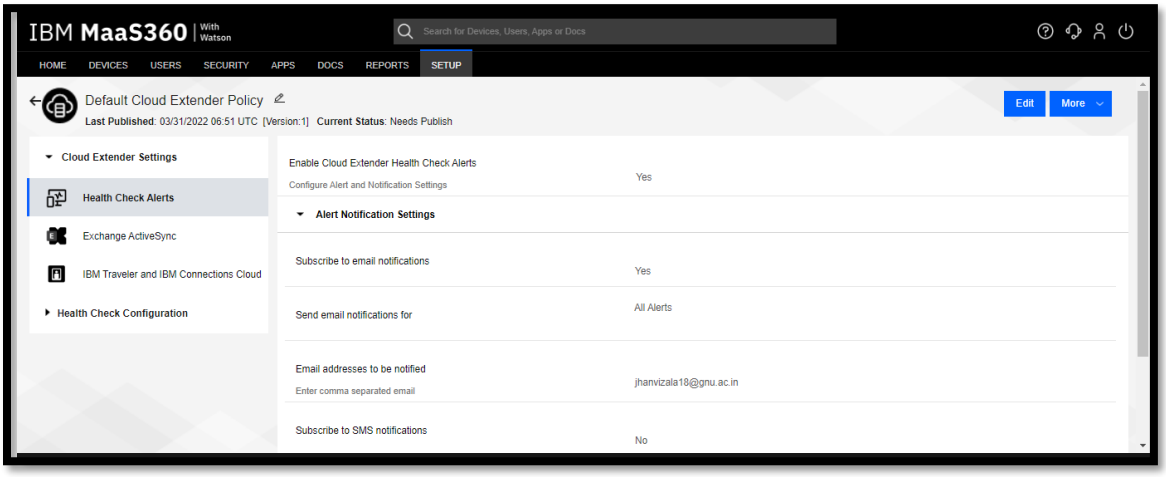


- After authenticating it we need to click on test to test the authenticity of that user and domain:

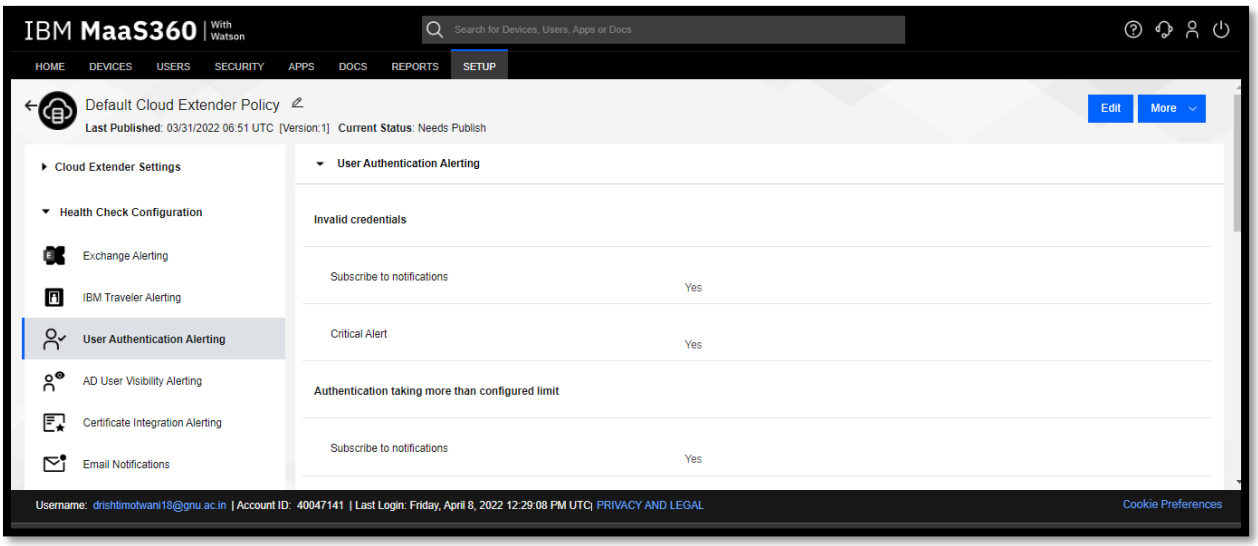


- From theMaaS360 Portal Home page, select **Setup** > **Cloud Extender Settings**.

