

# **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**



Institute of  
Computer  
Technology

## 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**

<b>Title</b>	<b>Page No</b>
<b><u>CHAPTER 1: INTRODUCTION</u></b>	<b>01-03</b>
<b><u>CHAPTER 2: PROJECT SCOPE</u></b>	<b>04-05</b>
<b><u>CHAPTER 3: SOFTWARE AND HARDWARE REQUIREMENT</u></b>	<b>05-06</b>
<b><u>CHAPTER 4: PROCESS MODEL</u></b>	<b>07-08</b>
<b><u>CHAPTER 5: PROJECT PLAN</u></b>	<b>09-10</b>
<b>5.1 List of Major Activities</b>	<b>10</b>
<b>5.2 Estimated Time Duration in Days</b>	<b>10</b>
<b><u>CHAPTER 6: IMPLEMENTATION DETAILS</u></b>	<b>11-78</b>
<b>6.1 Mobile Device Management</b>	
<b>6.1.1 Setup of IBM Maas360</b>	
<b>6.1.2 Android configuration:</b>	
<b>6.1.3 License configuration:</b>	
<b>6.1.4 Users:</b>	
<b>6.1.5 Devices</b>	
<b>6.1.6 Groups</b>	
<b>6.2 Security</b>	
<b>6.2.1 Policies</b>	
<b>6.2.2 Administrative settings</b>	
<b>6.2.3 Android OEM config</b>	
<b>6.3 Mobile Application Management</b>	
<b>6.4 Mobile Content Management</b>	
<b>6.4.1 content library</b>	
<b>6.4.2 managing document</b>	
<b>6.4.3 G drive</b>	
<b>6.5 Secure Browser</b>	
<b>6.6 Remote support for mobile devices and laptop/desktops:</b>	
<b>6.7 Configure End user portal:</b>	
<b>6.8 Configuration of server setup:</b>	
<b>6.9 Configure DNS server:</b>	
<b>6.10 Configuring Cloud extender:</b>	
<b>6.10.1 User authentication:</b>	
<b>6.10.2 User Visibility:</b>	
<b>6.10.3 Configure Exchange:</b>	
<b>6.11 API integration</b>	
<b><u>CHAPTER 7: CONCLUSION AND FUTURE WORK</u></b>	<b>79-80</b>
<b><u>CHAPTER 8: REFERENCE</u></b>	<b>81-82</b>

## **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 specific 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.

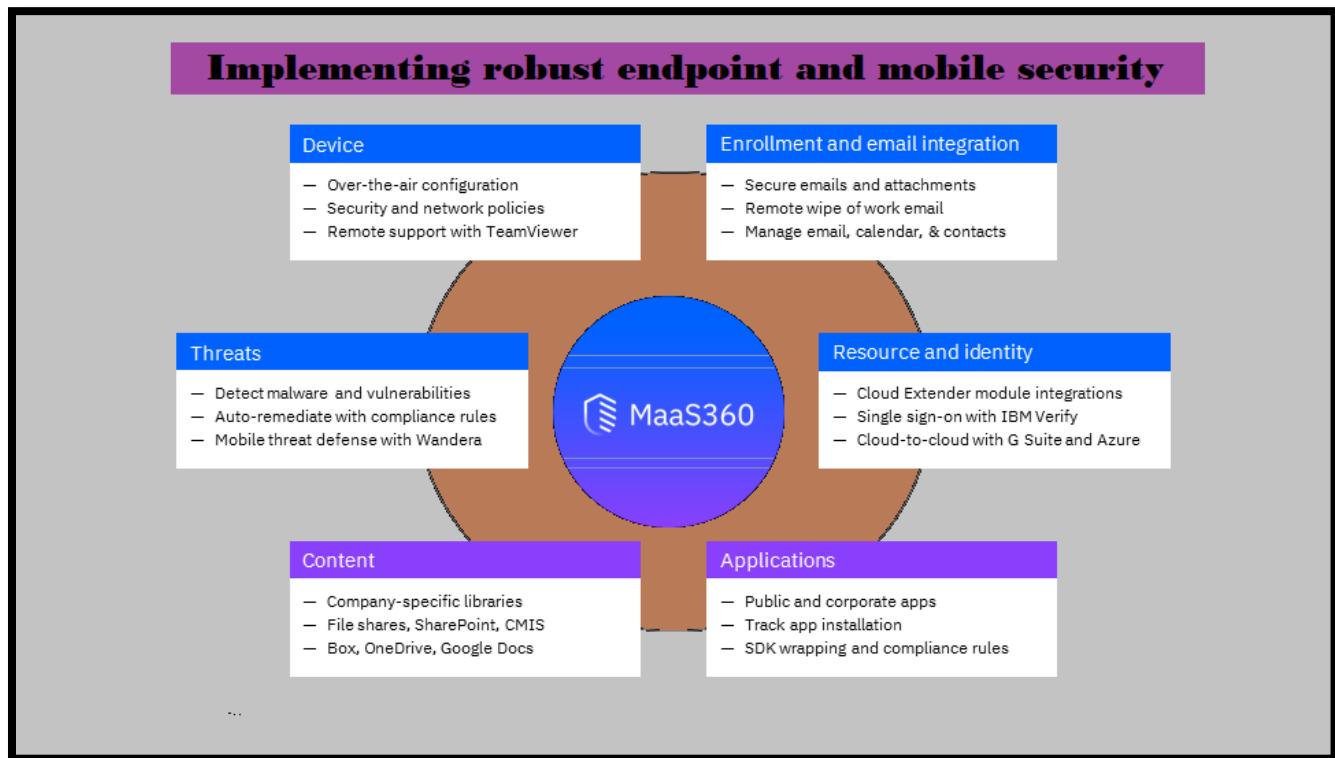
MDM is being used to manage mobile devices but companies can also use UEM. Also, UEM is used for endpoints connected to company networks like routers, servers, the Internet of Things, and wearables devices. If a company has a UEM tool, then it is not required to have an EMM tool as it lowers IT costs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

<b>Processor</b>	4.2 GHz
<b>RAM</b>	16GB
<b>HDD</b>	30GB

*Table 3.1 Minimum Hardware Requirements*

### Minimum Software Requirements for IBM Maas 360

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

*Table 3.2 Minimum Software Requirements*

## **CHAPTER: 4 PROCESS MODEL**

## CHAPTER 4 PROCESS MODEL

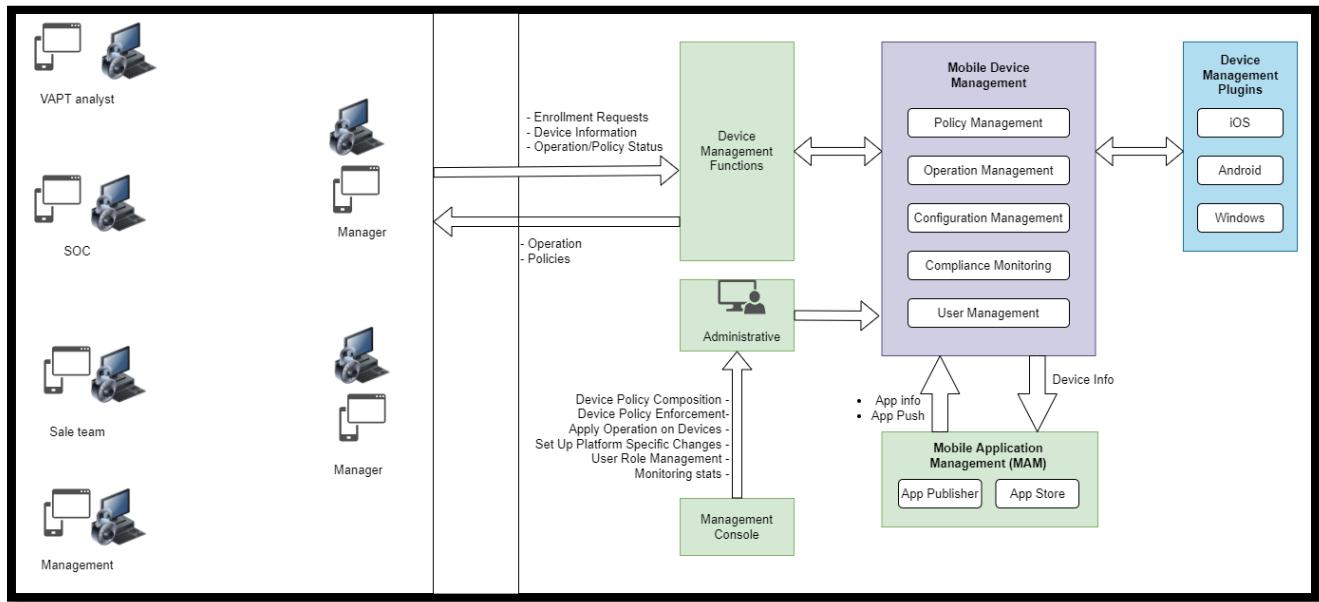


Figure 4.1 Process Model of Project

## **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

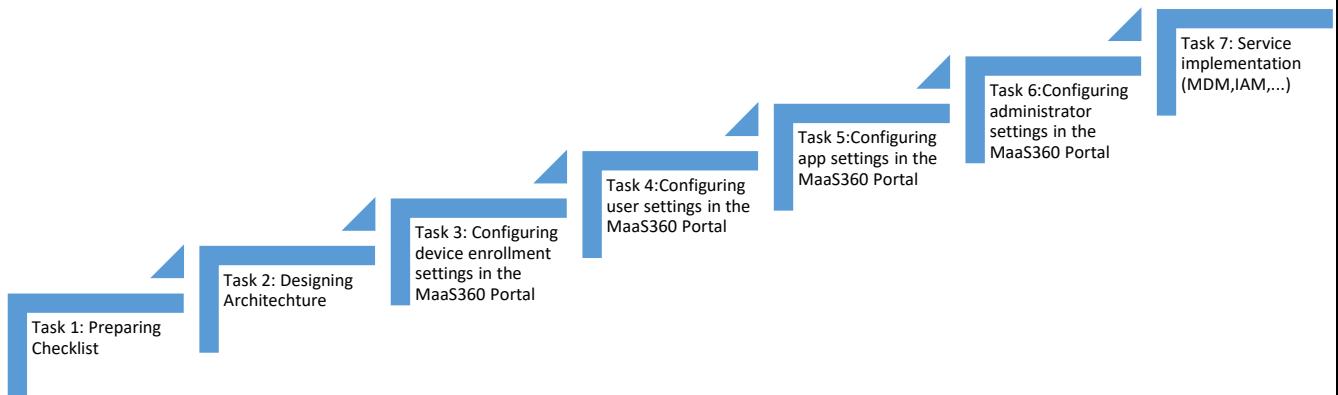


Figure 5.1 Task Completion Estimated Time Duration in Days

## **CHAPTER: 6 IMPLEMENTATION DETAILS**

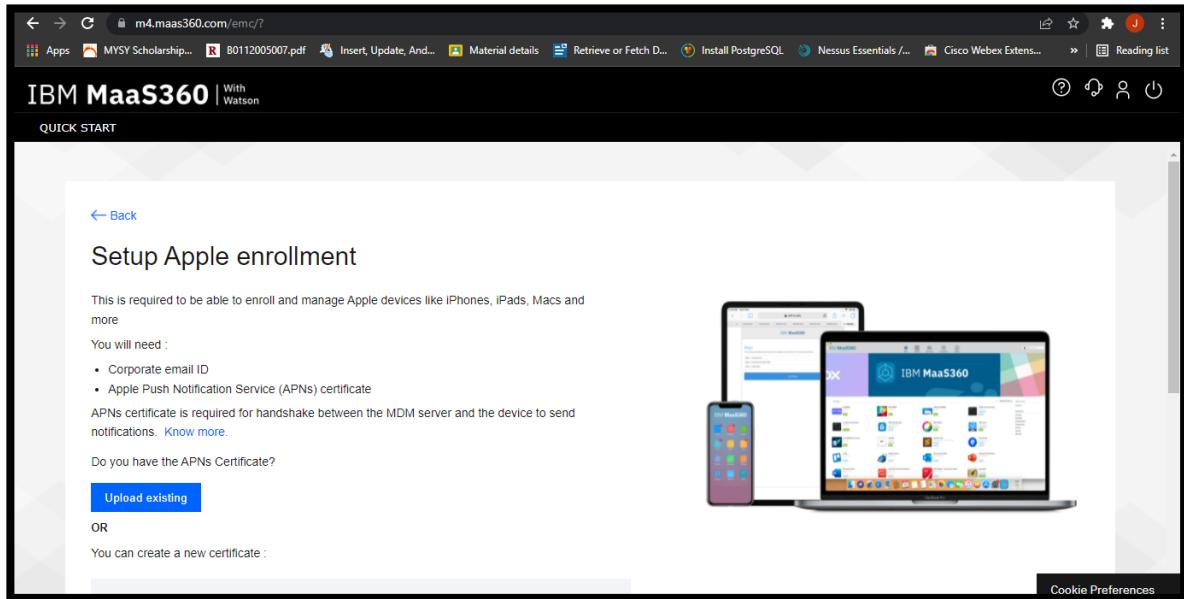
## CHAPTER 6 IMPLEMENTATION DETAIL

### 6.1 Mobile Device Management

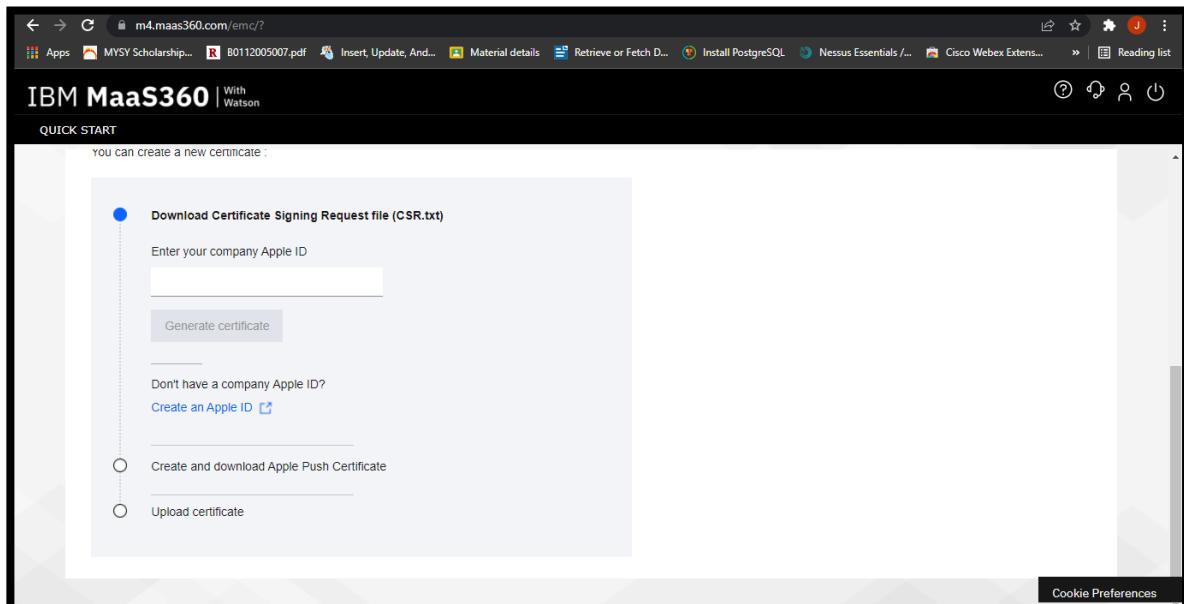
#### 6.1.1 Setup of IBM Maas360

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.

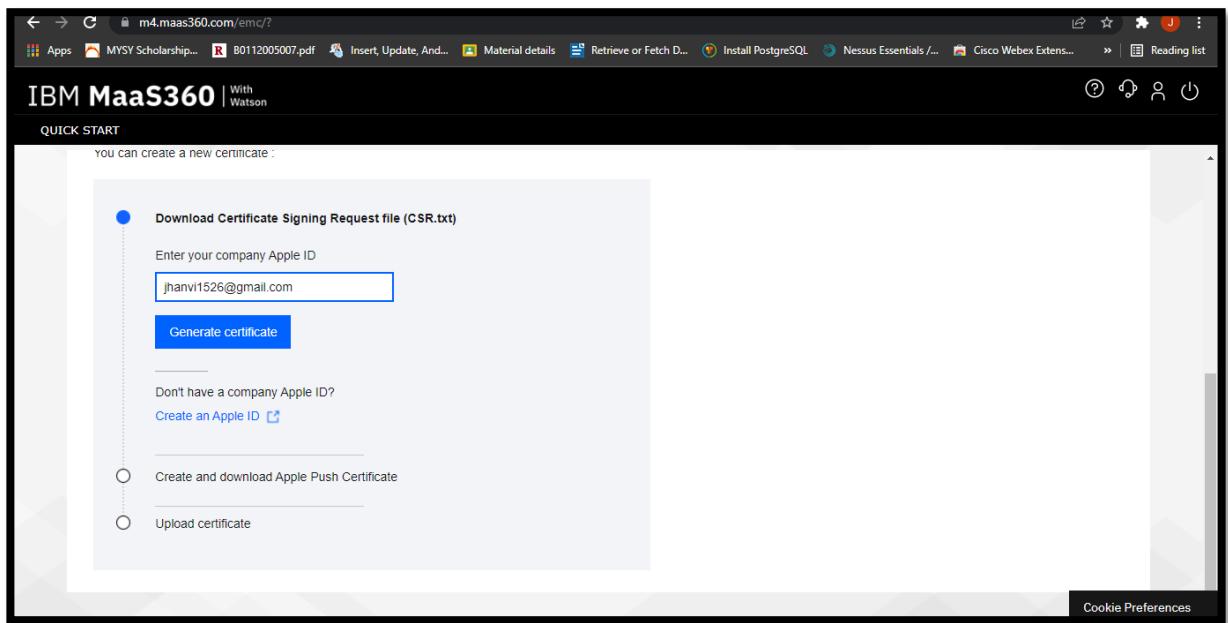
1. Click Setup iOS Now. Use either the Safari, Chrome, or Firefox web browser to download the certificate.



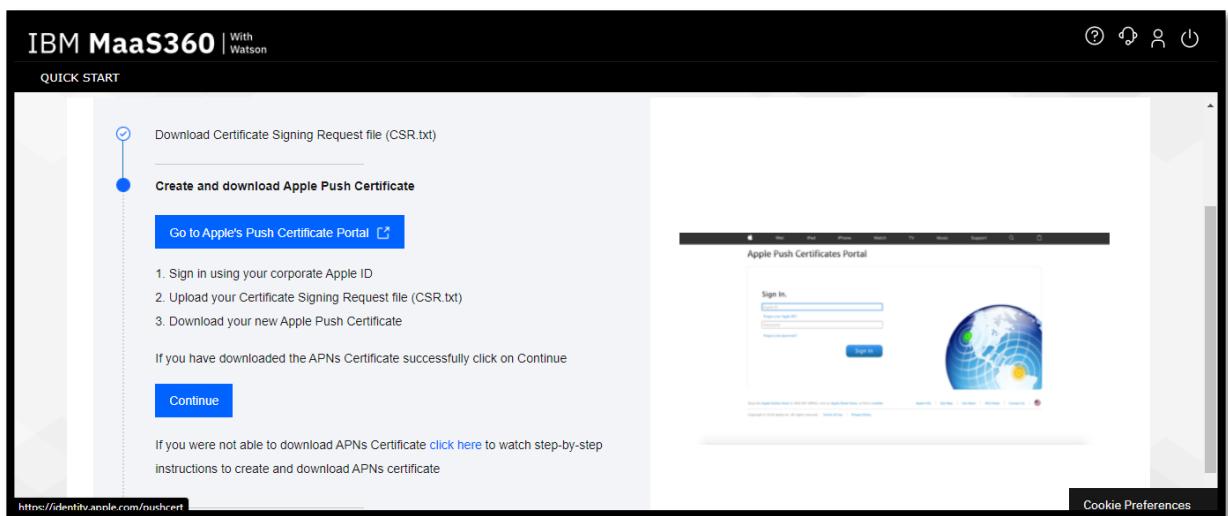
2. Type your corporate Apple ID and click Next. You must use the same Apple ID every year when you renew your APNs certificate. If you do not have an Apple ID, mouse over Create ID and click Apple Website to access a page where you create a corporate Apple ID.



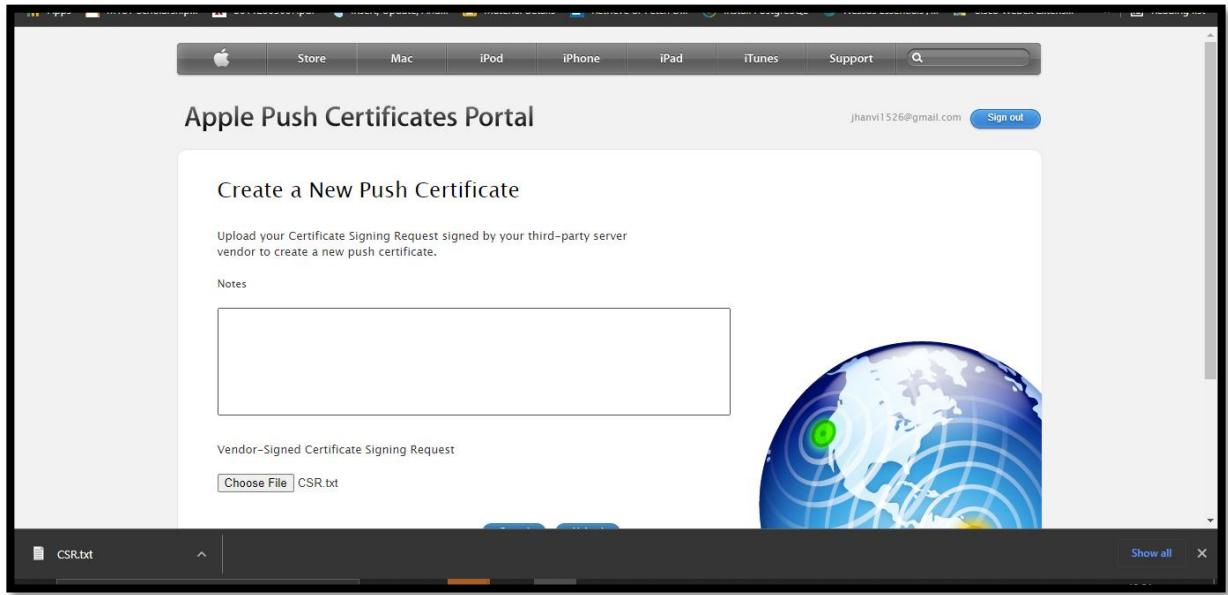
3. To create a PEM file. Click on generate a Certificate.