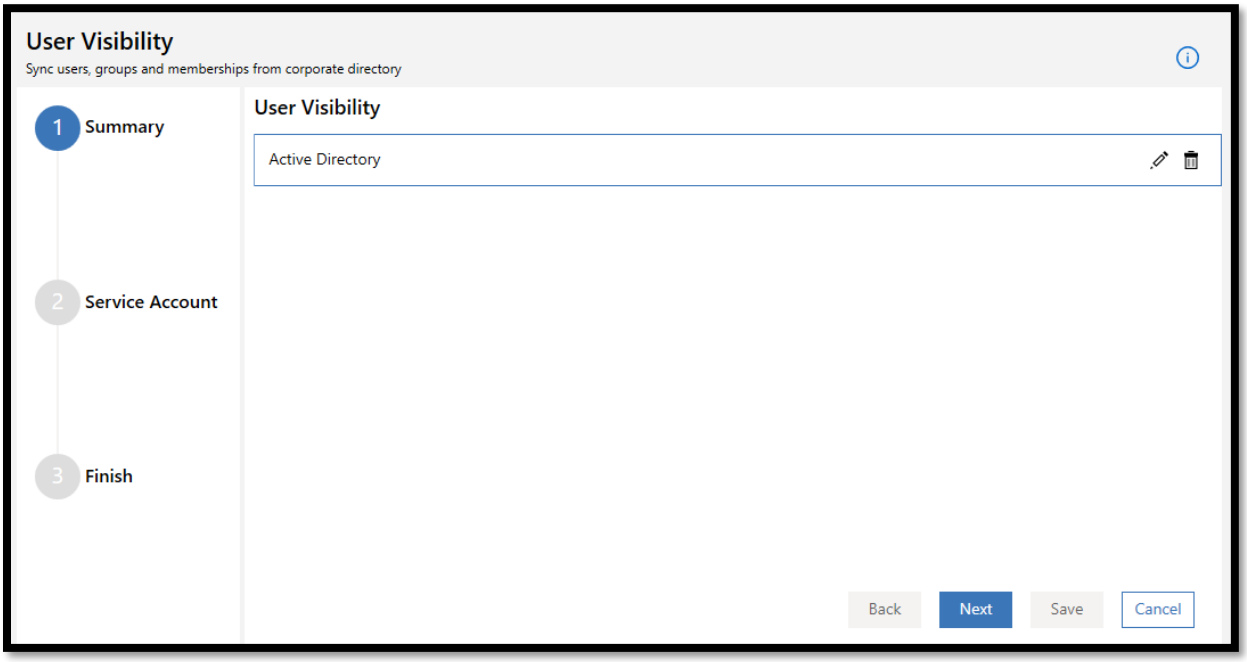



- After configuring in cloud extender administrator need to check its health configuration so for that go to **Health Check Configuration** > **User Authentication Alerting**.

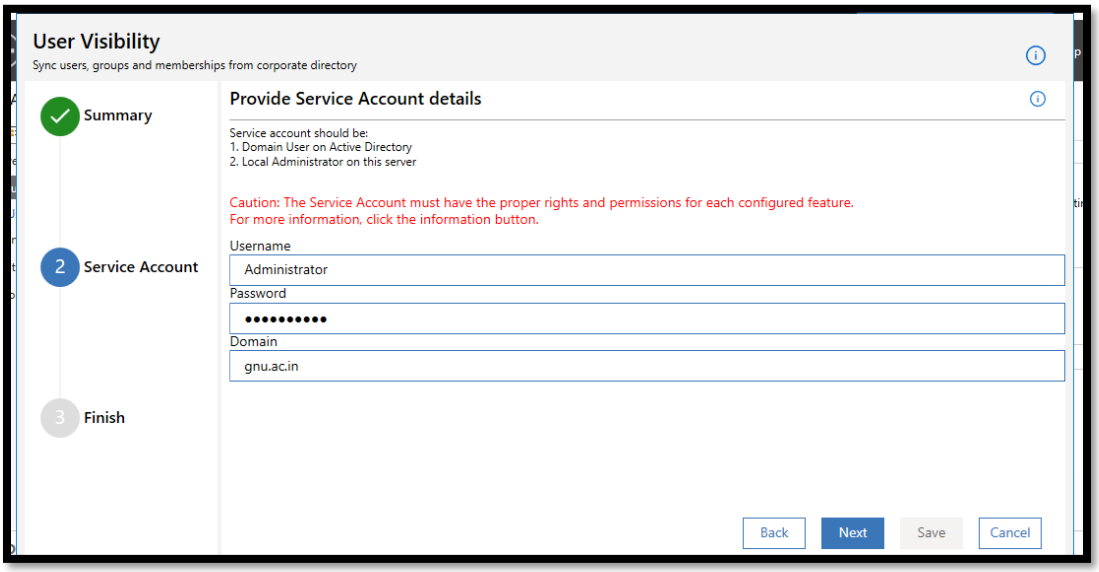


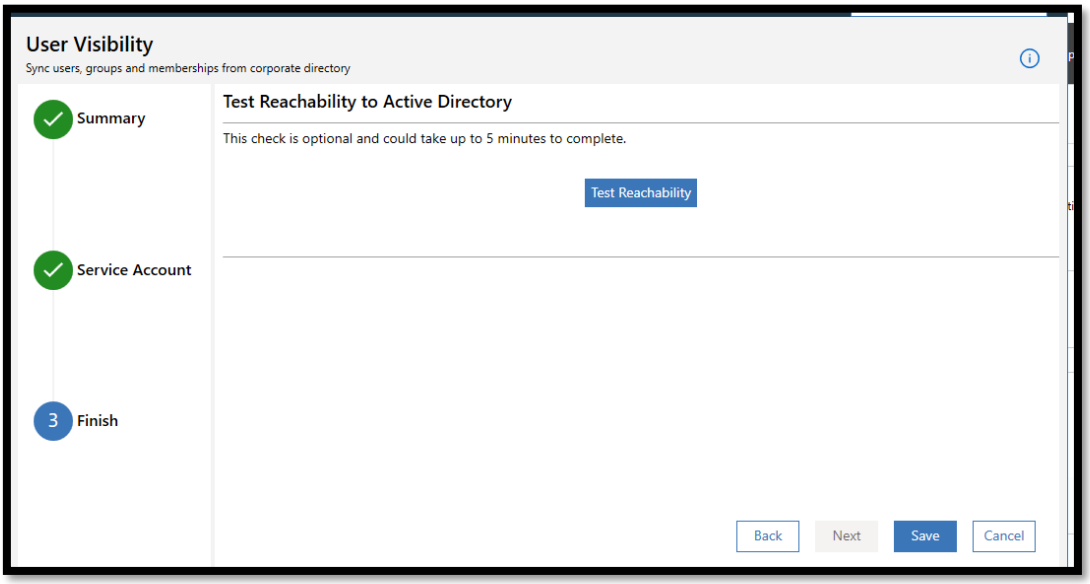
### 6.10.2 User Visibility:

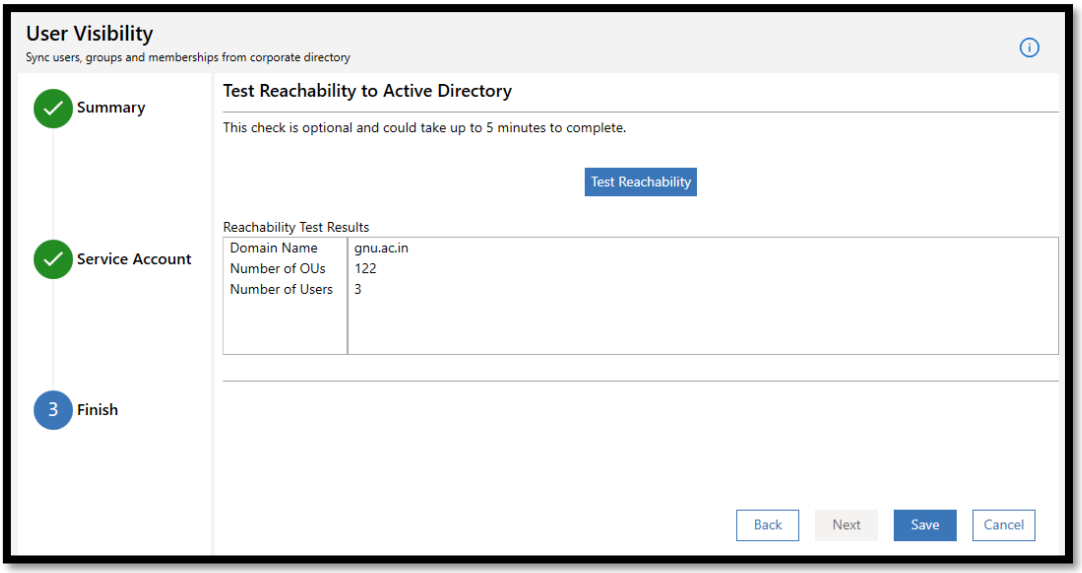
- Select user visibility module in Maas360 and then click on next. The Cloud Extender® prompts you to confirm the scope of the integration.

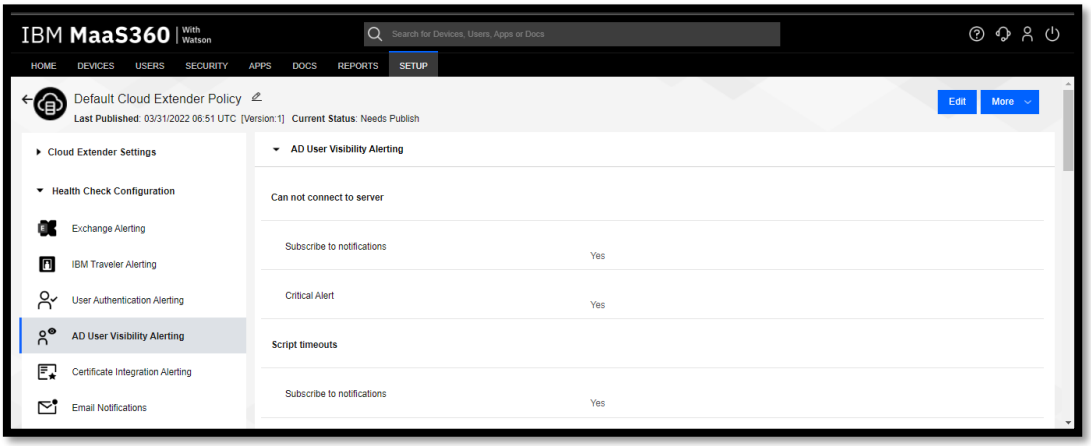



- Choose Basic to see a list of all users and groups in the directory.
- To see if your service account can discover domains, object users (OU), and users, run a reachability test.



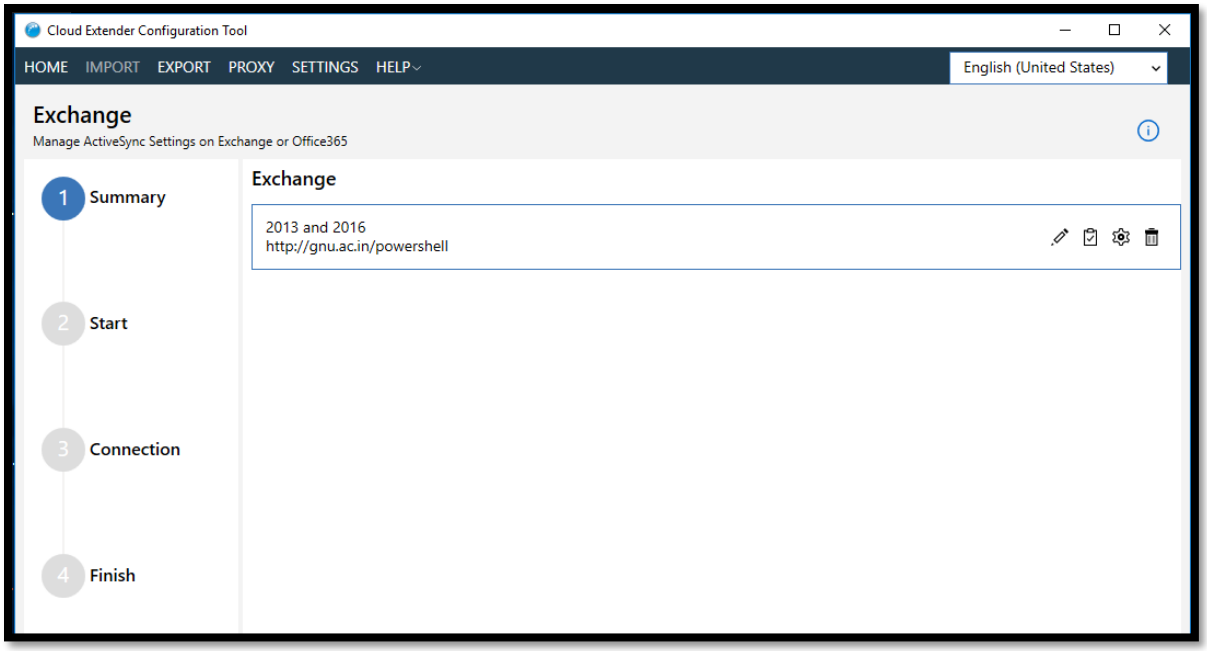

User Visibility
Sync users, groups and memberships from corporate directory
Summary
Service Account
3
Finish
Test Reachability to Active Directory
This check is optional and could take up to 5 minutes to complete.
Test Reachability
Back
Next
Save
Cancel


User Visibility
Sync users, groups and memberships from corporate directory
Summary
Service Account
3
Finish
Test Reachability to Active Directory
This check is optional and could take up to 5 minutes to complete.
Test Reachability
Reachability Test Results
Domain Name
gnu.ac.in
Number of OUs
122
Number of Users
3
Back
Next
Save
Cancel

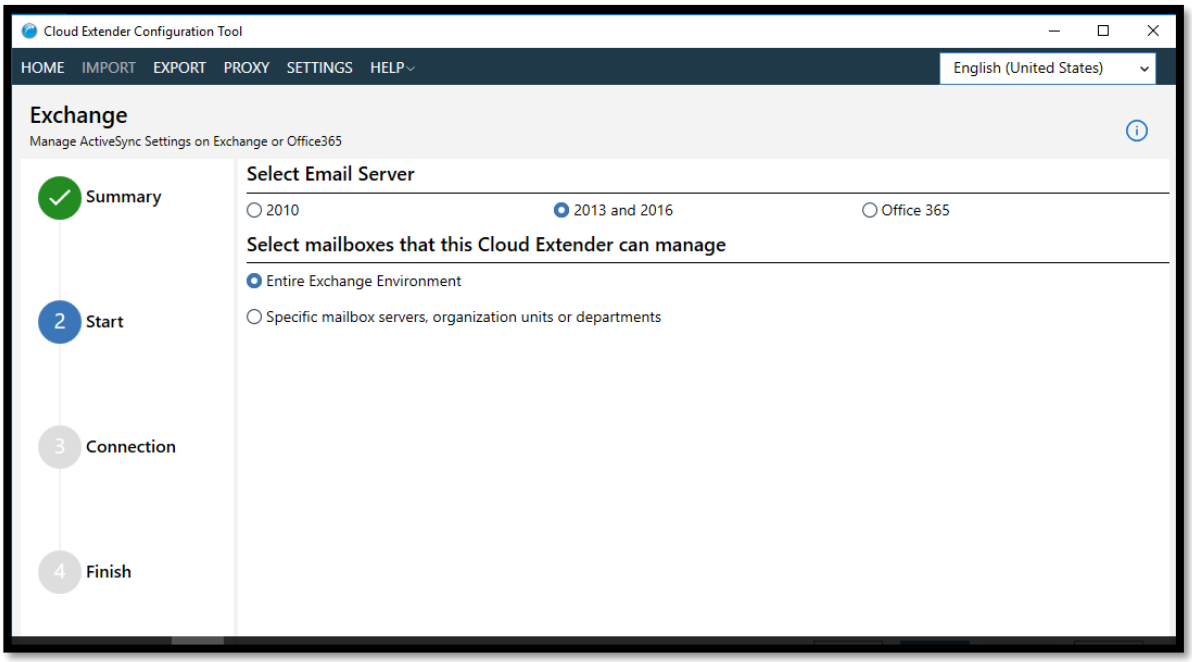

IBM MaaS360
With Watson
Search for Devices, Users, Apps or Docs
HOME
DEVICES
USERS
SECURITY
APPS
DOCS
REPORTS
SETUP
Default Cloud Extender Policy
Last Published: 03/31/2022 06:51 UTC [Version:1] Current Status: Needs Publish
Edit
More
Cloud Extender Settings
Health Check Configuration
Exchange Alerting
IBM Traveler Alerting
User Authentication Alerting
AD User Visibility Alerting
Certificate Integration Alerting
Email Notifications
AD User Visibility Alerting
Can not connect to server
Subscribe to notifications
Yes
Critical Alert
Yes
Script timeouts
Subscribe to notifications
Yes

### 6.10.3 Configure Exchange:

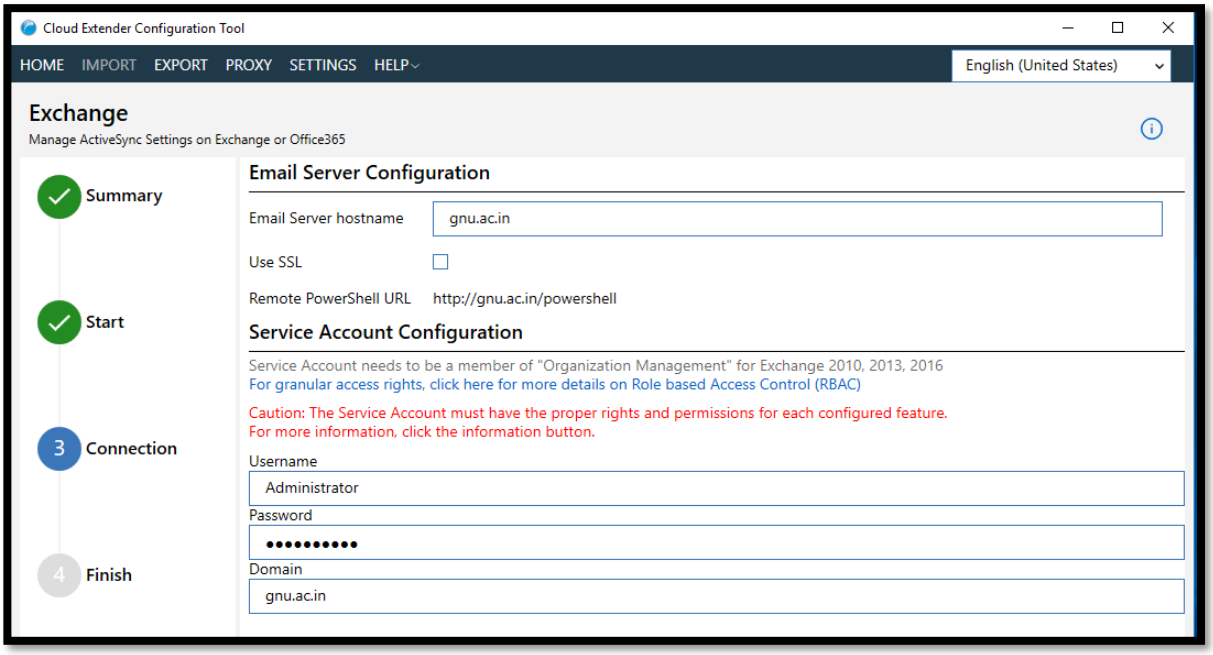
- Open the Cloud Extender Configuration Tool and select **Exchange**.
- Select the version of Exchange that you are using, and click **Next**.