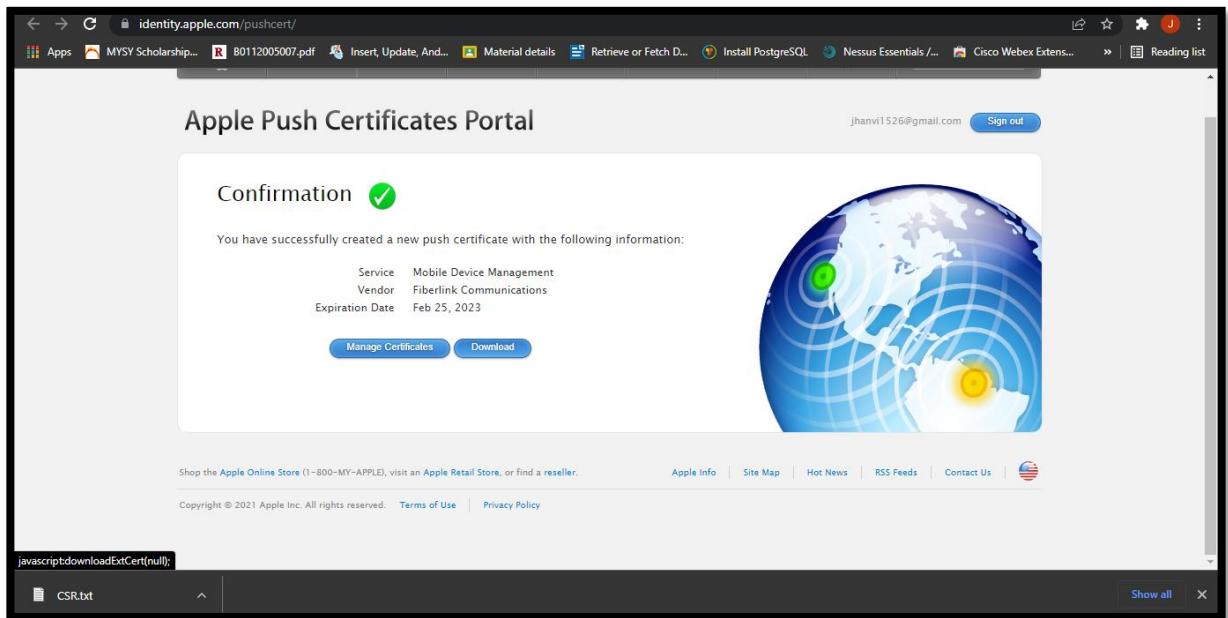
4. After you've completed the previous step. Accept the terms and conditions by checking the box. Then press the accept button.



- 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.
- Click Open, and then click Upload.

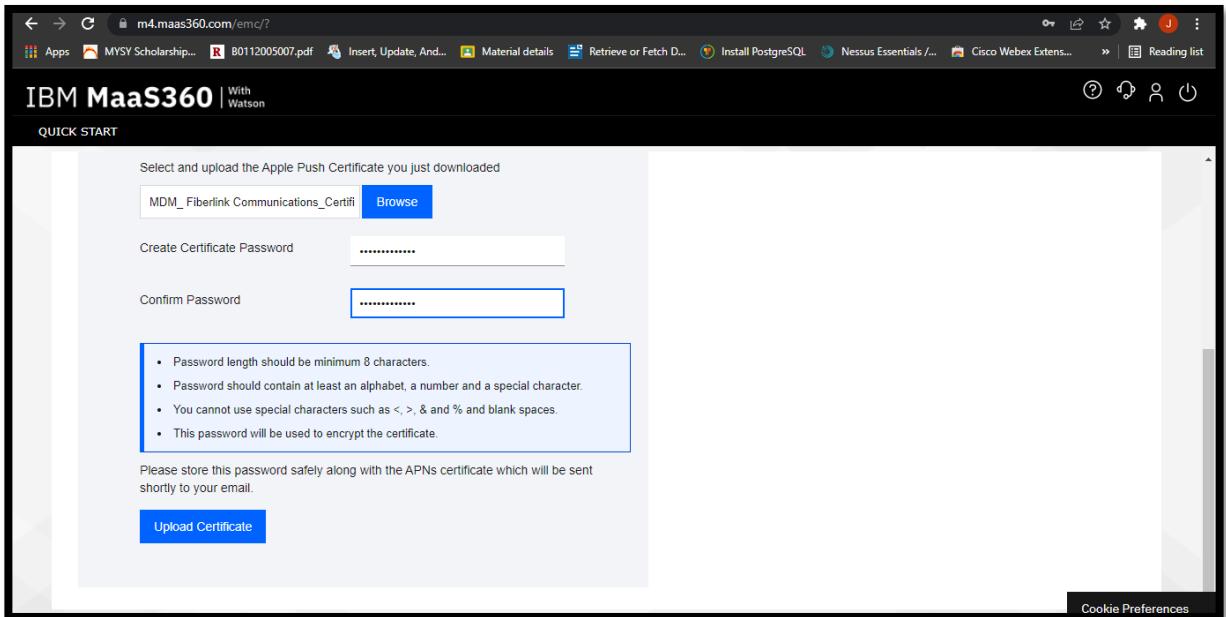


- Click Download to download the PEM file.

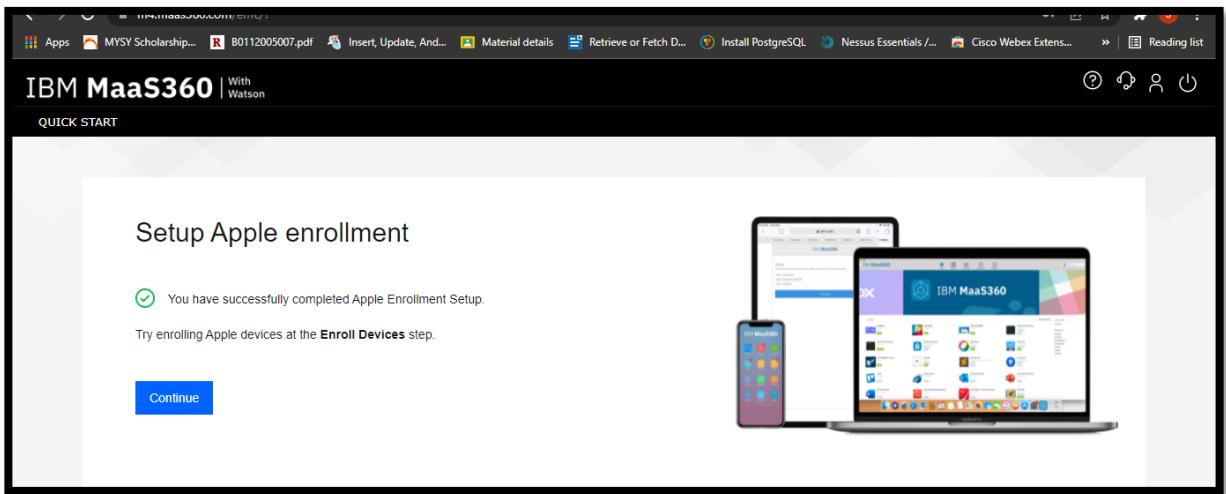


- Click OK to save the PEM file to your Downloads folder, and then click Next.
- Click Browse to upload the certificate to MaaS360.

10. Locate the MDM\_Fiberlink\_Communications.pem file in your Downloads folder, and then click Open.



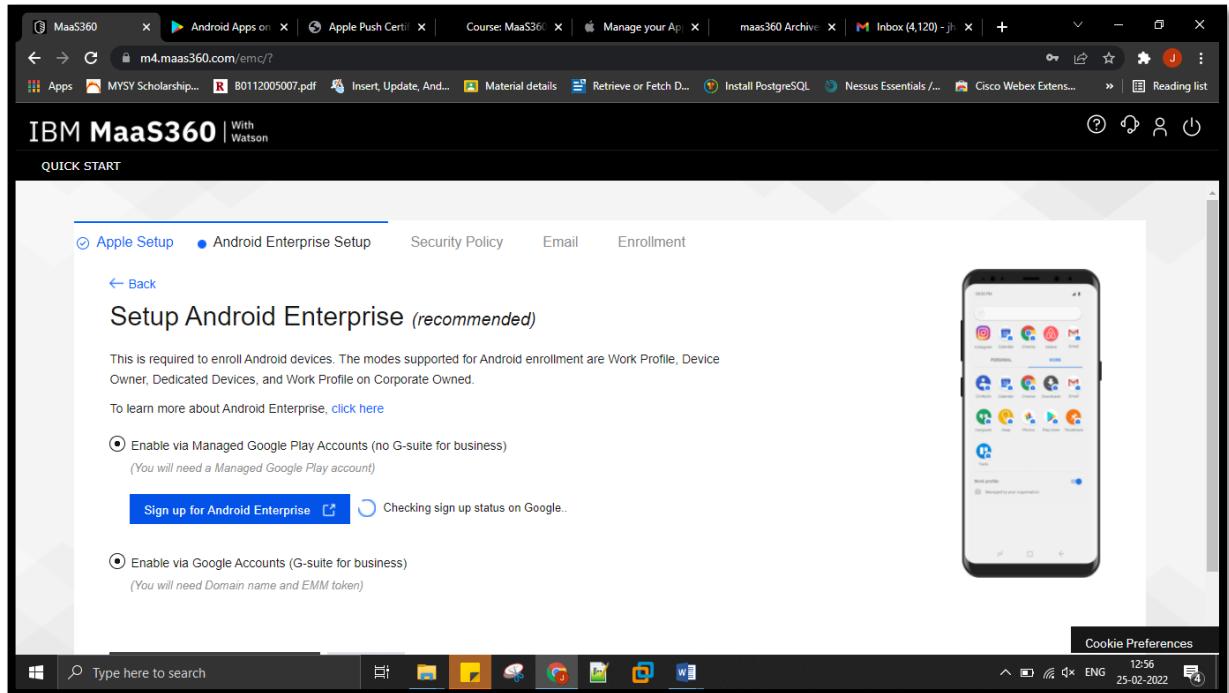
11. Type a password, and then click Upload. Note: This password has no minimum security requirement. To help you remember the password, you might want to use the password that you used for your Apple ID password. The APNs certificate is created.



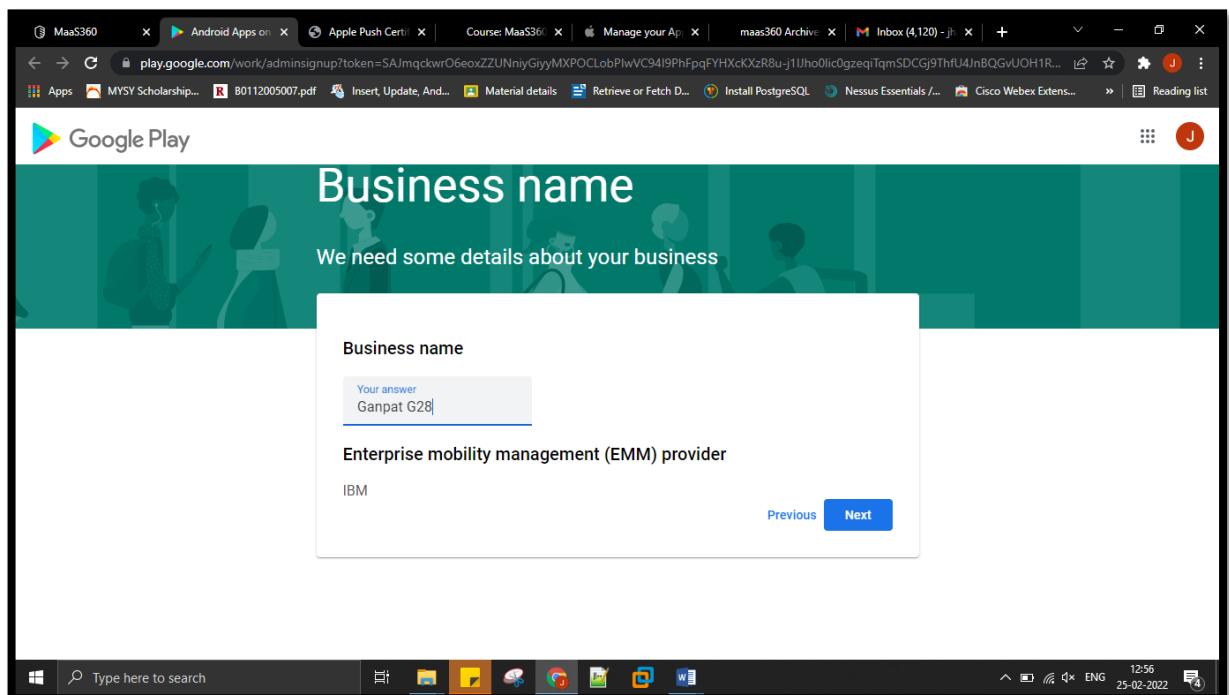
12. Click Close.

### 6.1.2 Android configuration:

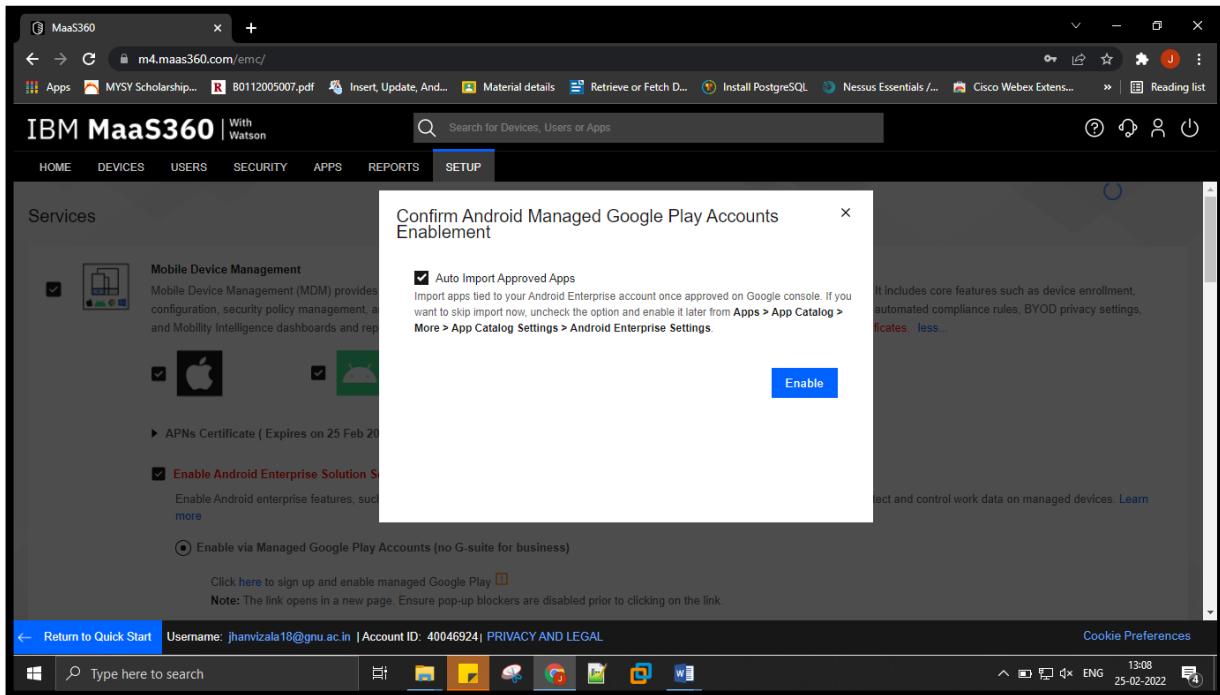
1. To navigate to MDM service. Go to Setup > Services > Mobile Device Management, and then select Enable Android for Work > Enable via Google Accounts.



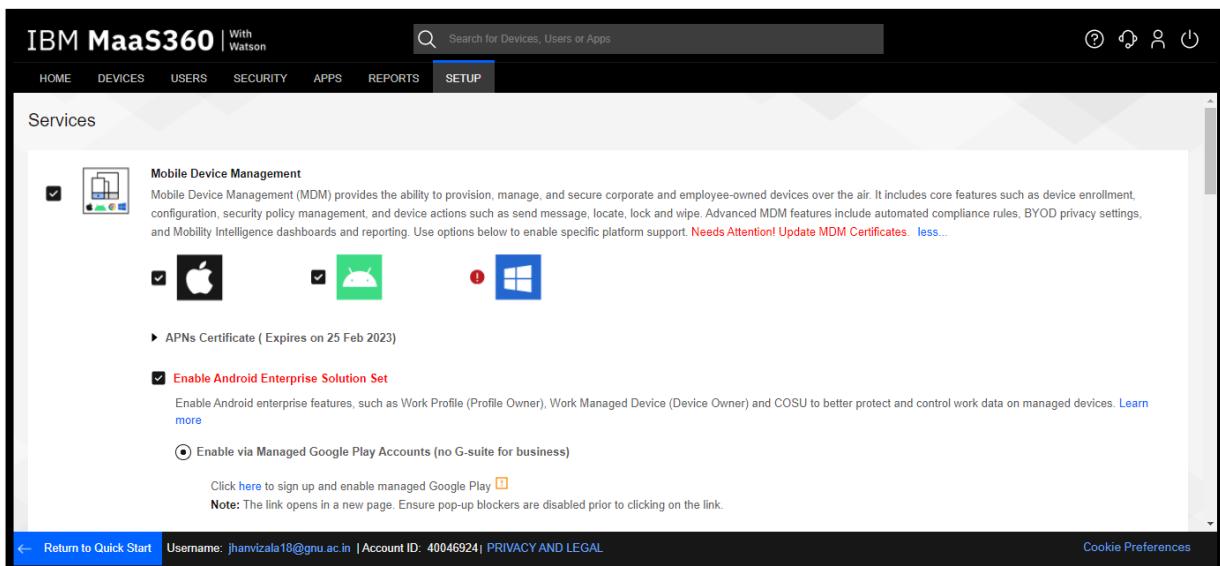
2. Go to the G Suite Admin console (admin.google.com), and then enable the Android Enterprise app (enabled by default in the standalone version of Android Enterprise). You can manage the EMM provider from the Billing subscriptions, which is a free service.



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**:

The screenshot shows the IBM MaaS360 interface with the URL m4.maas360.com/emc/#. The top navigation bar includes links for Apps, MYSY Scholarship..., Insert, Update, And..., Material details, Retrieve or Fetch D..., Install PostgreSQL, Nessus Essentials ..., Cisco Webex Extens..., and a Reading list. The main menu has options like HOME, DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP, with SETUP being the active tab. On the left, a sidebar titled 'Settings' lists categories: Directory and Enrollment, User Settings, App Settings, Doc Settings, Administrator Settings, and License settings. Under License settings, 'Basic' is selected. The main content area has sections for 'Overage settings' (with a note about enabling extra device enrollment) and 'Default licenses for bulk and self enrollments'. A dropdown menu under 'Select base license' shows 'EMM Trial' as the current selection. At the bottom, there's a note to 'Select add on licenses'. The footer displays the username jhanvizala18@gnu.ac.in, Account ID 40046924, Last Login Friday, March 4, 2022 12:16:36 PM IST, and links for PRIVACY AND LEGAL and Cookie Preferences.

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.

The screenshot shows the 'License Overview' page in the IBM MaaS360 portal. The table displays the following data:

MaaS360 Part Name	License Type	MaaS360 Part Number	Units Purchased	Units Consumed
EMM Trial	Trial	D1P3TRL	10000	11

Below the table, there are navigation buttons (Back, Forward, Home) and a search bar. At the top right, there are buttons for 'Licenses To be Assigned' and 'Export Assigned Licenses'.

The screenshot shows the 'EMM Trial' details page. It includes sections for 'MaaS360 Part Details' and 'Subscription Details'.

**MaaS360 Part Details:**

MaaS360 Part Name	EMM Trial	Units Purchased	10000	MaaS360 Part Number	D1P3TRL
Units Consumed	11	Overage Allowed	Yes	Units Available	9989

**Subscription Details:**

Subscription State	Subscription ID	Charge Agreement Nu...	Subscription Start Date	Subscription End Date	Units Purchased
Active	508090882	null	02/25/2022 00:00 UTC	03/27/2022 00:00 UTC	10000

The screenshot shows the 'License Overview' page again, but with a modal dialog open over it. The dialog is titled 'Export Assigned Licenses' and contains the message: 'Click Confirm to request the License Assignment Report over Email.' At the bottom of the dialog are two buttons: 'Cancel' and 'Confirm'.

#### 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.

The screenshot shows the 'User Directory' page of the IBM Maas360 web interface. At the top, there's a navigation bar with links for HOME, DEVICES, USERS (which is selected), SECURITY, APPS, DOCS, REPORTS, and SETUP. Below the navigation is a search bar labeled 'Search for Devices, Users, Apps or Docs'. A sidebar on the left lists various system components like 'Cloud Extender', 'Nessus Essentials', and 'Cisco Webex'. The main content area is titled 'User Directory' and contains a table of user information. The columns are: Username, Full Name, Domain, Email Address, Status, User Source, and Last Updated Date. The table lists several users, each with a 'View' link and other options like 'Add Device', 'Change Policy', and 'More...'. The last user listed is 'kavya'.

Username	Full Name	Domain	Email Address	Status	User Source	Last Updated Date
administrator	Administrator	gnu.ac.in	-	Active	User Directory (AD)	03/10/2022 16:31 IST
dhwani	Dhwani Patel	gnu.ac.in	dhwaniplate18@gnu.ac.in	Active	Local Directory	02/25/2022 16:51 IST
drishti	Drishti Motwani	gnu.ac.in	drishitmotwani18@gnu.ac.in	Active	Local Directory	02/27/2022 13:18 IST
jatin	Jatin Bhimani	gnu.ac.in	jatinbihmani18@gnu.ac.in	Active	Local Directory	02/27/2022 17:15 IST
jhanviz	Jhanvi Zala	gnu.ac.in	jhanvizala18@gnu.ac.in	Active	Local Directory	03/08/2022 12:21 IST
jhanvizala18	Jhanvi M. Zala	gnu.ac.in	-	Active	User Directory (AD)	03/10/2022 16:31 IST
kavya	Kavya Patel	gnu.ac.in	kavyakumarpatel18@gnu.ac.in	Active	Local Directory	02/25/2022 17:42 IST

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.

The screenshot shows the 'Add User' dialog box. It has two tabs: 'Basic' (which is selected) and 'Advanced'. The 'Basic' tab contains fields for: Full Name (with placeholder 'Enter full name'), Username\* (placeholder 'Enter corporate username'), Domain\* (placeholder 'Enter corporate domain'), Email\* (placeholder 'Enter email address'), Managed Apple ID (placeholder 'Enter Managed Apple ID'), Authentication Type\* (dropdown menu showing 'MaaS360'), User Groups (text input field with placeholder 'Enter a few characters of Group Name'), WorkPlace Persona Policy (dropdown menu), Phone Number (input field with '+1' and 'Phone Number' placeholder), and Location (input field with placeholder 'Enter office location'). On the right side of the dialog, there's a sidebar titled 'User Source' with a list of options: 'User Directory (AD)', 'Local Directory', 'Local Directory', 'Local Directory', 'User Directory (AD)', and 'Local Directory'.

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.

The screenshot shows a configuration interface with the following fields:

- WorkPlace Persona Policy:** A dropdown menu labeled "Select Policy".
- Platform & MDM Policy:** Two dropdown menus: "Select Platform" and "Select Policy".
- Compliance Rule Set:** A dropdown menu labeled "Select Rule Set".
- Device Ownership:** A dropdown menu labeled "Corporate".
- Comments:** A text area with the placeholder "Comments (255 characters max.)".

At the bottom right are two buttons: "Cancel" and "Send Request".

### 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.

- 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.

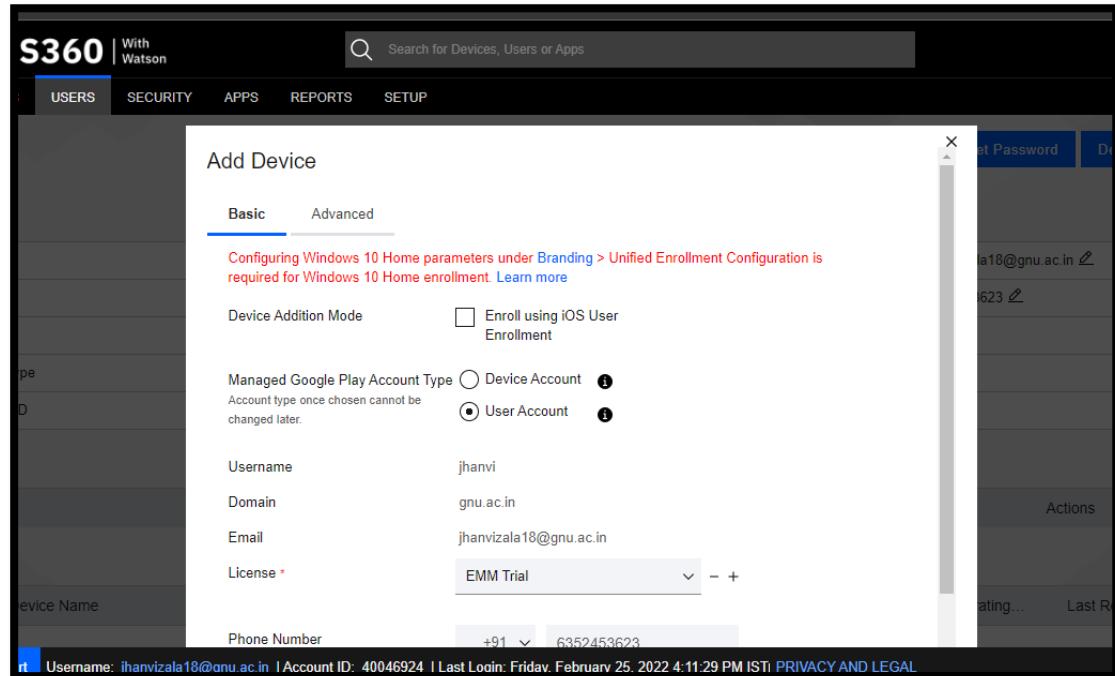
Device Name	Username	Platform	Model	Operating S...	Installed Date	Last Reported	Mailbox Ma...	Email Address	Managed St...
DESKTOP-TJ	tejas	💻	HP 240 G6 Notebook PC	Windows 10 Pro	02/27/2022 15:01 IST	03/10/2022 23:09 IST	No	tejastripathi18@gnu.ac.in	Enrolled
RAHUL	rahul	💻	HP 240 G6 Notebook PC	Windows 11 Pro	02/27/2022 17:42 IST	03/10/2022 23:04 IST	No	rahulprajapati18@gnu.ac.in	Enrolled
PATEL	rutvik	💻	HP 240 G6 Notebook PC	Windows 10 Pro	02/27/2022 13:13 IST	03/10/2022 23:01 IST	No	rutvikkumarpatel18@gnu.ac.in	Enrolled
rutvik-SM-M405F	rutvik	📱	SM-M405F	Android 11 (RP1A.200720.012)	02/27/2022 13:14 IST	03/10/2022 21:58 IST	No	rutvikkumarpatel18@gnu.ac.in	Enrolled
tanvi-SM-J810G	tanvi	📱	SM-J810G	Android 10 (QP1A.190711.020)	02/25/2022 22:36 IST	03/10/2022 20:45 IST	No	tanvibentivedi18@gnu.ac.in	Enrolled
dhwani-vivo 1804	dhwani	📱	vivo 1804	Android 10 (QP1A.190711.020)	02/25/2022 16:56 IST	03/10/2022 20:08 IST	No	dhwaniapatel18@gnu.ac.in	Enrolled
jhanviz-SM-M305F	jhanviz	📱	SM-M305F	Android 10 (QP1A.190711.020)	03/04/2022 14:35 IST	03/08/2022 12:27 IST	No	jhanvizada18@gnu.ac.in	Enrolled
drishti-POCO F1	drishti	📱	POCO F1	Android 10 (QKQ1.190828.002)	02/27/2022 10:22 IST	03/08/2022 12:14 IST	No	drishtimotwani18@gnu.ac.in	Enrolled
DESKTOP-6GKT46R	jatin	💻	HP 240 G6 Notebook PC	Windows 10 Pro	02/27/2022 17:26 IST	03/08/2022 12:03 IST	No	jatinbhiman18@gnu.ac.in	Enrolled

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

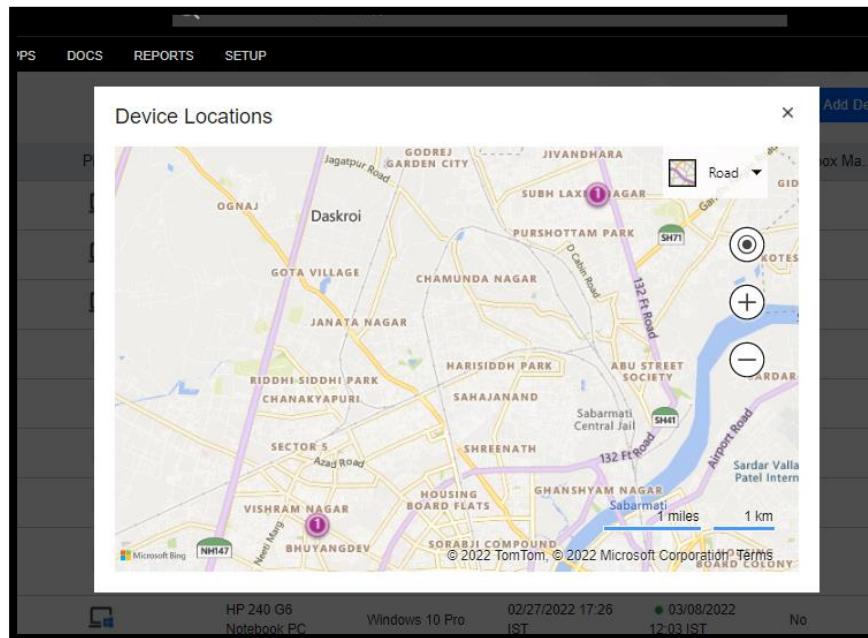
- Select the column header and filter for a specific type of device. For example, select the Platform column and then sort devices based on the device operating system.

Username	Platform	Model	Operating S...	Installed Date	Last...
tejas	Sort ascending	240 G6 ebook PC	Windows 10 Pro	02/27/2022 15:01 IST	23:09 IST
rahul	Sort descending	240 G6 ebook PC	Windows 11 Pro	02/27/2022 17:42 IST	23:04 IST
rutvik	iOS	240 G6 ebook PC	Windows 10 Pro	02/27/2022 13:13 IST	23:01 IST
rutvik	Android	M405F	Android 11 (RP1A.200720.012)	02/27/2022 13:14 IST	21:58 IST
tanvi	Windows Phone	J810G	Android 10 (QP1A.190711.020)	02/25/2022 22:36 IST	20:45 IST
dhwani	macOS	1804	Android 10 (QP1A.190711.020)	02/25/2022 16:56 IST	20:08 IST
jhanviz	Windows Laptops	M305F	Android 10 (QP1A.190711.020)	03/04/2022 14:35 IST	12:27 IST
drishti	Others	POCO F1	Android 10 (QKQ1.190828.002)	02/27/2022 10:22 IST	12:14 IST
jatin		HP 240 G6	Windows 10 Pro	02/27/2022 17:26 IST	23:03 IST

- 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.

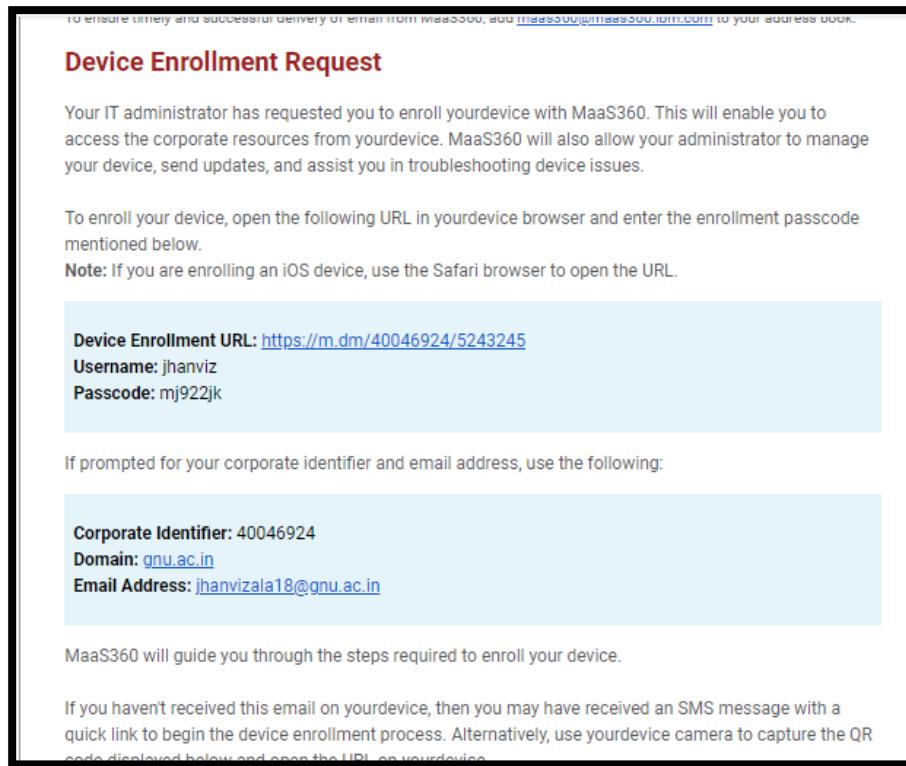


- Click Delete Device to delete an inactive device.
- Click More > Directory and Enrollment to configure the default authentication mode, unified enrollment settings, advanced management settings, and more enrollment settings for iOS, Android, Windows, and other devices.

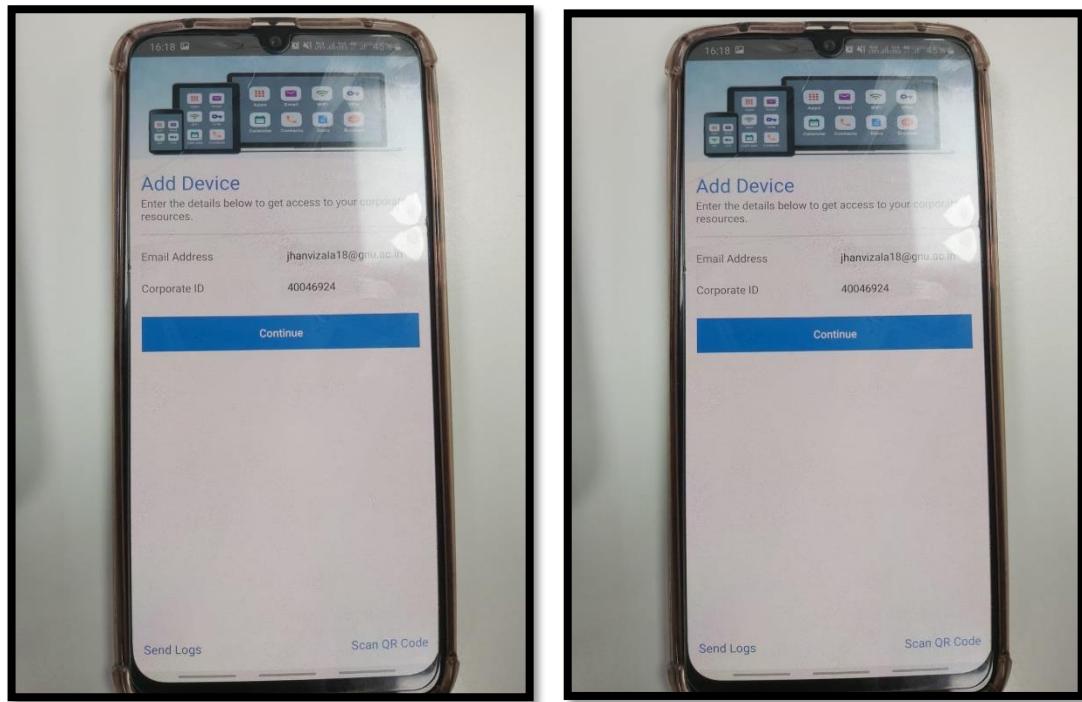
The screenshot shows the IBM MaaS360 web interface. The top navigation bar includes links for HOME, DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. The SETUP tab is active. On the left, a sidebar under 'Directory and Enrollment' lists 'Directory and Authentication', 'Basic Enrollment Settings', 'Advanced Enrollment Settings', and 'Enrollment Programs'. The 'Enrollment Programs' item is selected and highlighted with a blue border. The main content area is divided into two sections: 'iOS' and 'Android'. The 'iOS' section contains 'Apple Configurator' and 'Apple Device Enrollment Program', each with a 'Configure' button. The 'Android' section contains 'Android Enterprise QR Code Provisioning' and 'Android Enterprise Zero Touch Enrollment/KME enrollment', also each with a 'Configure' button.

### 3. If we have added an android device. Then configuration of it is as follow:

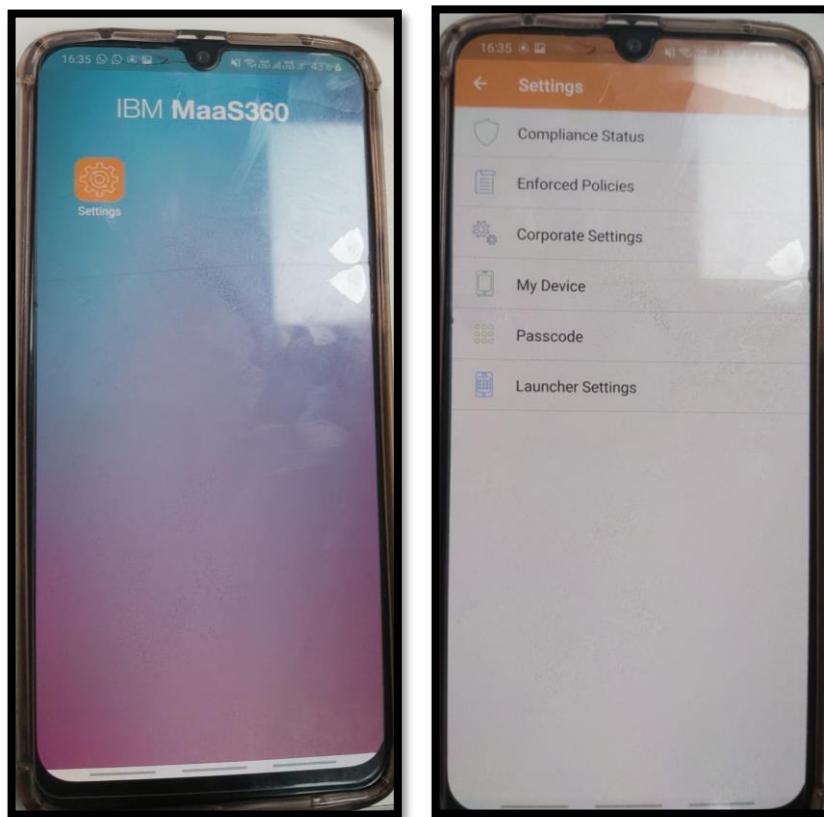
- After adding device user will get a passcode and URL to download IBM Maas360 in user email which they provide while creating user:



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

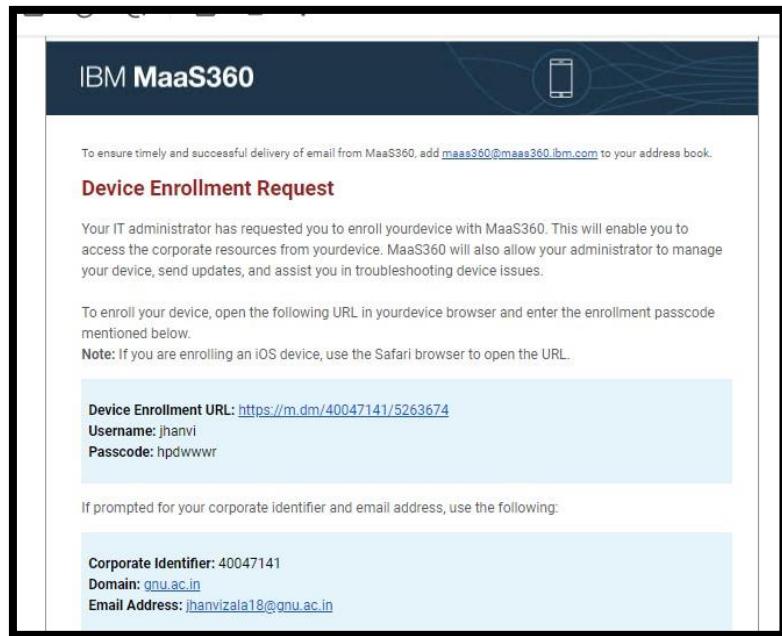


- After installing it we get application of settings and in that we are having compliance status, already enforced policy, corporate settings, my device information, passcode, launcher settings:

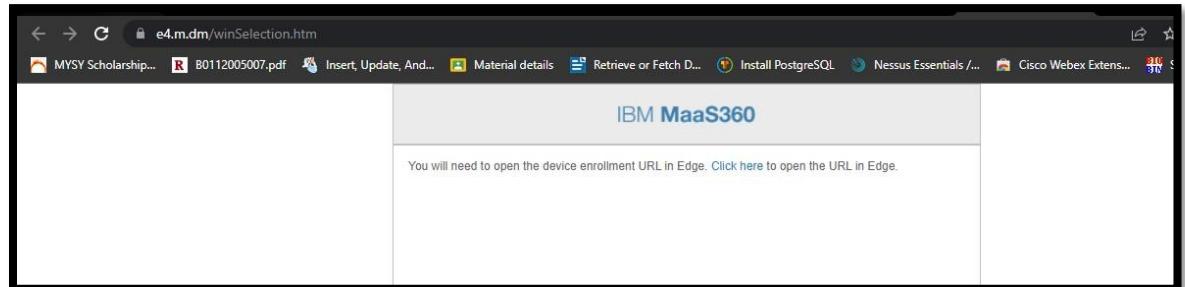


If we have to add device in windows devices. Then configuration is as follow

- 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:



#### 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.

The screenshot shows a modal dialog titled "Add User Directory Group". It has a text input field labeled "Enter Distinguished Name of User Group" with a placeholder "Enter a few characters of the Group Name" and a search icon. Below this is a section titled "User group to be available for" with four checkboxes:

- Security (Policies, Compliance Rules, Locations and Privacy Settings)
- App distribution
- Doc distribution
- Administrative access control

At the bottom right are "Cancel" and "Save" buttons.