- Now select email server and mail box that cloud extender are using:

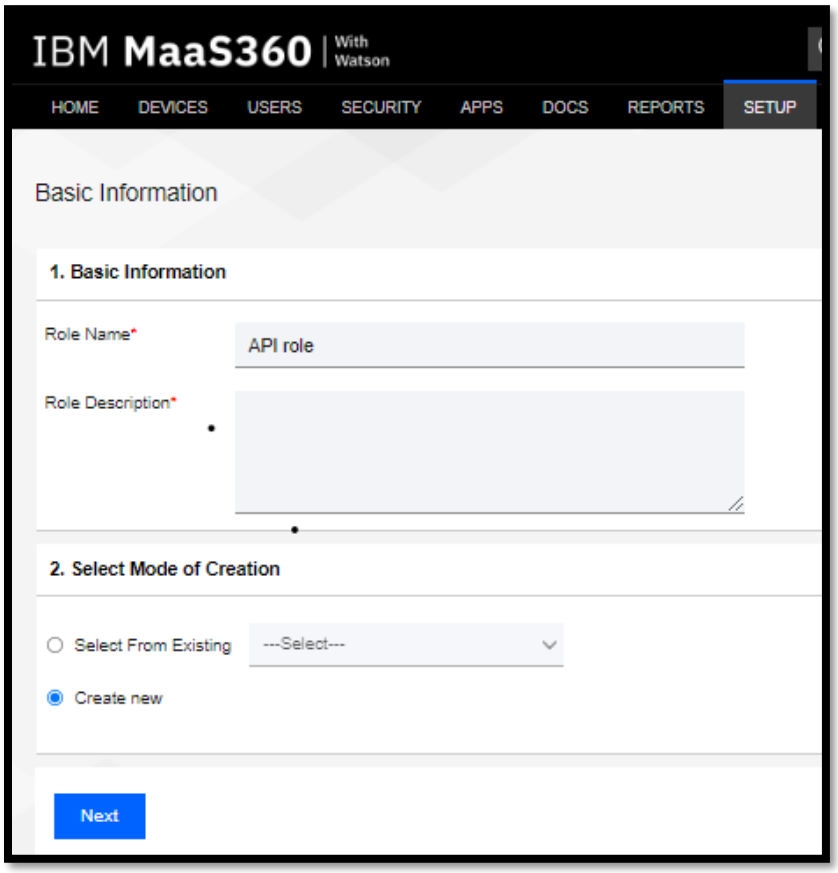


- Click on next and there enter user details and email server configuration:

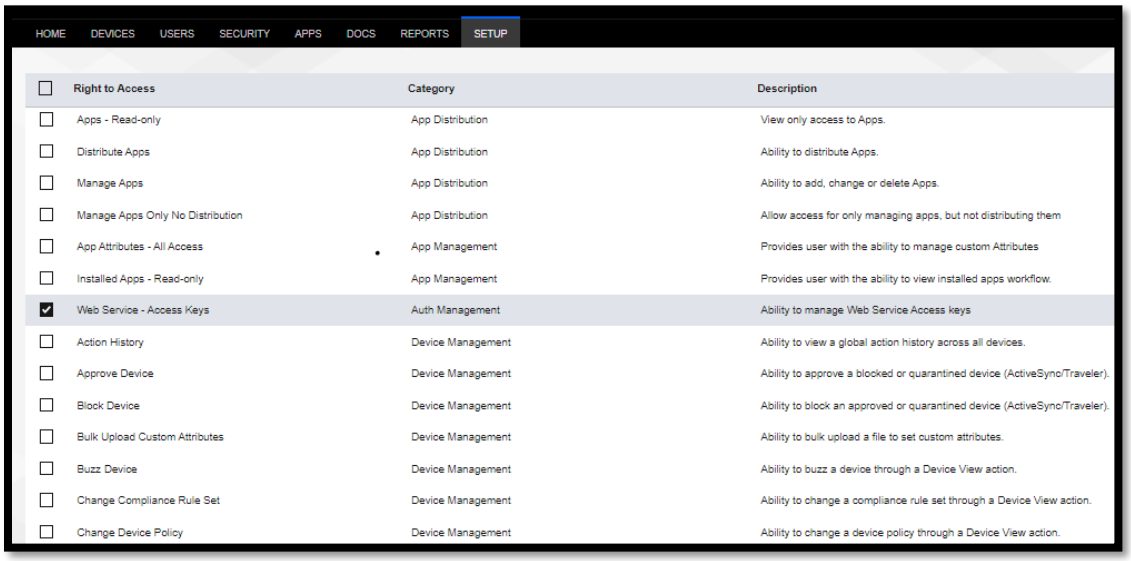


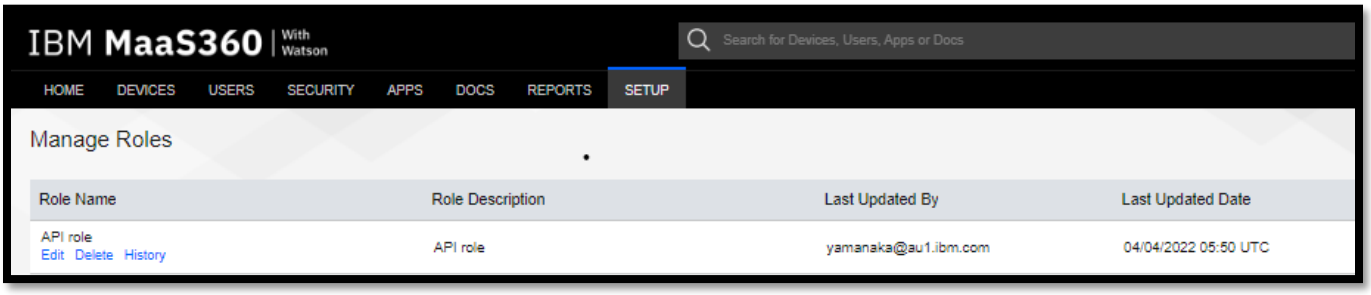
## 6.11 API integration

a. Create API role

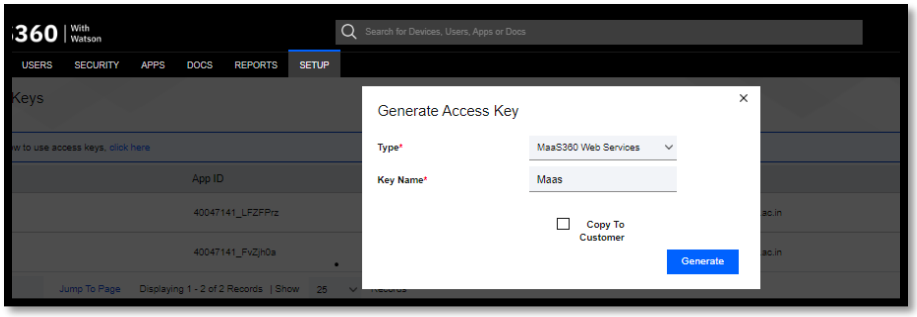


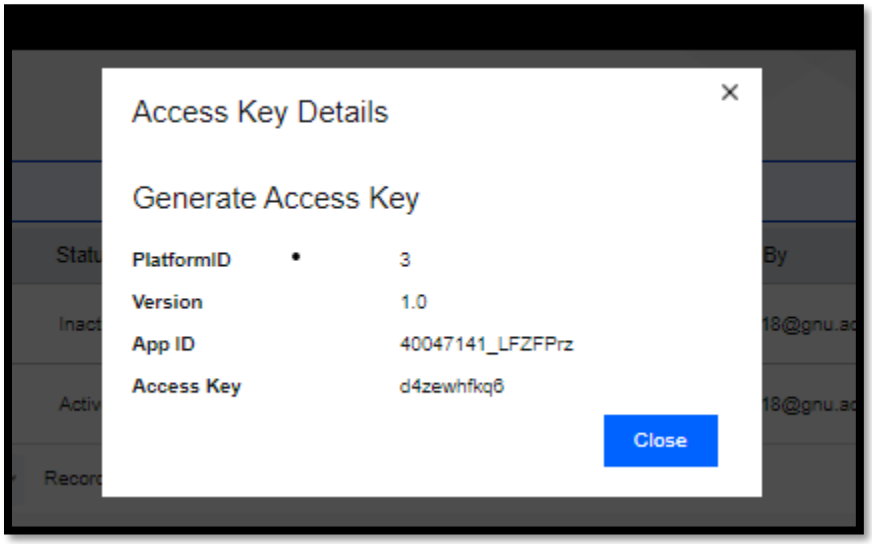

b. Adding Web services access keys



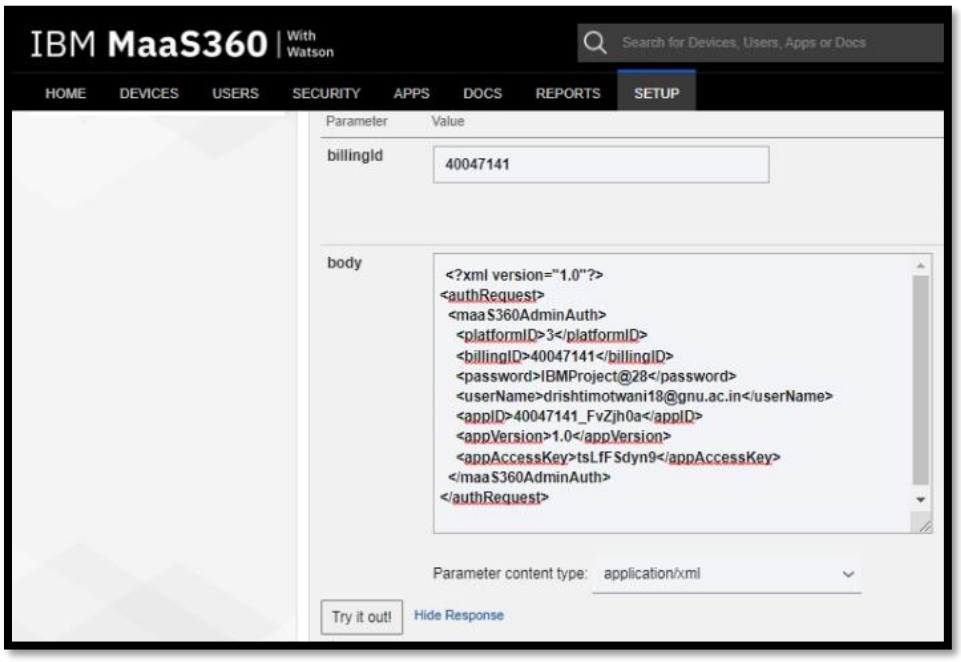