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

The screenshot shows the IBM MaaS360 interface with the 'USERS' tab selected. The main area displays a table of 'Groups'. The columns include Name, Type, Policies, Rule Sets, Apps, Docs, Updated by, Updated, Last Evaluat..., and Administrativ... . There are 10 entries in the table:

Name	Type	Policies	Rule Sets	Apps	Docs	Updated by	Updated	Last Evaluat...	Administrativ...
Sales	①	②				jhanvizala18@gnu.a.c.in	03/10/2022 18:28 IST		Inactive
Management	①	②				jhanvizala18@gnu.a.c.in	03/10/2022 15:46 IST		Disabled
Manager	①	②				jhanvizala18@gnu.a.c.in	03/10/2022 15:43 IST		Inactive
SOC Analyst INTERNs	①	②		□ SOC		jhanvizala18@gnu.a.c.in	03/10/2022 15:35 IST		Inactive
VAPT Analyst INTERNs	①	②	Default iOS MD... Default macOS ... more...		□ VAPT	jhanvizala18@gnu.a.c.in	03/10/2022 15:33 IST		Active
VAPT	①	②			□ VAPT	jhanvizala18@gnu.a.c.in	03/04/2022 15:54 IST	03/10/2022 07:31 IST	
All Devices	①	②			✉ b_qradar_users...	jhanvizala18@gnu.a.c.in	03/01/2022 23:22 IST	03/10/2022 07:31 IST	
Unreachable iOS MDM Devices	①	②				System Administrator	06/09/2018 16:25 IST		
Windows Devices	①	②				System	04/16/2011 06:39		

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

This is a modal dialog box titled 'Enter User Group Description'. It contains a text input field labeled 'Description' with the placeholder 'Enter User Group Description'. Below the input field is a section titled 'User group to be available for' with four checkboxes:

- Security (Policies, Compliance Rules, Locations and Privacy Settings)
- App distribution
- Doc distribution
- Administrative access control

At the bottom right of the dialog are two buttons: 'Cancel' and 'Save'.

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

**Passcode Settings**

Configure Device Passcode Policy  Select this option to enforce the use of a Passcode before using Android for Work. Android 5.0+ (PO & DO)

Minimum Passcode Complexity Android 12.0+ (PO & DO)

Requires Android App 7.50+ for PO. Requires Android App 7.70+ for DO. Takes precedence over "Minimum Passcode Quality" and "Minimum Passcode Length" if both are configured. Unset this field to continue using deprecated settings : "Minimum Passcode Quality" and "Minimum Passcode Length".

Minimum Passcode Quality Android 5.0+ (PO & DO)

Requires Android 5.0+ and Android App 6.05+ for restricting passcode quality to Numeric Complex. Requires Android App 6.30+ for Weak Biometric, else defaults to Numeric. Android 12 onwards, this setting is deprecated and "Minimum Passcode Complexity" takes precedence over it.

Minimum Passcode Length (4-16 characters) Android 5.0+ (PO & DO)

Android 12 onwards, this setting is deprecated and "Minimum Passcode Complexity" takes precedence over it.

Delay for Passcode prompt after lock screen DO With KNOX (SAFE 2.0+)

Passcode History Android 5.0+ (PO & DO)

Maximum Passcode Age (in Days) Android 5.0+ (PO & DO)

Allowed Idle Time (in minutes) Before Auto-Lock Android 5.0+ (PO & DO)

Allowed Idle Time (in hours) for Stronger Authentication Android 8.0+ (PO & DO)

When enabled, mandates the user on the device to use a stronger authentication (PIN, Password, Pattern) after the allowed idle time.

Number of Failed Passcode Attempts Before All Data is Erased (0-16) Activate Windows Android 5.0+ (PO & DO)

Possible values are 0 to 16. Add 0 to disable data wipe on failed attempts.

15 Go to Settings to activate Windows

## 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

▼ Device Security

Configure Keyguard features

**Note:** By default, all keyguard (lock screen) features are allowed on the device. Configuring this policy automatically enables lock screen and swipe even if it was explicitly disabled by the user.

Allow Remote Input	<input type="checkbox"/>	Android 5.0+ (DO)	Android 9.0+ (PO)
Allow fingerprint	<input checked="" type="checkbox"/>	Android 5.0+ (DO)	Android 9.0+ (PO)
Allow fingerprint on personal profile	<input checked="" type="checkbox"/>	Android 11+ (WPCO)	
Allow secure camera	<input type="checkbox"/>	Android 5.0+ (DO)	Android 11+ (WPCO)

Activate Windows

Allow secure notifications	<input checked="" type="checkbox"/>	Android 5.0+ (DO)	Android 11+ (WPCO)
Allow Unredacted Notifications	<input checked="" type="checkbox"/>	Android 5.0+ (DO)	Android 9.0+ (PO)
Allow IRIS Recognition	<input type="checkbox"/>	Android 9.0+ (PO & DO)	
Allow IRIS Recognition on personal profile	<input checked="" type="checkbox"/>	Android 11+ (WPCO)	
Allow Face Recognition	<input checked="" type="checkbox"/>	Android 9.0+ (PO & DO)	
Allow face recognition on personal profile	<input checked="" type="checkbox"/>	Android 11+ (WPCO)	
Allow Trust agents	<input checked="" type="checkbox"/>	Android 5.0+ (DO)	Android 9.0+ (PO)

Activate Windows

Allow trust agents on personal profile	<input checked="" type="checkbox"/>	Android 11+ (WPCO)
Allow boot of device in Safe mode	<input type="checkbox"/>	Android 6.0+ (DO)
Allow Factory reset	<input checked="" type="checkbox"/>	Android 5.0+ (DO)
Allow configuration of credentials	<input checked="" type="checkbox"/>	Android 5.0+ (DO)
Allow User profile creation	<input checked="" type="checkbox"/>	Android 5.0+ (DO)
Allow removal of user profile	<input type="checkbox"/>	Android 5.0+ (DO)
Allow modification of accounts	<input checked="" type="checkbox"/>	Android 5.0+ (PO & DO)

Activate Windows

Enable Enterprise Security Logging	<input checked="" type="checkbox"/>	Android 7.0+ (DO)
Allow lock down of wallpaper	<input type="checkbox"/>	Android 7.0+ (DO)
Enabled this to lock down wallpaper on the device		
Allow lock down of customer user icon	<input type="checkbox"/>	Android 7.0+ (DO)
Enabled this to lock down customer user icon on the device		
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.		
<input type="text"/>		<input style="border: none; background-color: #f0f0f0; padding: 2px 5px; border-radius: 5px;" type="button" value="+"/>

Enable Device Attestation	<input checked="" type="checkbox"/>	
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	<input checked="" type="checkbox"/>	Android 5.0+ (DO)
Allow Settings Changes	<input checked="" type="checkbox"/>	DO With KNOX (SAFE 2.0+)
Allow users to make changes to Settings application		
Enable Power Saving Mode	<input checked="" type="checkbox"/>	DO With KNOX (SAFE 5.8+)
Enable to allow power saving mode on the device		
Enable Samsung Device Attestation	<input type="checkbox"/>	DO With KNOX 1.0.1+
Enabling this setting will trigger attestation check on the device every 24 hours as provided by Samsung. Not supported on Knox 3.0(24)+		
Restrict Jailbroken/Rooted Devices	<input checked="" type="checkbox"/>	Android 5.0+ (DO)
Prevent users from accessing secure content if their device is jailbroken or rooted. Note: Android App 5.85 is required		

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  
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  
Set default runtime permissions for apps      Android 6.0+ (PO & DO)

[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      Android 5.0+ (PO & DO)

Allow Accessibility Services Restriction Level      Android 5.0+ (PO & DO)

[Activate Windows](#)  
Go to Settings to activate Windows

Allow Clipboard  DO With KNOX (SAFE 2.0+)

Allow Clipboard Sharing between Apps  DO With KNOX (SAFE 4.0+)

Disabling this setting disables the global clipboard between applications.  
In this case, each App will have its own individual clipboard.

Allow Share List  DO With KNOX (SAFE 4.0+)

Disabling this setting disables the display of the Share Via List that is available to share data with other applications.

**▼ Work Profile-specific Settings**

Allow Clipboard Sharing  Within Work Profile Android 5.0+ (PO)

Enable Work Profile Intent Filters from Personal Profile  Android 5.0+ (PO)

Enable Personal Profile Intent Filters from Work Profile  Activate Windows Android 5.0+ (PO)

Allow work events on personal calendar  Do not allow Android 10.0+ (PO)

Enable users to view work events on personal calendar app (Requires MaaS360 app 7.30+)

Set maximum number of days a work profile can remain off  0 Android 11+ (WPCO)

Personal apps are suspended on the device if the profile is turned off for longer. Minimum possible value is 3 days. Enter 0 if no limit.

Allow cross-profile apps  + Android 11.0+ (PO)

Allowed apps will request user consent for cross-profile communication.

**▼ Advanced Settings**

Configure Global Settings

[Click here](#) for the list of supported settings.

Supported only on Android 5.0+ (DO) Android 5.0+ (DO)

### 3. Configuring App compliance

- Configure Required Apps:
  - Maas360 Chat
  - Maas360 Remote Support

**▼ Configure Application Compliance**

Configure allowed system applications  Android 5.0+ (PO & DO)

Allowed apps will be available for use on device and in work profile if available for the device

Configure Required Apps  Android 5.0+ (PO & DO)

Apps that cannot be uninstalled by user.

**Application Name** com.fiberlink.maas360.android.secure  + - Android 5.0+ (PO & DO)

Application Name com.fiberlink.maas360.android.remote  + - Android 5.0+ (PO & DO)

Configure Disabled Apps

Activate Windows Go to Settings to activate Windows.

Cookie Preferences

**MaaS360 Chat App Summary:**

Available for	All	App ID	com.fiberlink.maas360.android.securechat
Type	Google Play App	Category	Business
Supported On	Smartphones	Distributions	All Devices
Installs	4 installed   7 distributed	App Bundles	No App Bundles
App Version (Full Version)	5.56 (5.56)	Update Date (Uploaded By)	03/08/2022 11:30 IST (jhanvizala18@gnu.ac.in)
Available Tracks	- Refresh		

**MaaS360 Remote Support App Summary:**

Available for	All	App ID	com.fiberlink.maas360.android.remoteControl
Type	Google Play App	Category	Business
Supported On	Smartphones	Distributions	All Devices
Installs	5 installed   7 distributed	App Bundles	No App Bundles
App Version (Full Version)	7.70 (7.70)	Update Date (Uploaded By)	03/08/2022 11:30 IST (jhanvizala18@gnu.ac.in)
Available Tracks	- Refresh		

#### 4. Brower Settings

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

**Browser Settings:**

- Allow Browser (Chrome):** Enabled (checked).
- Blocked URLs (Blocklist):**
  - <https://www.facebook.com/> (Android 5.0+ (PO & DO))
  - <https://www.instagram.com/> (Android 5.0+ (PO & DO))
- Allowed URLs (Allowlist):**
  - <https://en.wikipedia.org/> (Android 5.0+ (PO & DO))
- Managed Bookmarks:** Specified as "Allowlist works only if blocklist is configured".
- Cookie Preferences:** Available at the bottom right.

5. Save the policy and publish.

The screenshot shows the 'Default Android MDM Policy' configuration page. On the left, there's a sidebar with icons for Passcode, Security, Restrictions, Accounts, App Compliance (which is selected), ActiveSync, Wi-Fi, and VPN. The main area has two sections: 'Configure Application Compliance' and 'Configure allowed system applications'. Under 'Configure Application Compliance', there are two sections: 'Configure Required Apps' (set to Yes) and 'Application Name' (set to com.fiberlink.maas360.android.securechat). A note says 'Android 5.0+ (PO & DO)'. Below that is another 'Application Name' section (set to com.fiberlink.maas360.android.remoteControl) with a note 'Activate Windows'. In the top right corner, there's a dropdown menu with options: Edit, More, View Audit History, Show Variables, **Publish Policy** (which is highlighted in blue), and View Recent Changes.

The screenshot shows a 'Publish' dialog box. At the top, it says 'Region' and 'Asia'. Below that is a text input field with placeholder text: 'Enter a description to help with any future audits (Maximum of 255 characters)'. There are two checkboxes: 'Apply changes to more Policies' (unchecked) and 'Show me the differences before publishing' (checked). At the bottom right are 'Cancel' and 'Continue' buttons. The 'Continue' button is highlighted in blue.

## 6.2.2 Administrative settings:

The screenshot shows a software interface with a dark header bar containing navigation links: HOME, DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. The SETUP link is highlighted with a blue border. Below the header is a sidebar with the following menu items:

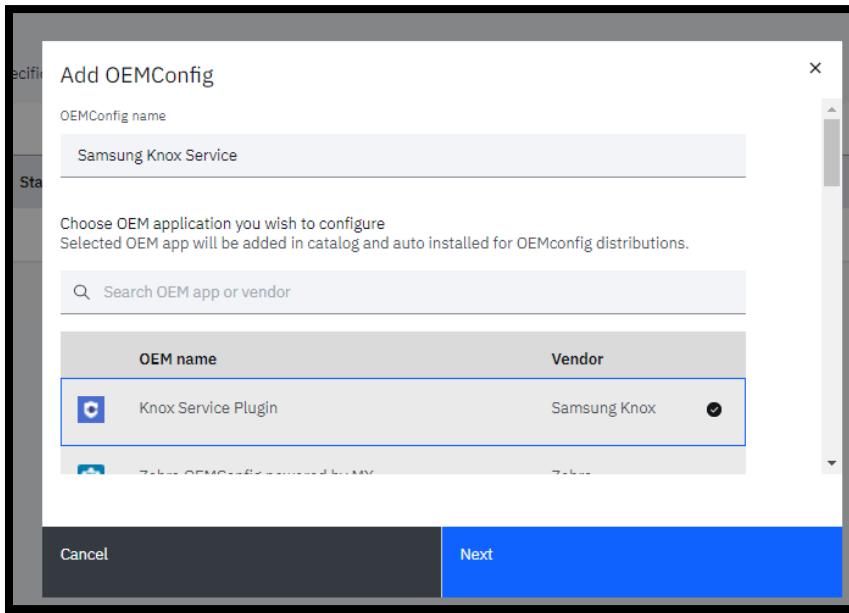
- Directory and Enrollment
- User Settings
- App Settings
- Doc Settings
- Administrator Settings
  - Basic (selected, indicated by a blue border)
  - Advanced
  - Analytics
  - License settings

On the right side of the screen, under the 'Administrator Settings' section, there is a 'Basic' configuration panel. To its right, under the 'Alerts' heading, are four alert configuration sections, each with a checkbox and a notification email address field:

- Alert administrator on new device discovery ⓘ  
Notification Email Address(es)  
drishtimotwani18@gnu.ac.in (+) Add
- Alert administrator on permanent user deletion ⓘ  
Notification Email Address(es) (disabled)
- Alert administrator when license is about to expire ⓘ  
Notification Email Address(es)  
drishtimotwani18@gnu.ac.in (+) Add
- Alert administrator on license expiry ⓘ  
Notification Email Address(es)  
drishtimotwani18@gnu.ac.in (+) Add
- Alert administrator on license removal ⓘ  
Notification Email Address(es)  
drishtimotwani18@gnu.ac.in (+) Add
- Alert administrator on discovery of new licenses ⓘ  
Notification Email Address(es)  
drishtimotwani18@gnu.ac.in (+) Add

### 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.

Profile name  
Add a unique profile name that highlights the policies and restrictions... Samsung Knox profile

KPE Premium or Knox Suite License key  
If your UEM console supports KPE license information, enter your KPE...

Debug Mode  
The informative mode shows policy results and errors on the device. We... No

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

Customize Dex Experience (Premium)  
Use this control to enable customization of your Dex mode.... No

VPN policy (Premium)  
A group of policies for VPN setup and configuration. IT admins can enforce these policies for fully managed devices with or without a Wor... Yes

Enable VPN controls  
Use this control to enable or disable VPN controls for the device....

VPN type  
Choose the VPN type applicable to the apps on the device. For full... Work profile/Separated Apps only

Manage list of apps that use VPN  
Use these controls to add a list of applications at a device-wide or Work profile/Separated Apps specific level that can use VPN and...

Select apps in the device, in the main user  
For fully managed devices with app-specific VPN, enter a... Select apps in the device, in the main user

Select apps in the Work profile/Seorated Apps  
Select apps in the Work profile/Seorated Apps

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

The screenshot shows the 'Distributions' tab of the Samsung Knox Services configuration page. It includes fields for setting a default configuration, assigning groups (with a search bar for 'Search group' containing 'Samsung Devices'), and selecting specific devices. On the right, 'Deployment details' show 0 devices in scope and an app config precedence of 1. Buttons at the bottom include 'Cancel', 'Back to configure', and a prominent blue 'Publish' button.

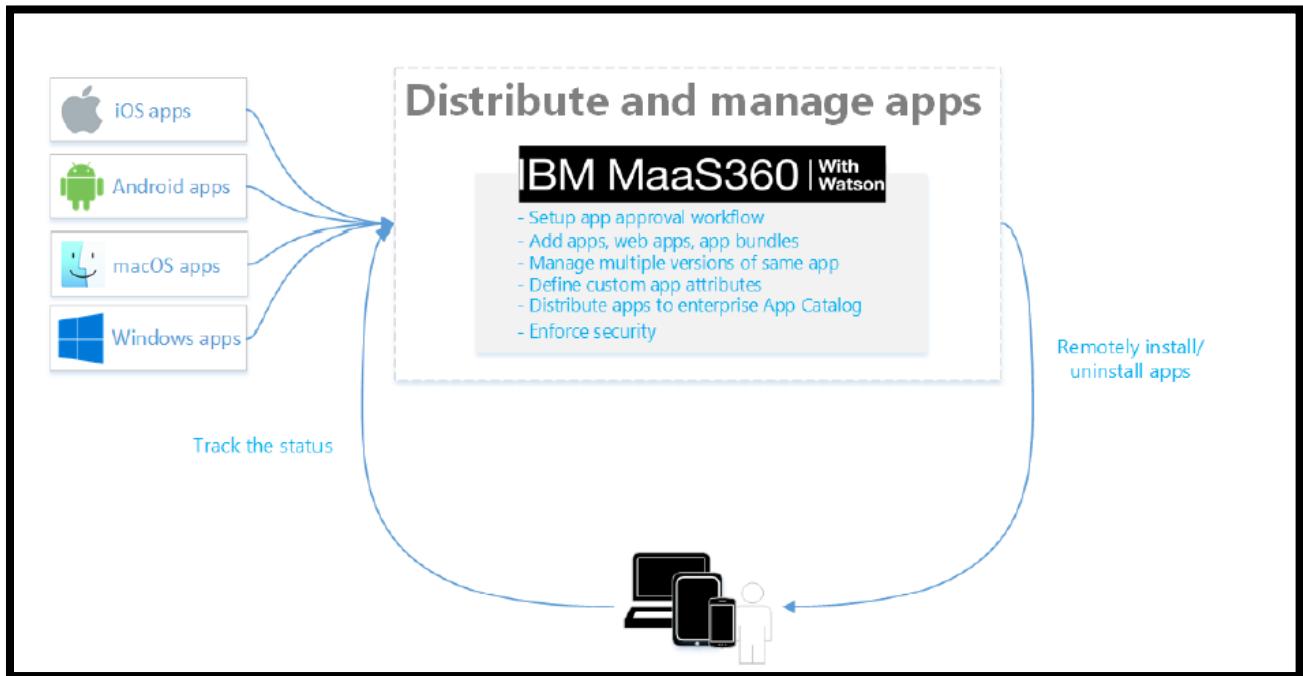
The screenshot shows the 'Groups' management page. It lists several device groups: 'Samsung Devices', 'All Devices', 'SOC', 'VAPT', 'Unreachable iOS MDM Devices', and 'Test Devices'. Each group entry includes a preview icon, type, policies, rule sets, apps, docs, updated by, updated date, and last evaluate date. A toolbar at the top provides options for Show Private Groups, Bulk Delete User Groups, Bulk Import Groups, and Add.

5. Publish the service.

The screenshot shows the 'Android OEMConfig' page. It displays a table of configurations, with one entry for 'Samsung Knox Services' which is published and applied to the 'Samsung Devices' group with a precedence of 1. The table includes columns for Name, Default, Status, OEM app name, Applied to groups, Precedence, and Last update date. A blue 'Add configuration' button is located at the top right. Navigation controls for items per page and pages are at the bottom.