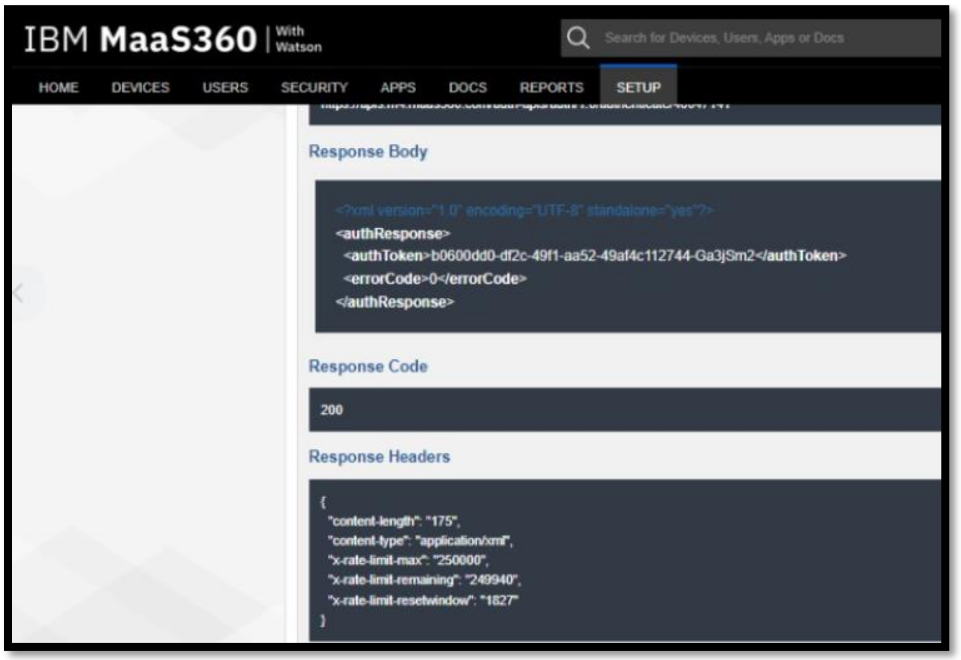

c. Now add this role to the administrator account
d. After that generate access keys



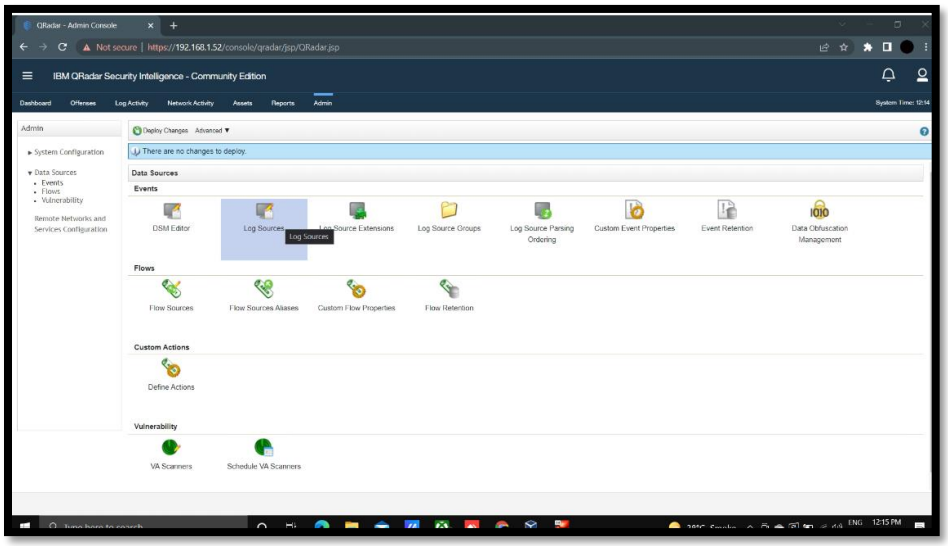



e. Now we can use these details to integrate other tools with MaaS360
f. Checking authentication details for API