## 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.

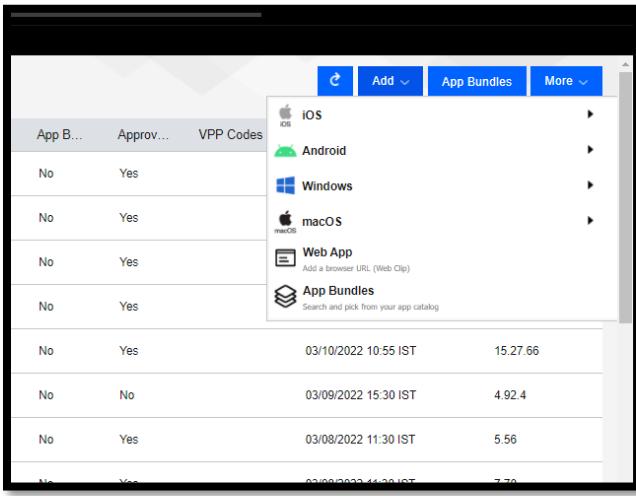


1. From the MaaS360 Portal Home page, select Apps > Catalog.

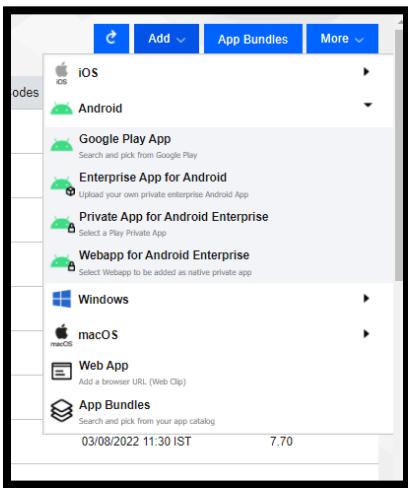
Screenshot of the IBM MaaS360 App Catalog interface. The top navigation bar includes links for HOME, DEVICES, USERS, SECURITY, APPS (which is currently selected), DOCS, REPORTS, and SETUP. A search bar is located at the top right. The main area is titled "App Catalog" and displays a table of installed applications. The columns in the table are: App ..., Name, Type, Categories, Installs and P..., Distrib..., App B..., Approv..., VPP Codes, Last Updated, and App Version. The table lists several apps, including TeamViewer Universal Add-On, TeamViewer QuickSupport, TeamViewer Host, TeamViewer Remote Control, IBM MaaS360, MaaS360 Chat, MaaS360 Remote Support, and MaaS360 Browser. Each row includes a "View" link and "Distribute" and "Delete" buttons.

App ...	Name	Type	Categories	Installs and P...	Distrib...	App B...	Approv...	VPP Codes	Last Updated	App Version
<input type="checkbox"/>	TeamViewer Universal Add-On		Productivity	less than 10		Yes	No	Yes	03/10/2022 12:40 IST	15.8.5
<input type="checkbox"/>	TeamViewer QuickSupport		Productivity	less than 10		Yes	No	Yes	03/10/2022 12:10 IST	15.27.67
<input type="checkbox"/>	TeamViewer Host		Productivity	less than 10		Yes	No	Yes	03/10/2022 11:10 IST	15.27.67
<input type="checkbox"/>	TeamViewer Remote Control		Productivity	less than 10		No	No	Yes	03/10/2022 11:00 IST	15.27.66
<input type="checkbox"/>	TeamViewer Remote Control		Productivity	less than 10		Yes	No	Yes	03/10/2022 10:55 IST	15.27.66
<input type="checkbox"/>	IBM MaaS360		Business	less than 10		Yes	No	No	03/09/2022 15:30 IST	4.92.4
<input type="checkbox"/>	MaaS360 Chat		Business	less than 10		Yes	No	Yes	03/08/2022 11:30 IST	5.56
<input type="checkbox"/>	MaaS360 Remote Support		Business	less than 10		Yes	No	Yes	03/08/2022 11:30 IST	7.70
<input type="checkbox"/>	MaaS360 Browser		Business	less than 10		Yes	No	Yes	03/08/2022 11:20 IST	7.70

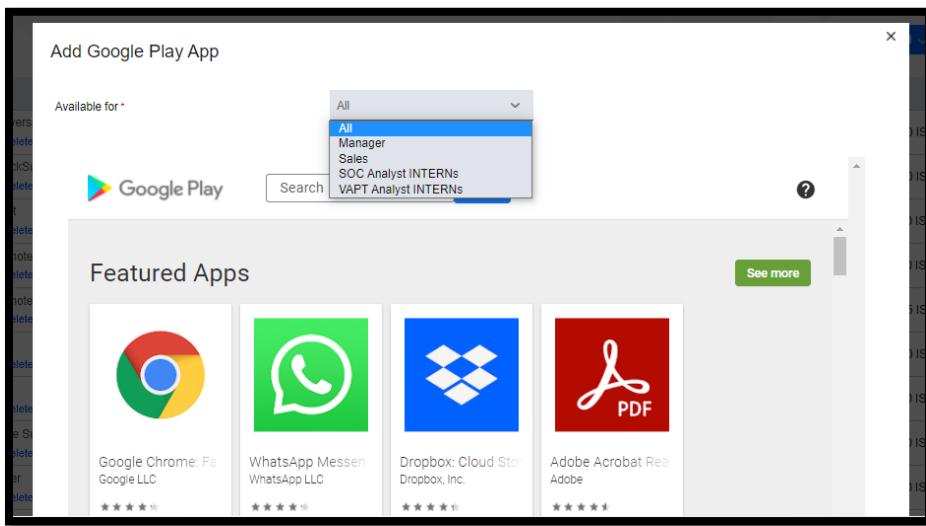
2. To add application click on add. There we are having different section iOS, android, Windows, macOS, web application, app bundles:



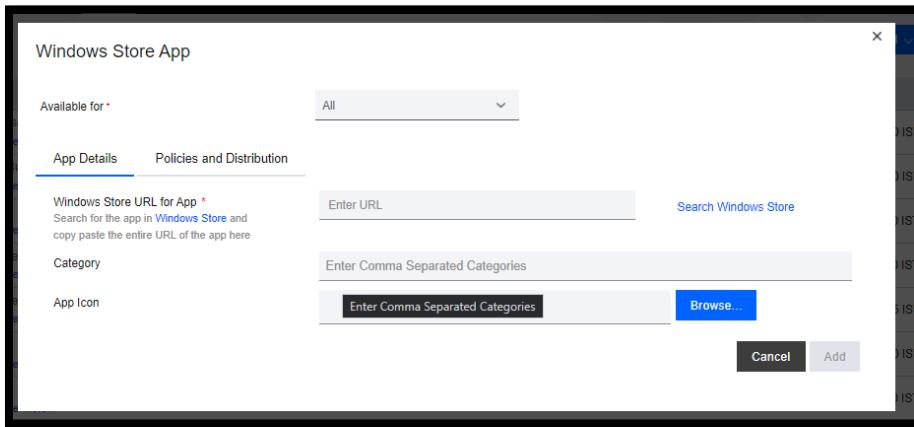
3. Now here, we have added application for android devices. So expand android section. In that add we have options to add application through google app, enterprise application for android, private app for android application, webapp for android enterprise.



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:



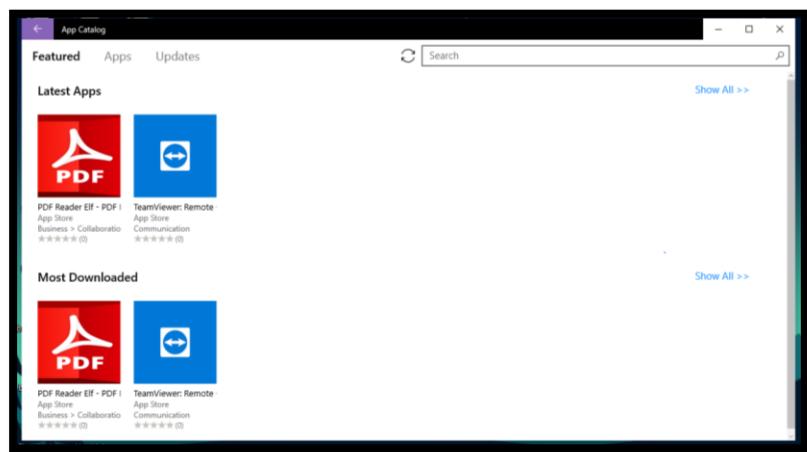
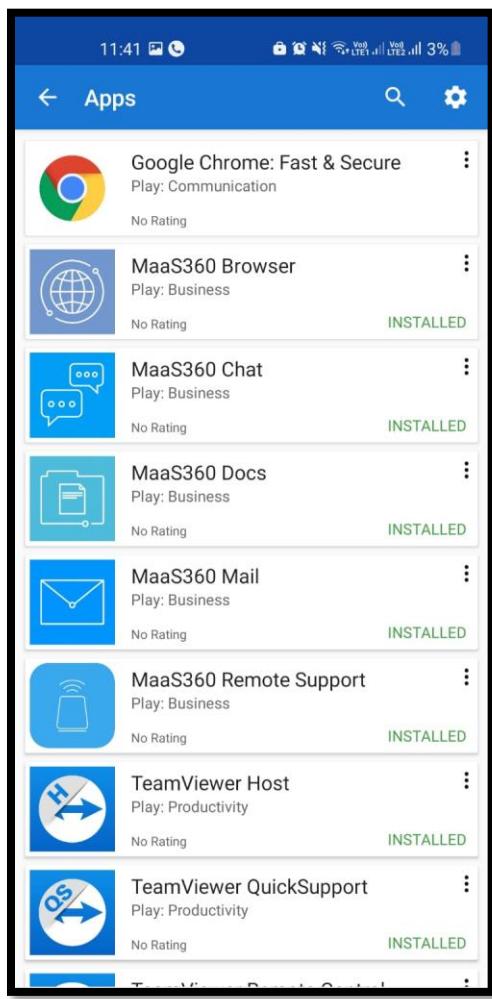
To distribute application which is added through above process.

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

The screenshot shows the IBM MaaS360 interface with the 'APPS' tab selected. Under the 'Mail and Calendar' application, the 'App Summary' section is displayed. It includes details such as Type (Windows Store App), Category (Communication), Supported On (Smartphones), Distributions (No Distributions), Installs (0 installed | 0 distributed), App Version (Full Version) (NA), Update Date (03/01/2022 23:27 IST), Minimum OS Version (NA), and Supported Architecture (Not Available). Below this, there is a 'Details' section with a 'Refresh App Details' button and a 'Description' section that states: 'The Mail and Calendar apps help you stay up to date on your email, manage your schedule and stay in touch with people you care about the most. Designed for both iOS and Android, these apps help you respond faster, smarter, and easier to hectic workday demands.'

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

The screenshot shows a modal dialog titled 'Distribute App: Mail and Calendar'. It has two main sections: 'Available for \*' (set to 'All') and 'Target\*' (set to 'Specific Device'). There is a search bar and a '+' button next to the target dropdown. Below these, there is a checkbox labeled 'Send Email'. At the bottom right are 'Cancel' and 'Distribute' buttons.



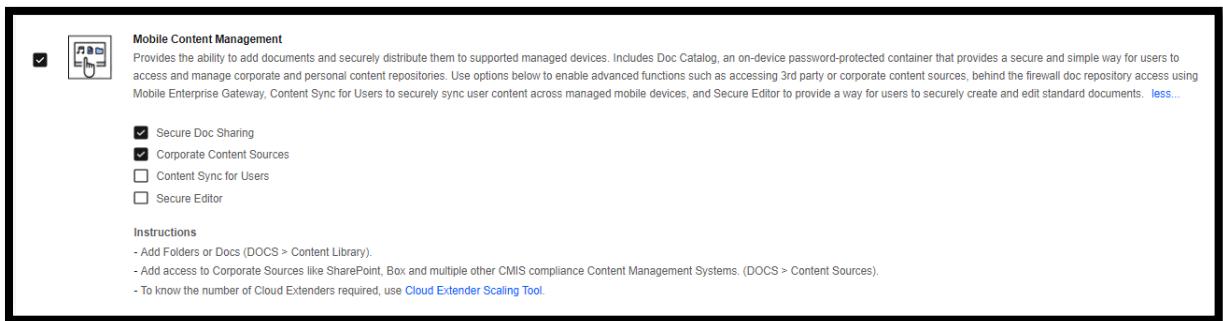
## 6.4 Mobile Content Management:

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:

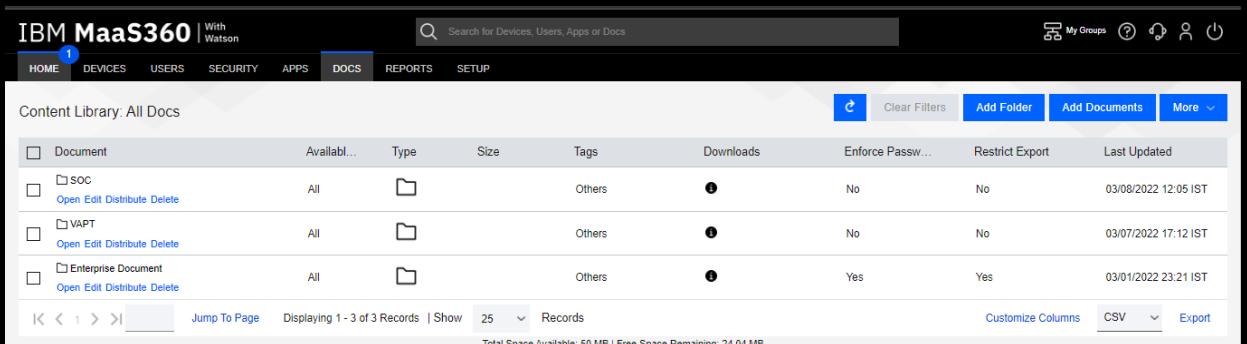
- Enterprise document catalogue to allow users to access and read documents on mobile devices in a secure manner.
- Document lifecycle management to help streamline and standardise workflows.
- Document and file protection and data leakage prevention through compliance and enforcement.



#### 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.

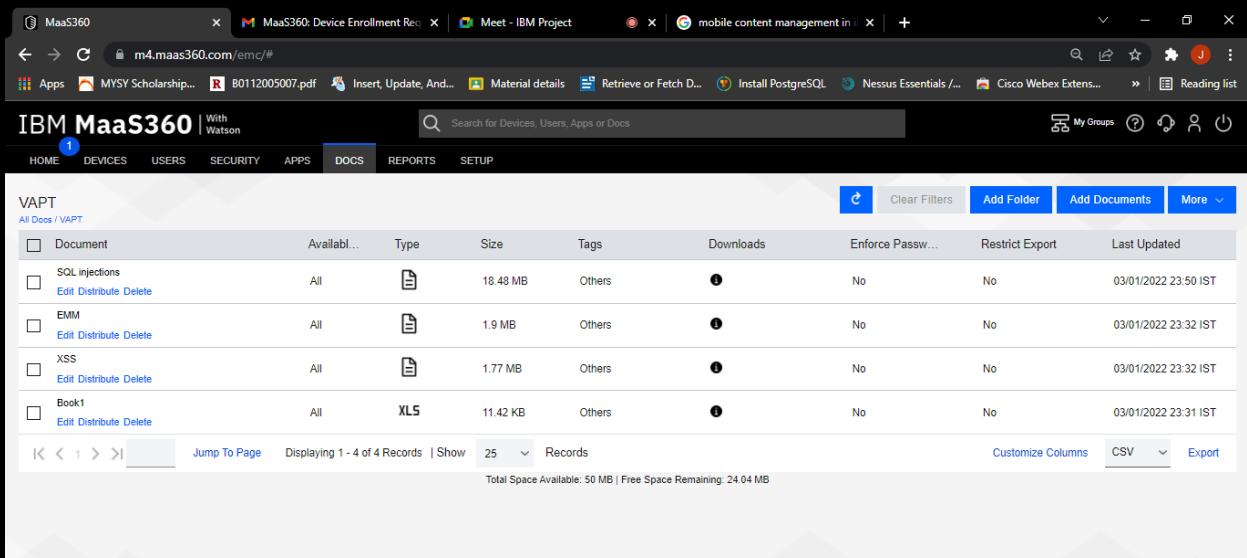


The screenshot shows the MaaS360 Content Library interface. At the top, there's a navigation bar with links for HOME, DEVICES, USERS, SECURITY, APPS, DOCS (which is highlighted in blue), REPORTS, and SETUP. A search bar is located at the top right. Below the navigation bar, the title "Content Library: All Docs" is displayed. The main area contains a table with the following columns: Document, Available..., Type, Size, Tags, Downloads, Enforce Passw..., Restrict Export, and Last Updated. There are three entries in the table:

Document	Available...	Type	Size	Tags	Downloads	Enforce Passw...	Restrict Export	Last Updated
SOC	All	Folder		Others	1	No	No	03/08/2022 12:05 IST
VAPT	All	Folder		Others	1	No	No	03/07/2022 17:12 IST
Enterprise Document	All	Folder		Others	1	Yes	Yes	03/01/2022 23:21 IST

At the bottom of the table, there are buttons for "Jump To Page", "Displaying 1 - 3 of 3 Records", "Show 25", and "Records". On the far right, there are links for "Customize Columns", "CSV", and "Export".

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.



The screenshot shows the MaaS360 Content Library interface, similar to the previous one but with a different breadcrumb trail at the top: "All Docs / VAPT". The rest of the interface is identical, showing a table of documents within the VAPT folder. The table has the same columns and data as the first screenshot.

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.

The screenshot shows the IBM MaaS360 interface with the 'DOCS' tab selected. The main area displays a table titled 'Content Library: All Docs' with the following data:

Document	Available...	Type	Size	Tags	Downloads	Enforce Passw...	Restrict Export	Last Updated
SOC	All	Folder		Others	1	No	No	03/08/2022 12:05 IST
VAPT	All	Folder		Others	1	No	No	03/07/2022 17:12 IST
Enterprise Document	All	Folder		Others	1	Yes	Yes	03/01/2022 23:21 IST

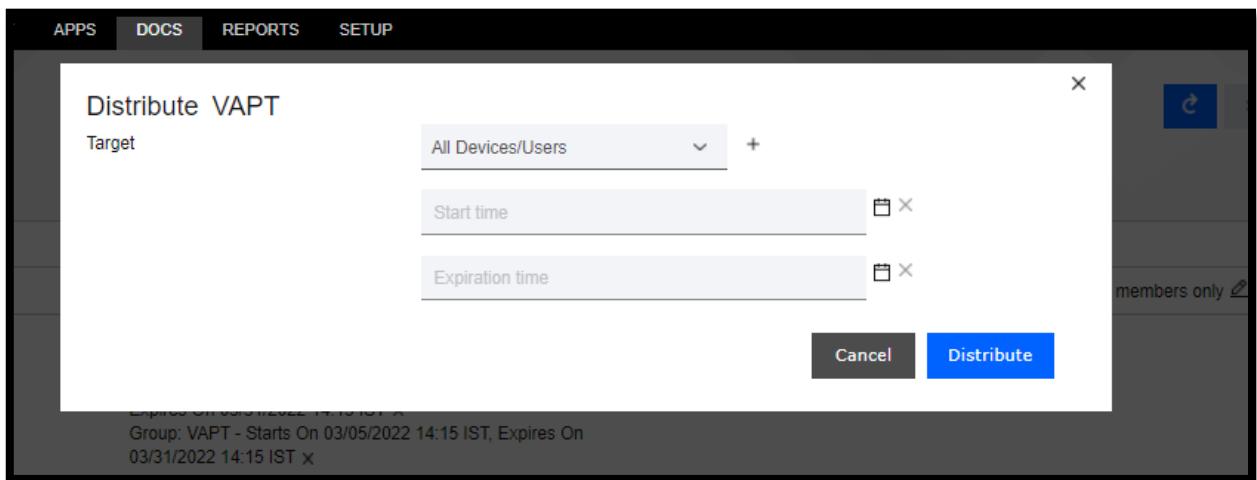
Below the table, there are navigation buttons (Jump To Page, Show 25 Records), a total space available message (Total Space Available: 50 MB | Free Space Remaining: 24.04 MB), and links for 'Customize Columns', 'CSV', and 'Export'.

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

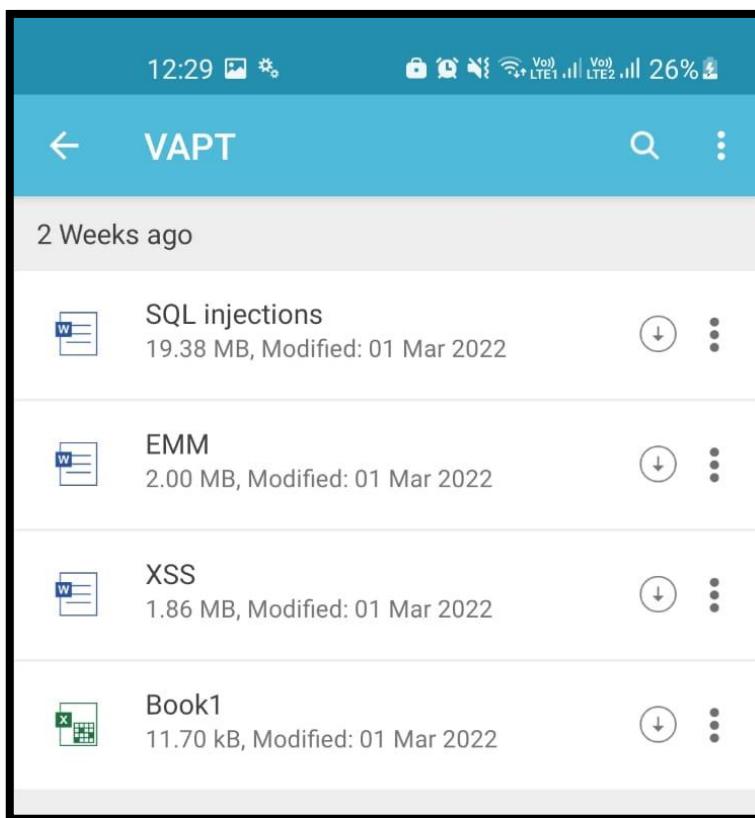
The screenshot shows the 'Edit' screen for the 'VAPT' folder. The top navigation bar shows 'DOCS' is selected. The main content area includes:

- Folder Summary:** Shows the folder name 'VAPT', download count (2), tags ('Others'), and a description ('for vapt members only'). It also lists distributions for users and groups.
- Security Settings:** Includes checkboxes for 'Restrict Export' (unchecked) and 'Ignore WorkPlace Restrictions' (unchecked). It also includes options for 'Restrict Cut/Copy/Paste' (checked).
- Download Policies:** A section for defining security settings for the current folder and all sub-folders/documents.