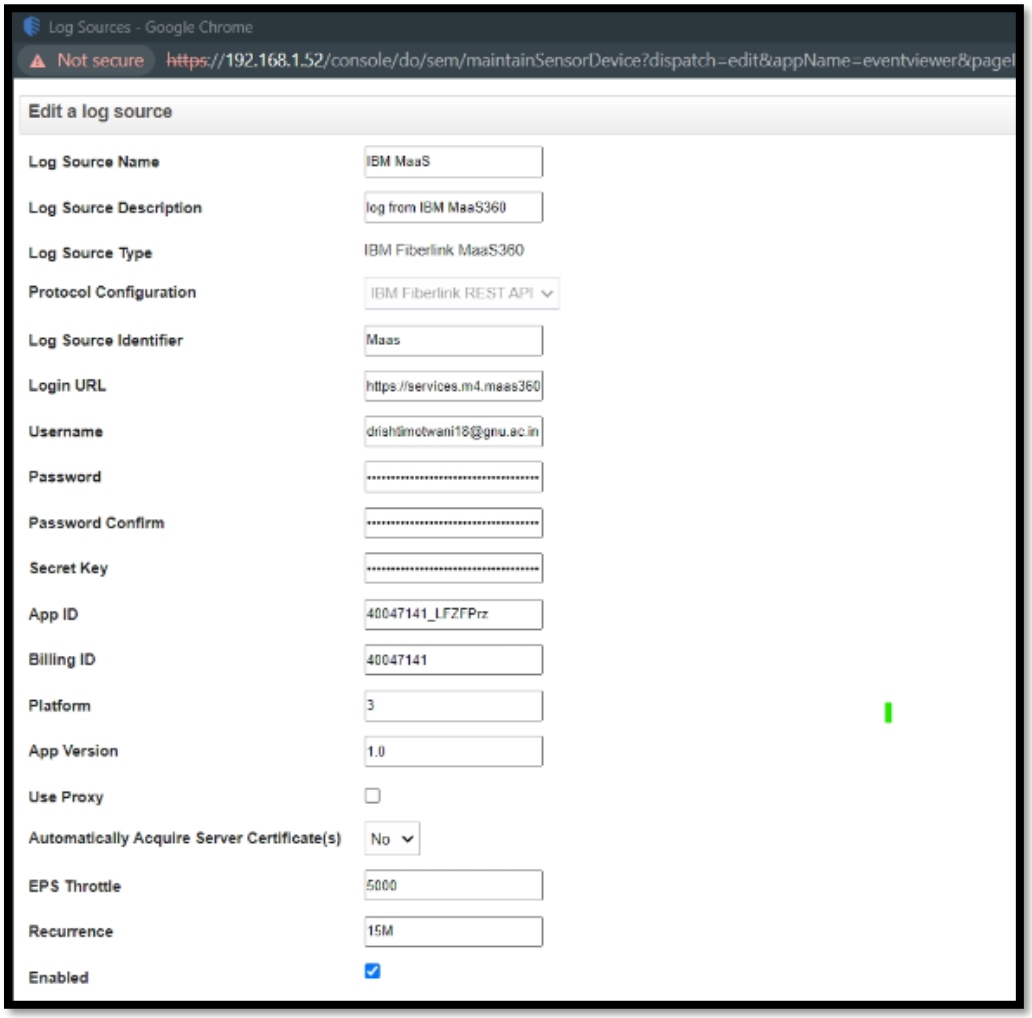


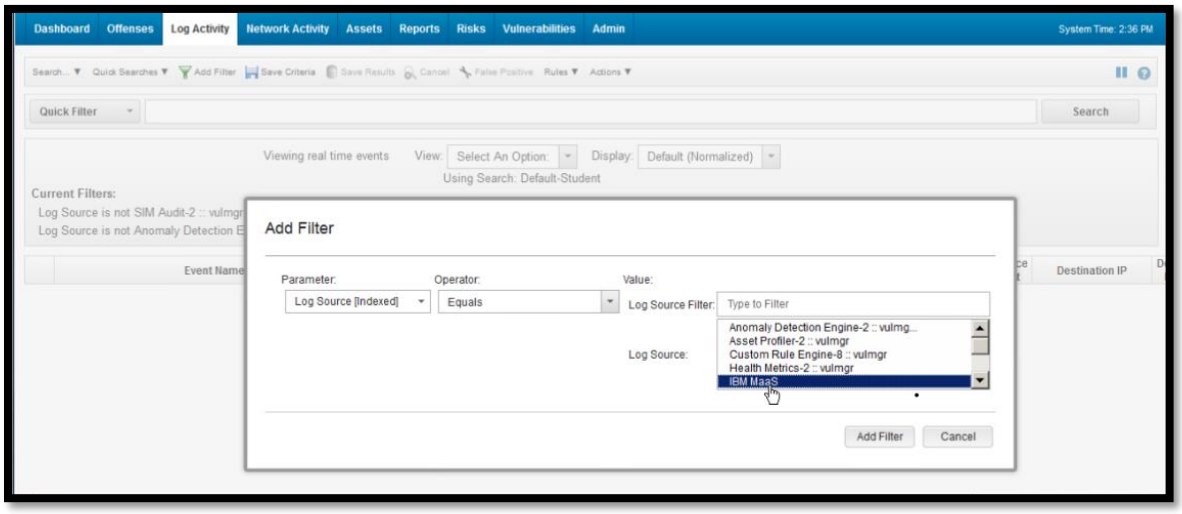
g. To integrate with Qradar go to log sources

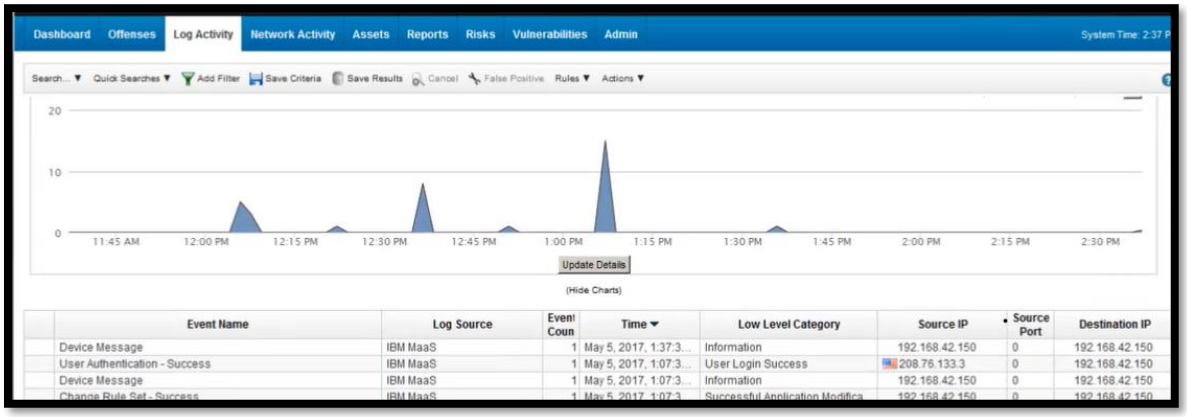



h. Create a new source



i. Click save and check log activity



# CHAPTER: 7 CONCLUSIONS

# CHAPTER7 CONCLUSION

## Conclusion

In the BFSI sector, EMM solutions have gained traction and popularity. However, many BFSI organizations have yet to adopt and deliver business objectives by leveraging mobility's true power. A well-planned EMM strategy in all aspects of workforce management and technology integration equips a BFSI organization to address dynamic market pressures in a rapidly changing industry. It provides an opportunity to reduce overall costs, improve customer experience and productivity, reduce IT deployment burdens, and differentiate organizations from the competition.

# CHAPTER: 8 REFERENCES

## CHAPTER 8 REFERENCES


1) https://www.ibm.com/security/enterprise-mobility-management
2) https://www.ibm.com/docs/en/maas360?topic=guide-getting-started-maas360-portal