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

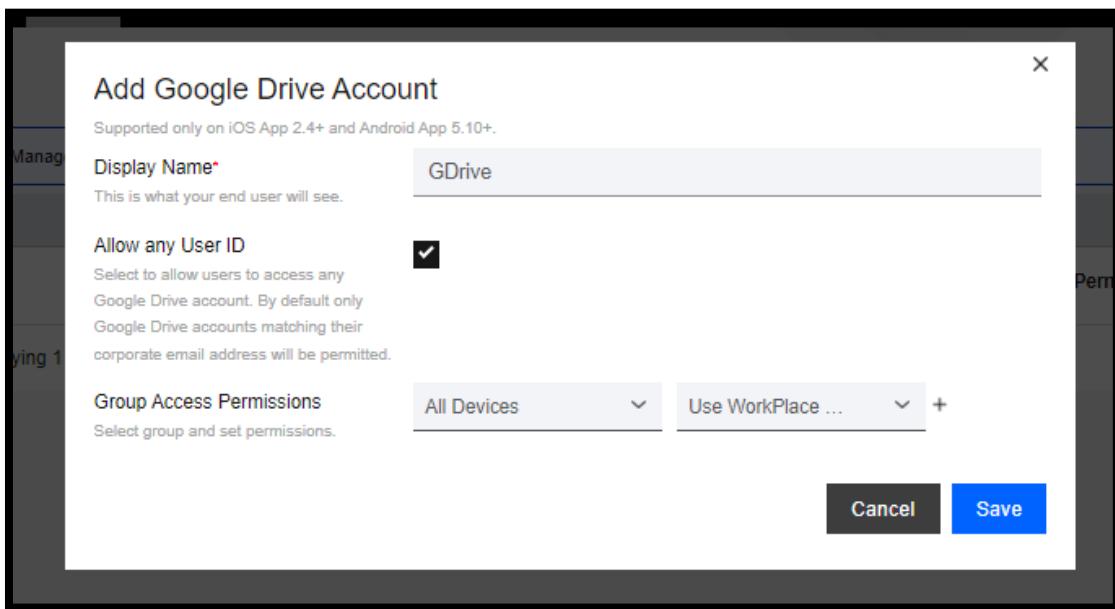


- Now after distribution in the document section in android device we are able to add that and screen will be like this:



#### 6.4.3 GDrive Content Source:

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

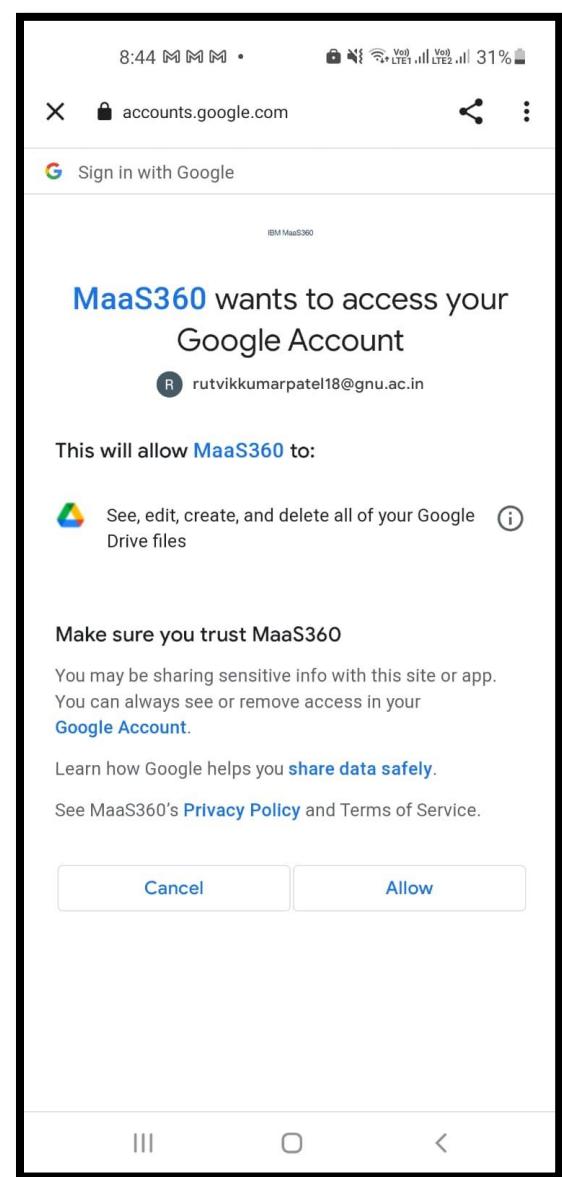
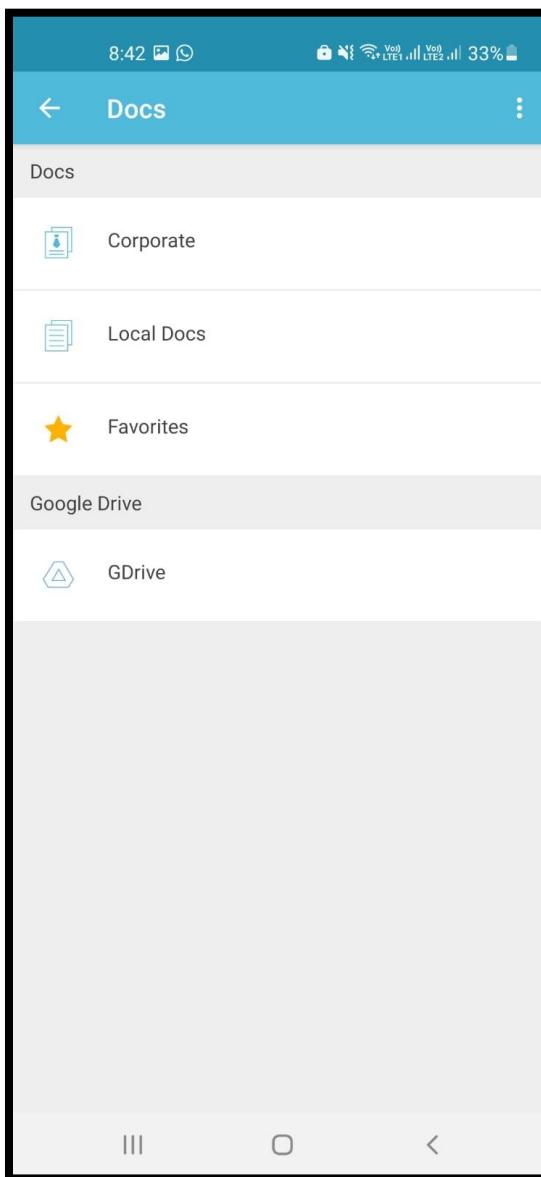


2. Assign name to the source and configure groups access permissions according to the requirements.

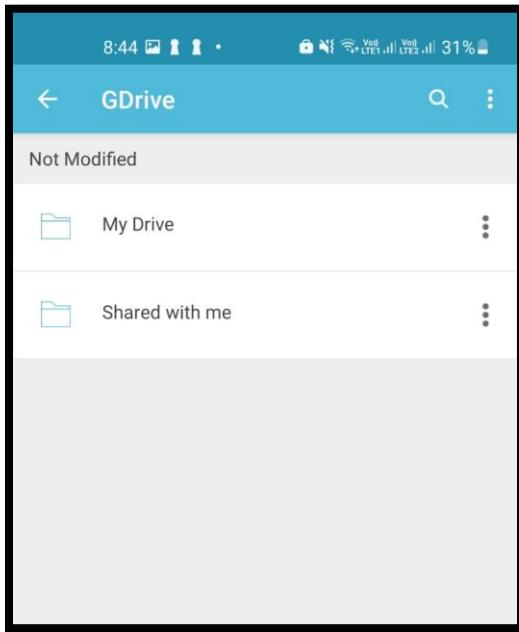
The screenshot shows the "Manage Content Sources" page in the IBM MaaS360 interface. It lists a single source named "GDrive" with Type "Google Drive", Library/Folder "N/A", and Gateway Name "N/A". The Group Access Permissions are set to "All Devices" and "Permissions: Use WorkPlace S...".

Share Name	Type	Library/Folder	Gateway Name	Group Access Permissions
GDrive <a href="#">Edit</a> <a href="#">Delete</a>	Google Drive	N/A	N/A	Group Name: All Devices Permissions: Use WorkPlace S...

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



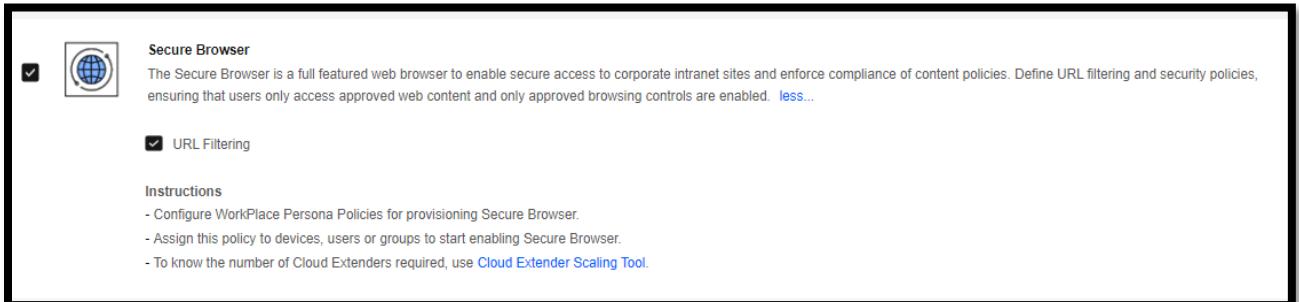
5. Now, we can access our google drive here.



## 6.5 Secure browser:

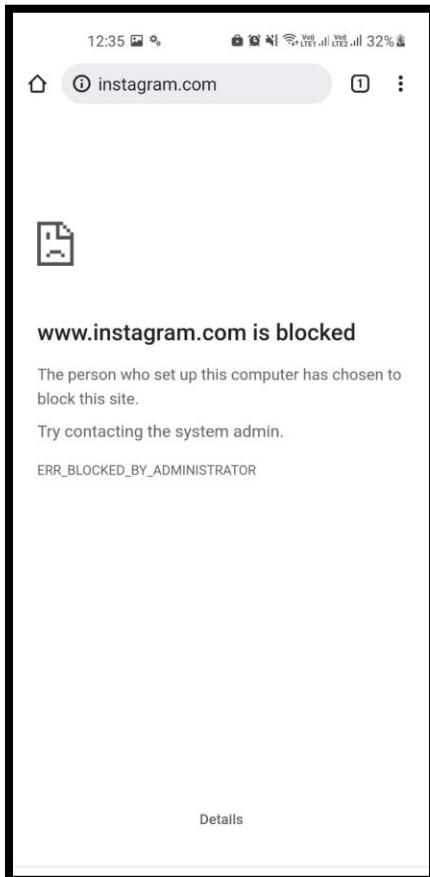
The IBM® MaaS360® Secure Mobile Browser will provide secure access to intranet sites , corporate web apps, and public websites.

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.

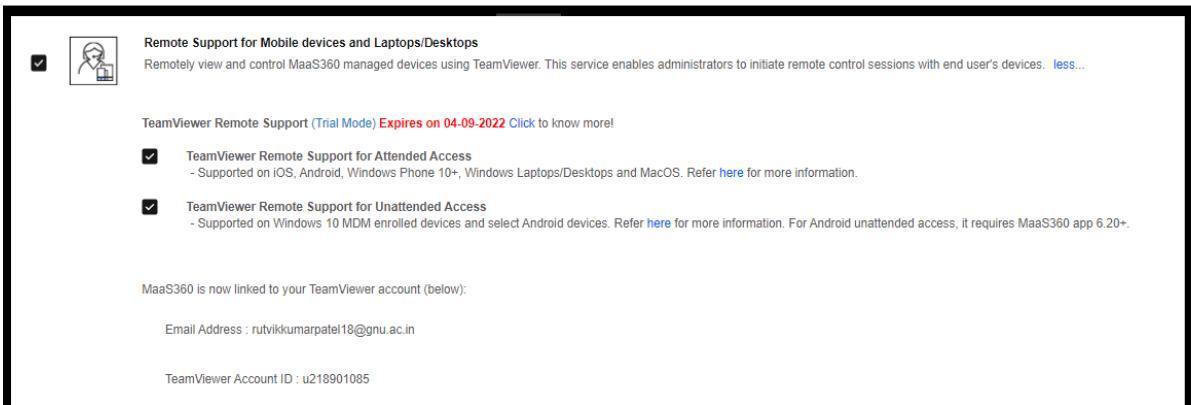


## 6.6 Remote support for mobile devices and laptop/desktops:

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.



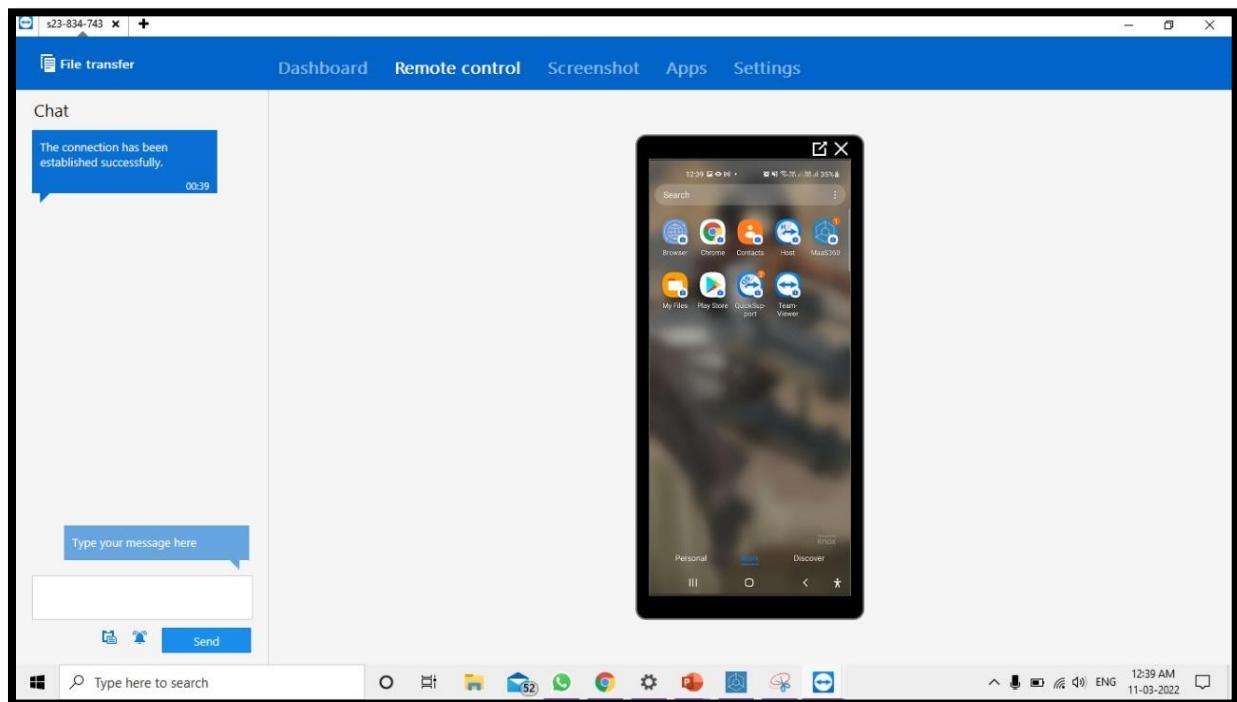
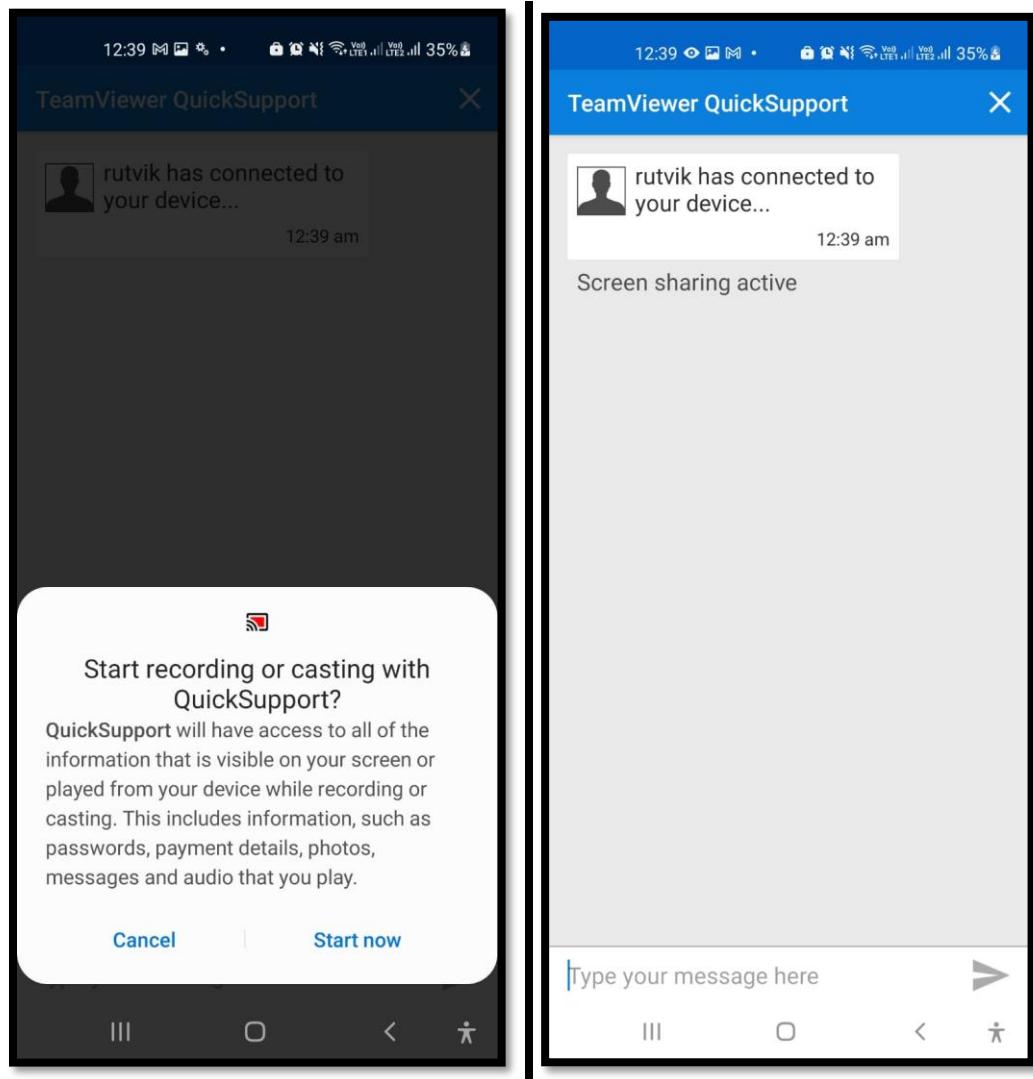
1. After deploying this. In mobile devices we will have team viewer application and messages application. Now while deploying it we will have this steps:

The screenshot shows the 'Device Inventory' section of the IBM MaaS360 interface. It lists several devices with their names, platforms, and various management actions available for each.

Device Name	Username	Platform
rutvik-SM-M405F	rutvik	iPad
dhwani-vivo 1804		Buzz
DESKTOP-TJ		Distribute App
PATEL		Distribute Doc
tanvi-SM-J810G		Change Policy
drishti-POCO F1		Change Rule Set
jhanviz-SM-M305F	jhanviz	Hide

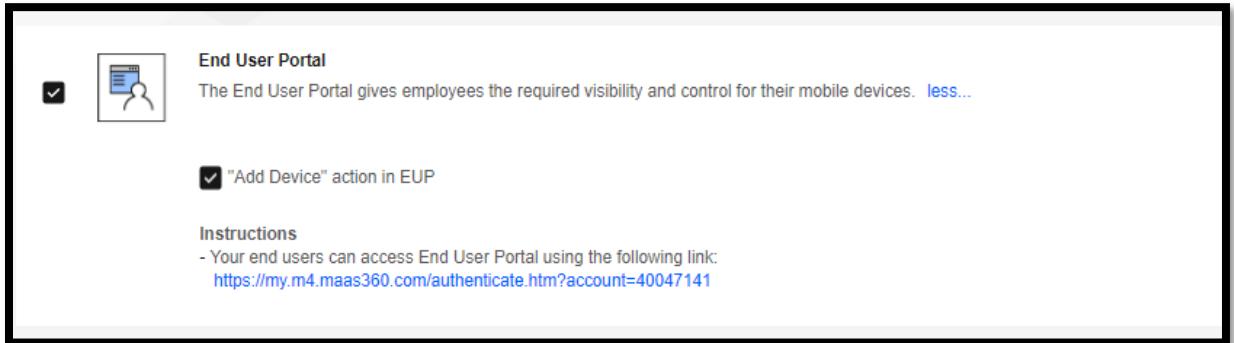
Actions listed for the first device (rutvik-SM-M405F):

- View Message
- Lock
- More...
- Buzz
- Distribute App
- Distribute Doc
- Change Policy
- Change Rule Set
- Hide
- Initiate Remote Support
- Change License Entitlements



## 6.7 Configure End user portal:

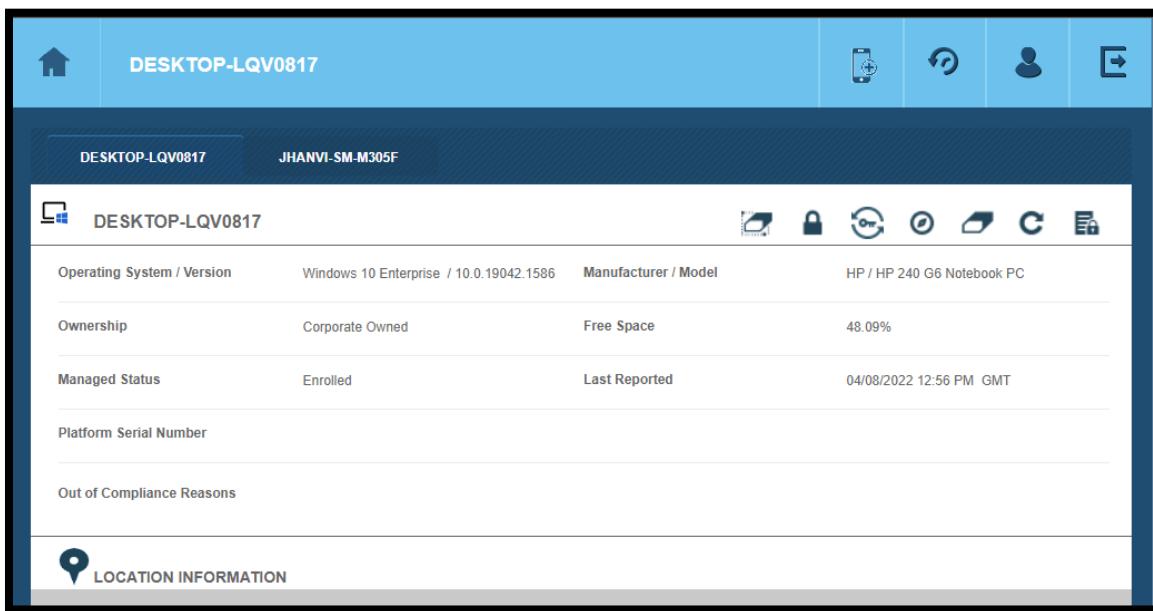
1. Go to setup->services. Enable end user portal:



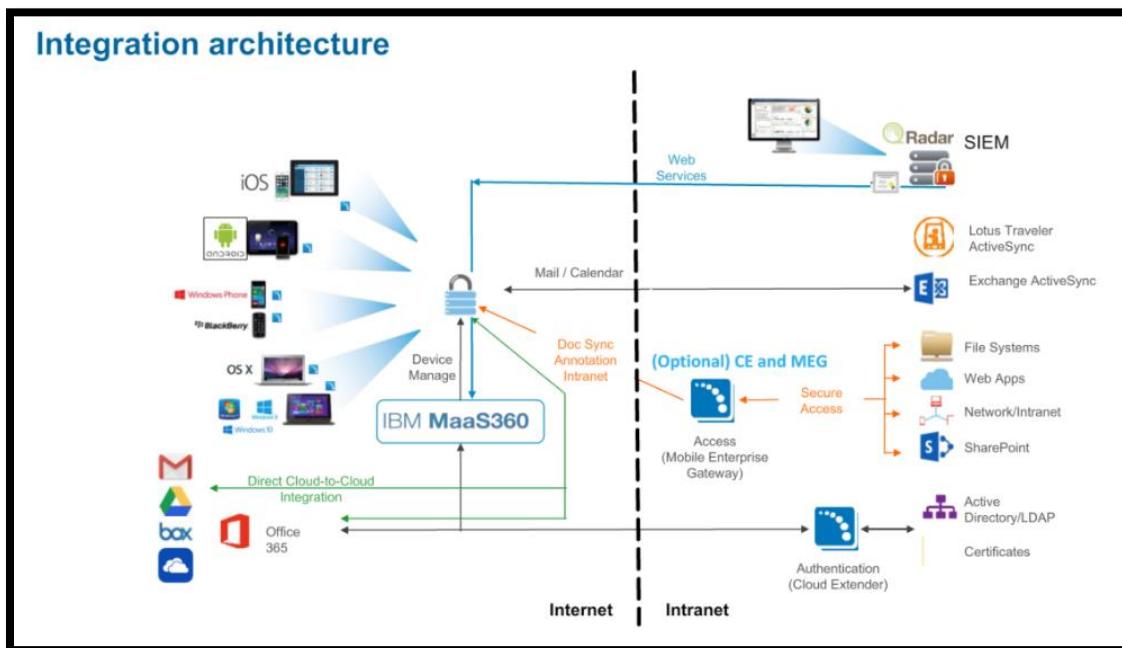
2. Now here click on link given:



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

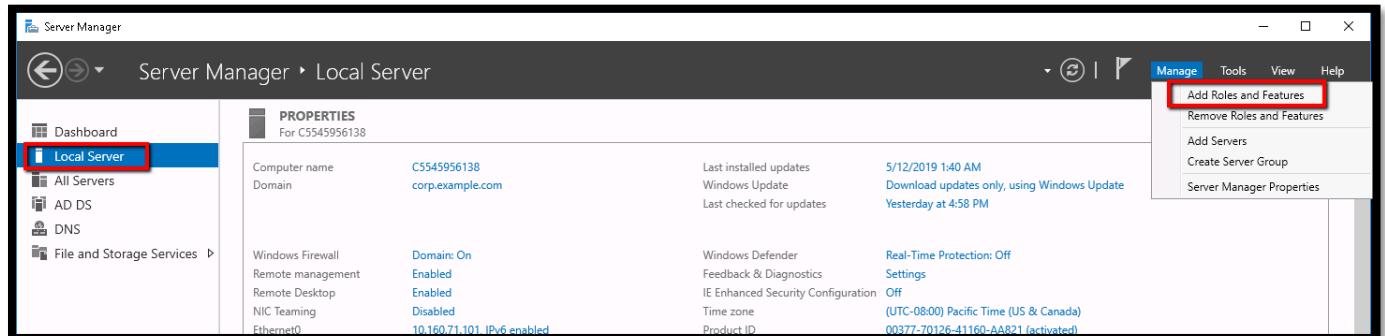


## 6.8 Configuration of server setup:



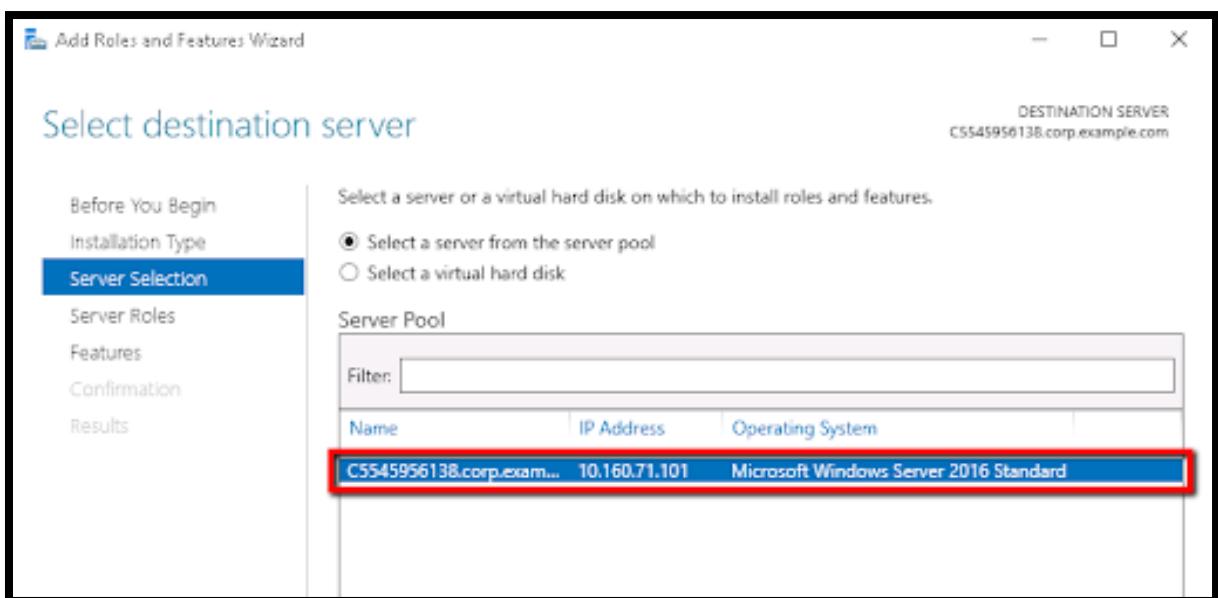
As per requirement to setup cloud extender configuration tool in project. First we need to setup Windows server as a system to download:

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:

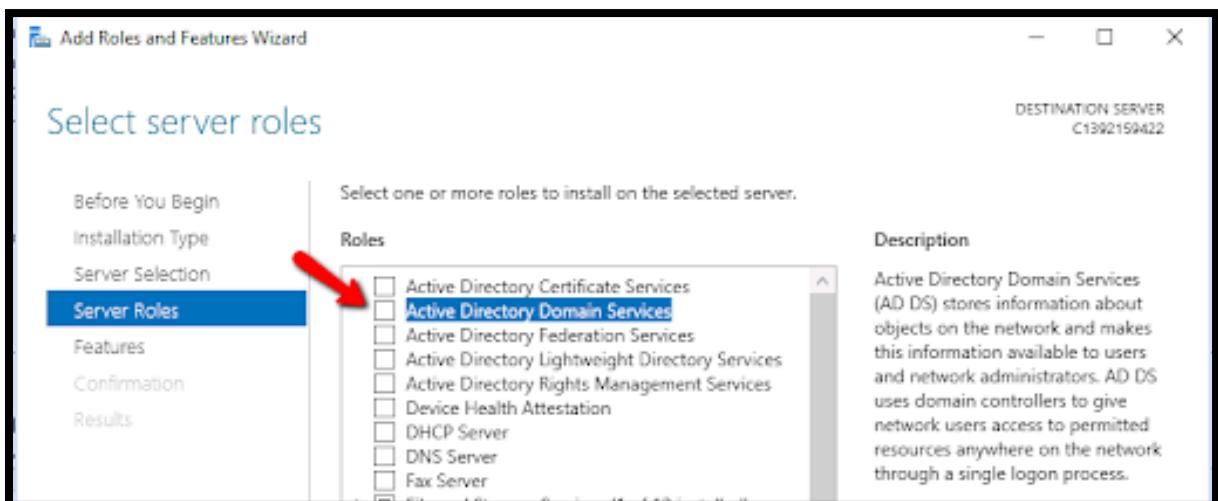


Next should be selected. The Wizard will now move on to the option for Installation Type.

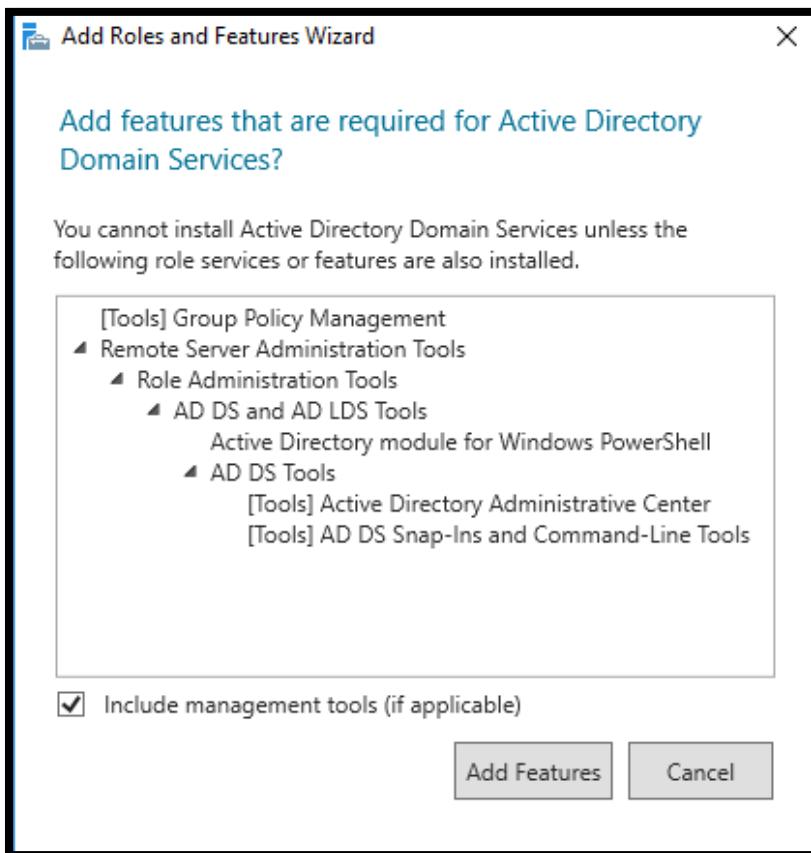
3. Choose between a role-based or feature-based installation.
4. Select Next. The panel Select destination server appears:



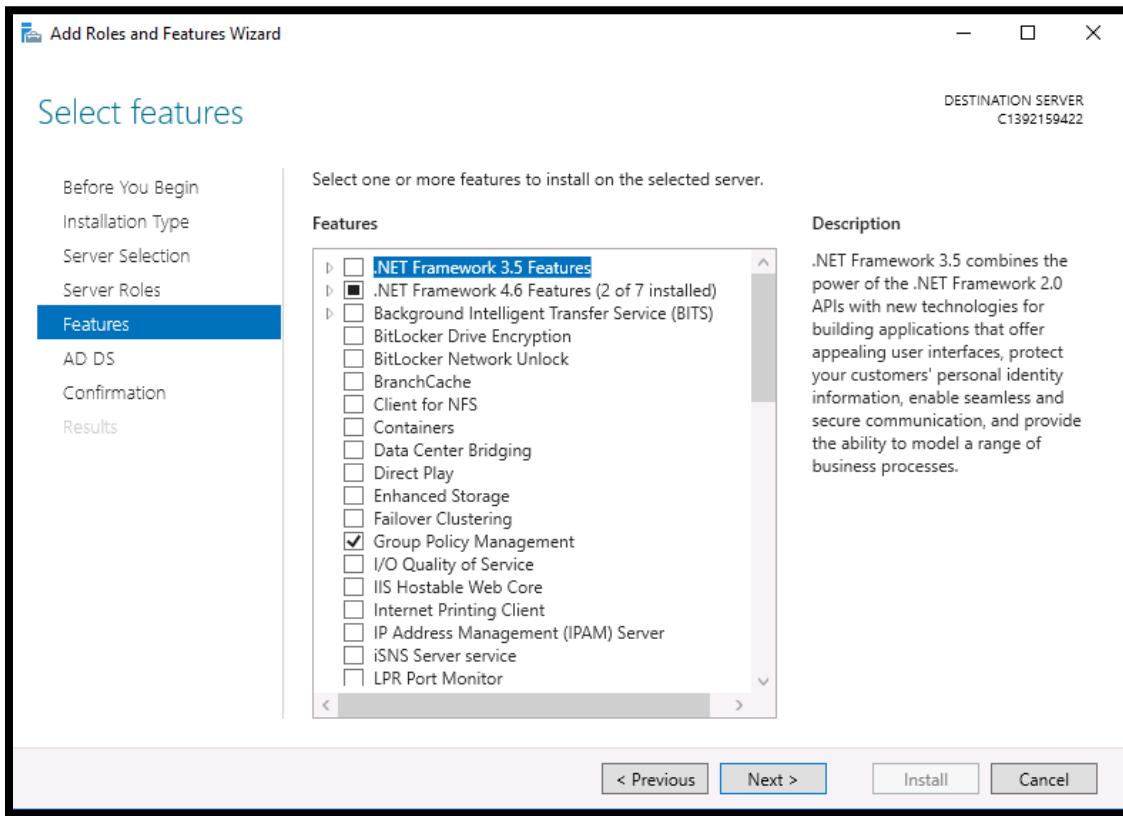
5. The server to which the installation will be applied should be selected by default. Click Next after confirming that the intended server has been picked from the server pool (or selecting the desired server). The Choose Server Roles screen appears:



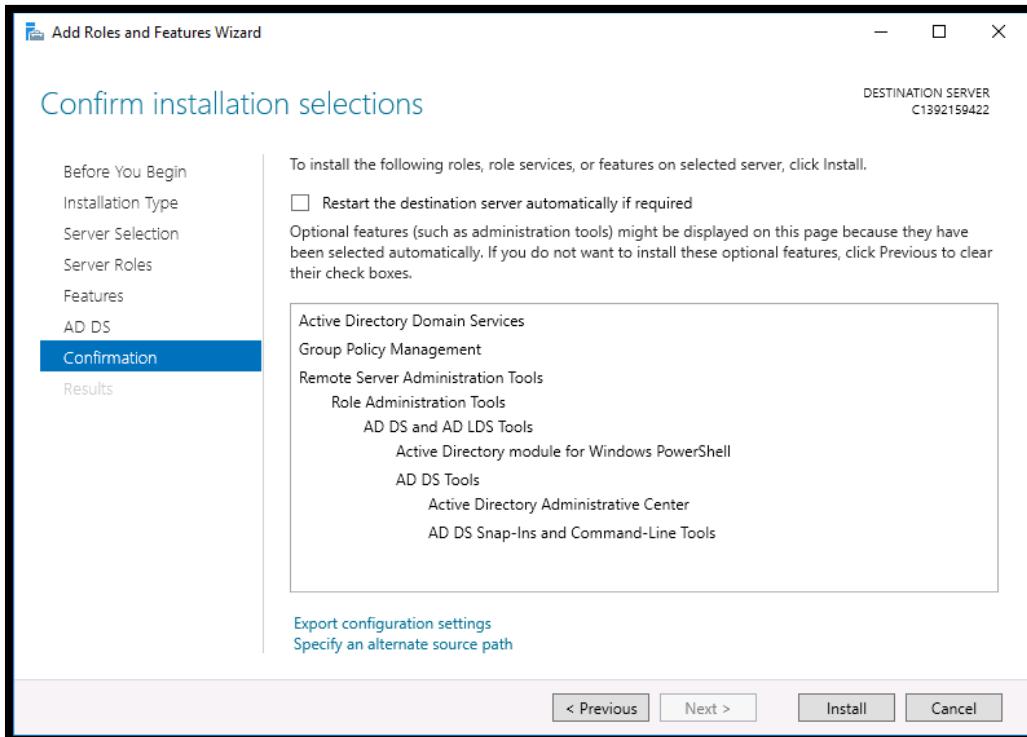
6. To activate user role in server, click on active directory domain services checkbox.
7. Click **Next**. The required features list is displayed:



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



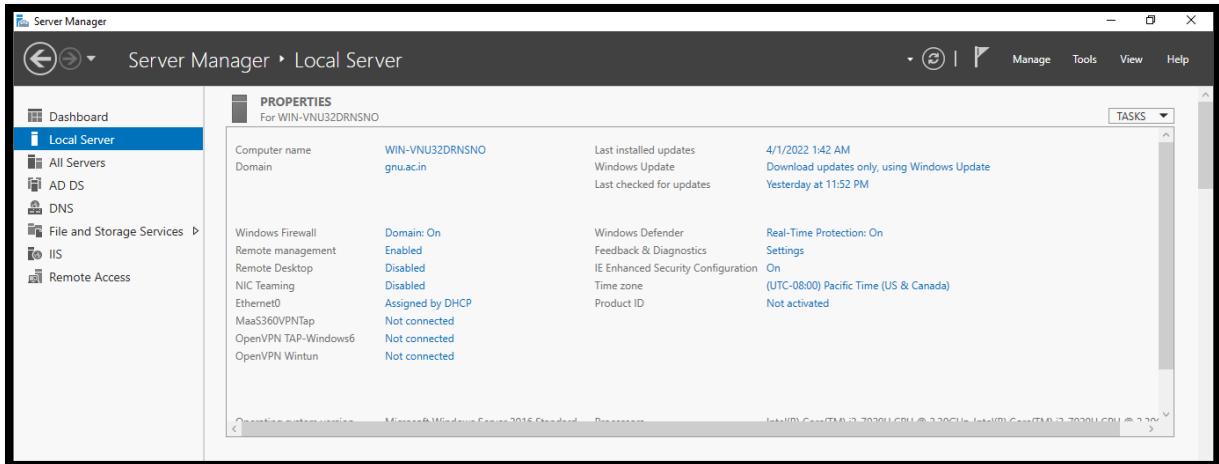
9. After clicking on next we get final option to install the particular update version of server:



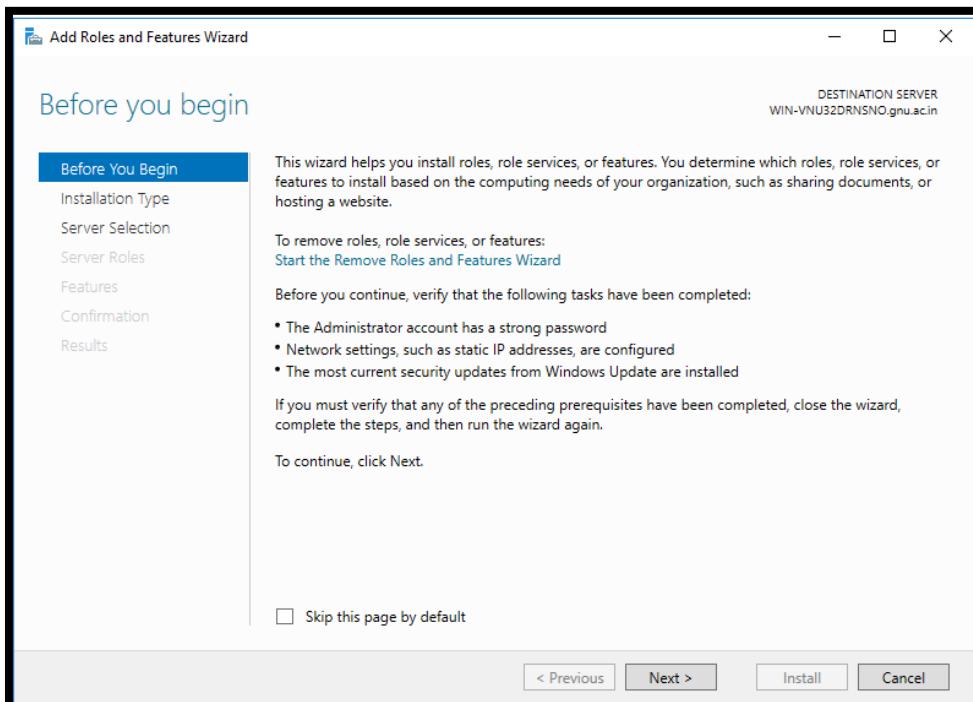
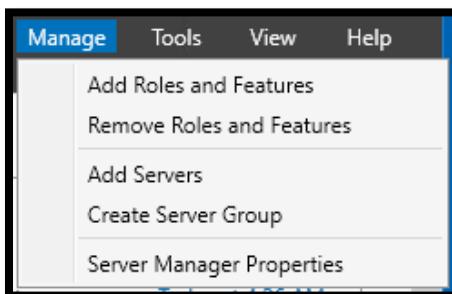
10. If all selections are correct, click **Install**.

## 6.9 Configure DNS server:

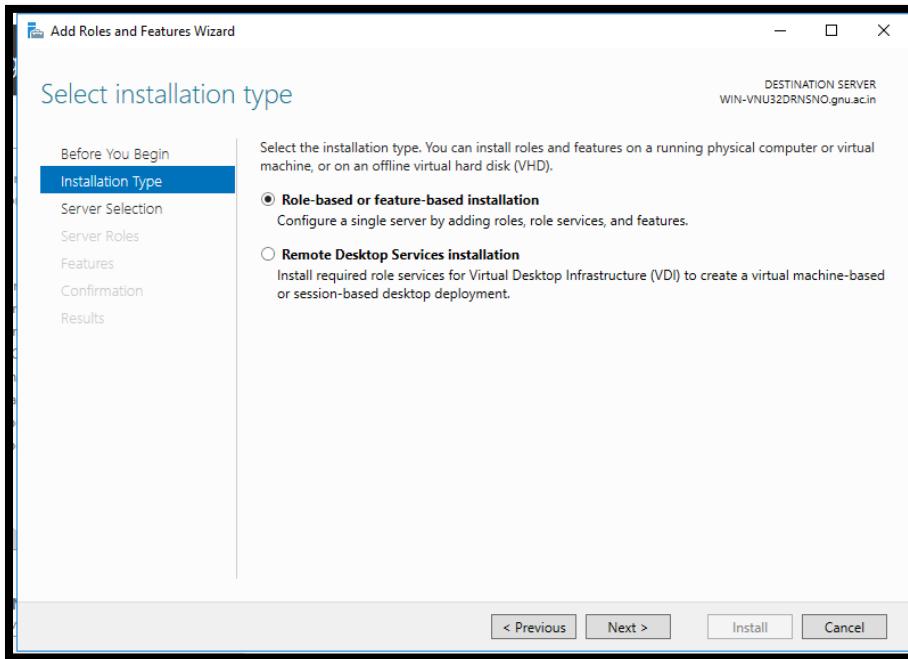
1. To proceed to local server first open the server manager window:



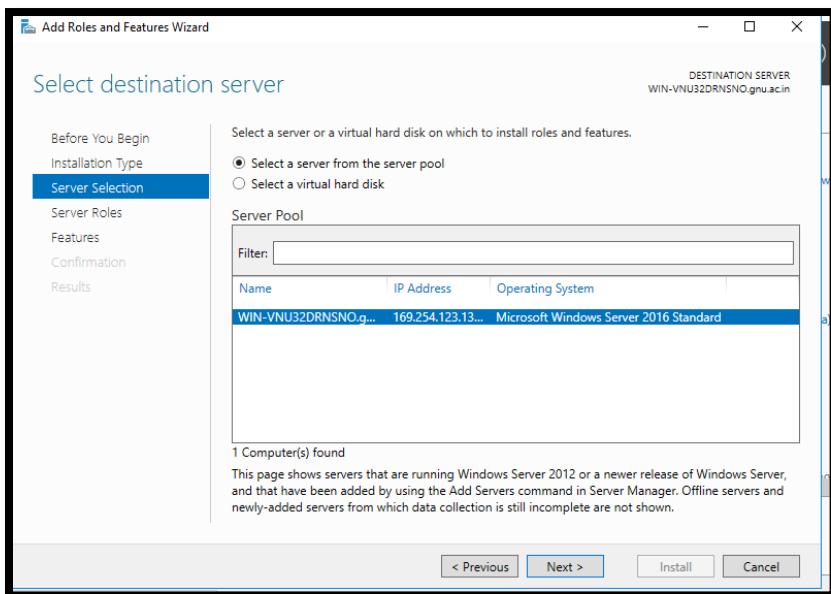
2. To add feature and roles in this click on tools and select add roles and features:



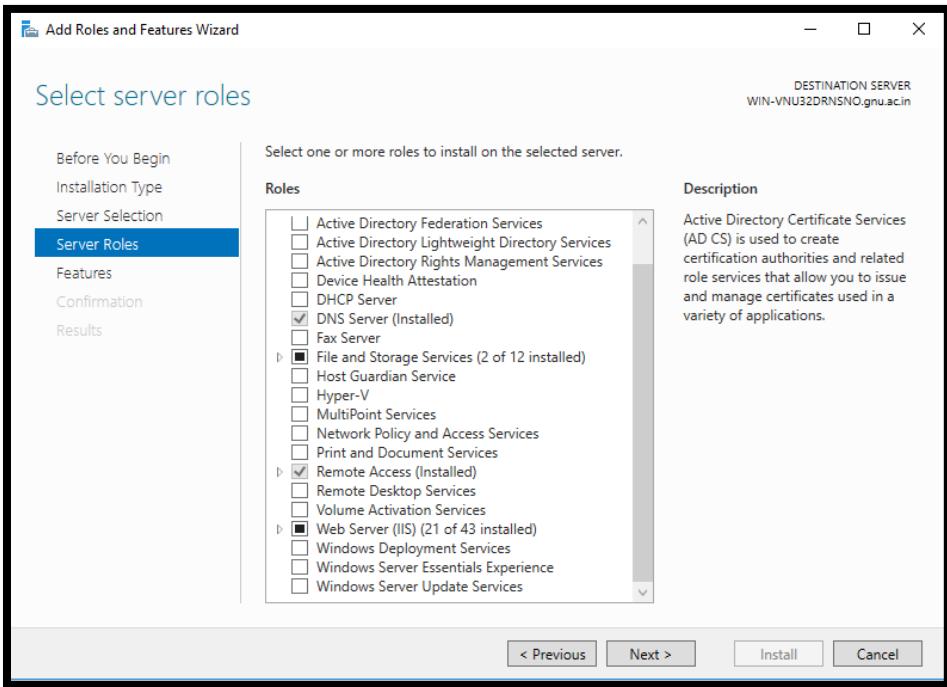
3. If you are using Role-based or Feature-based installation, select the radio button next to it



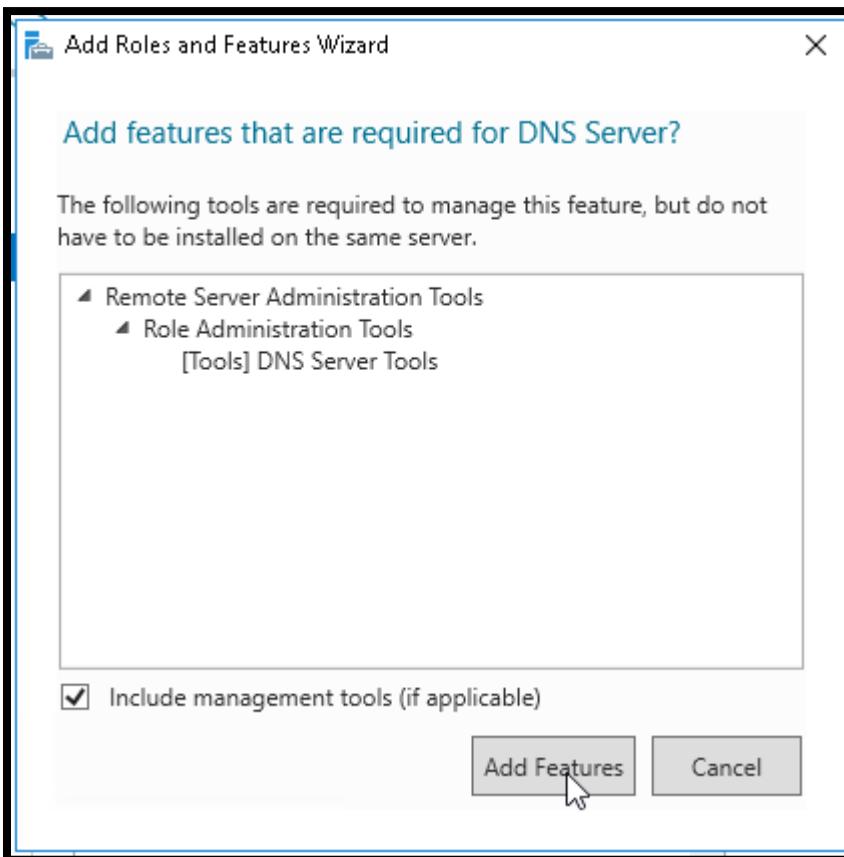
4. Choose the server that will be used for this function. It's usually the same as the machine you're looking at this on for a DNS-Only configuration. However, there is the ability to install the role remotely.



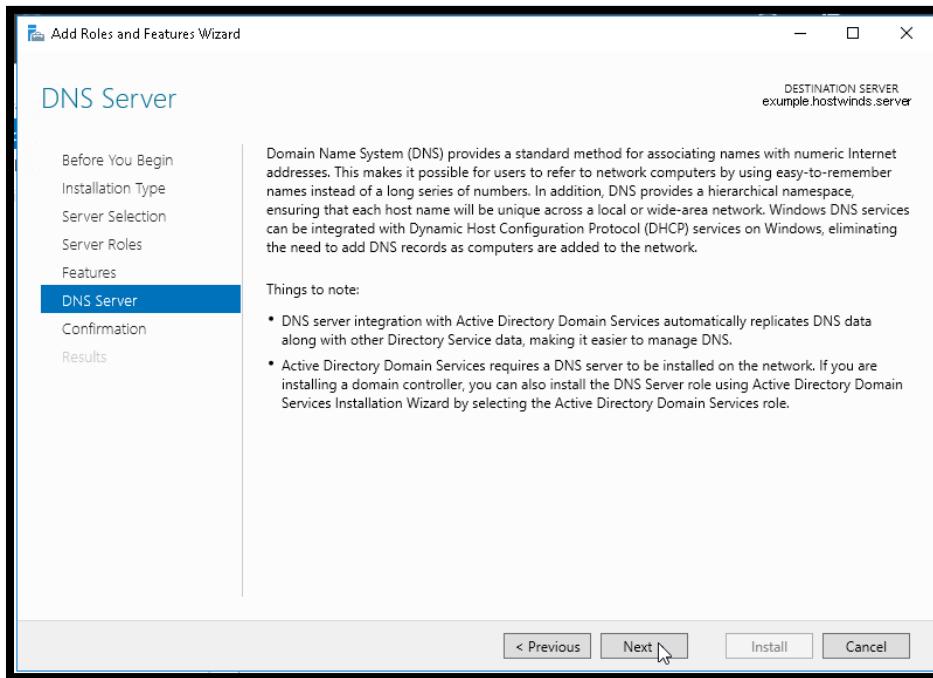
5. Tick mark checkbox of DNS Server.



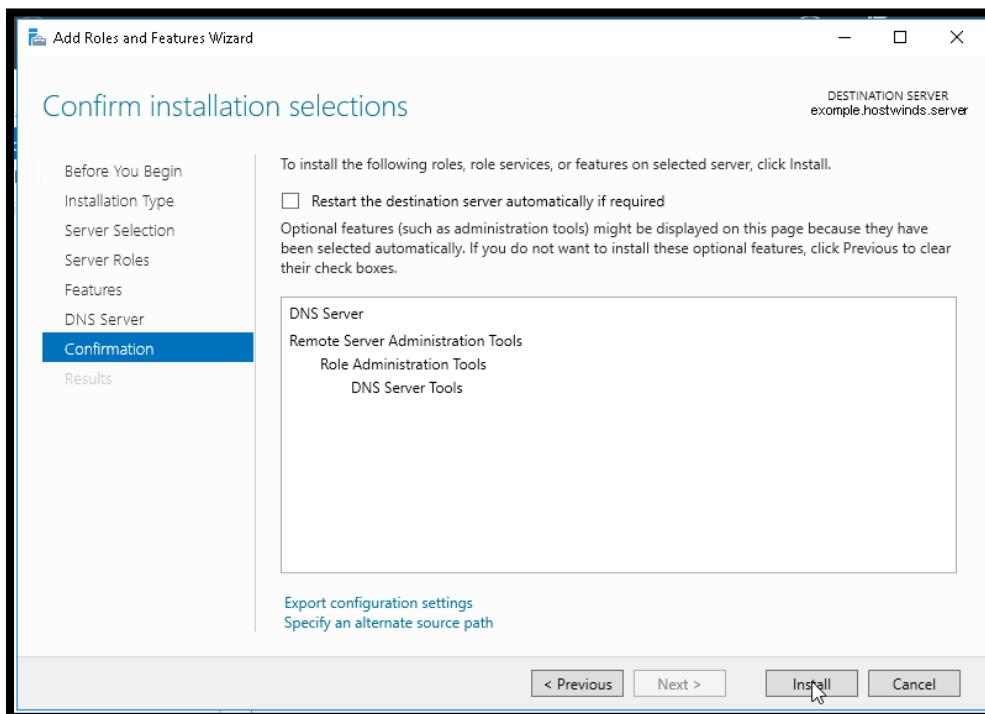
6. A window then asks you to confirm the dependencies (usually just the Administration Tools required for the DNS role) also to be installed. Click Add Features, as this is usually required

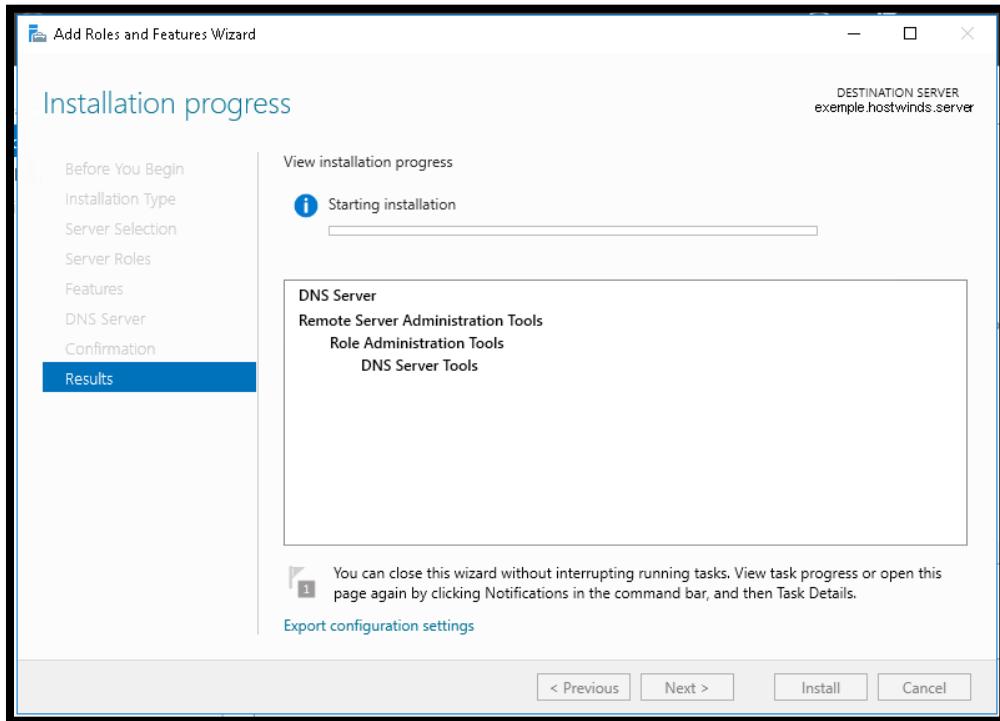


- A black check icon should be placed next to the check box. This is usually reserved for File & Storage Services by default). Then, to proceed, click Next.
- In the next box, it offers you a brief description of the services and their tasks, as well as a list of objects that this role may affect or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



- 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.





## **6.10 Configuring Cloud extender:**

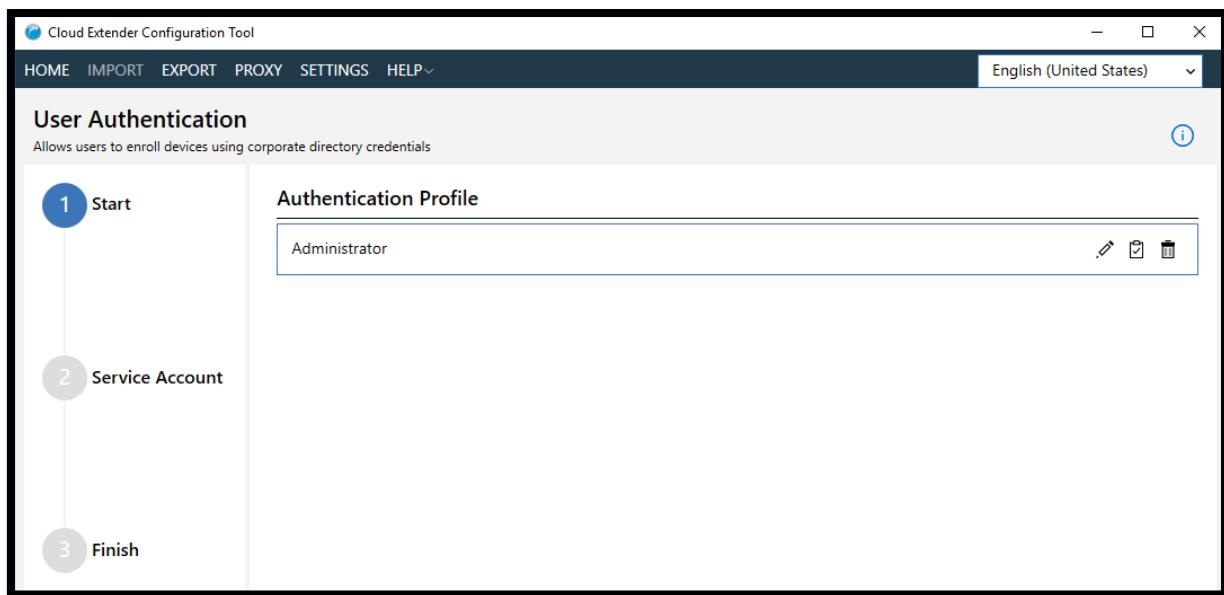
1. Double-click the MaaS360 Cloud Extender Install icon to begin the installation process.
2. To go to the Install Location screen, click Next.
3. Click Next after selecting your destination folder.
4. Enter your Account ID and the licence key number you received in the Welcome email message, then click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

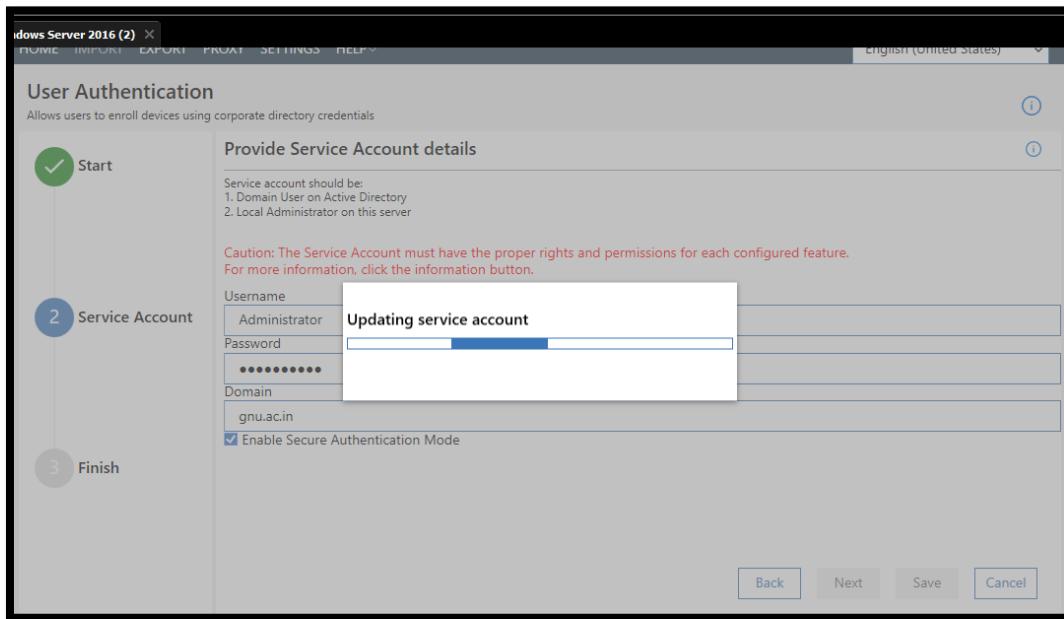
5. Click Install, and then click Next to continue the installation.
6. When prompted, click Finish to start the Cloud Extender Configuration Tool

### 6.10.1 User authentication:

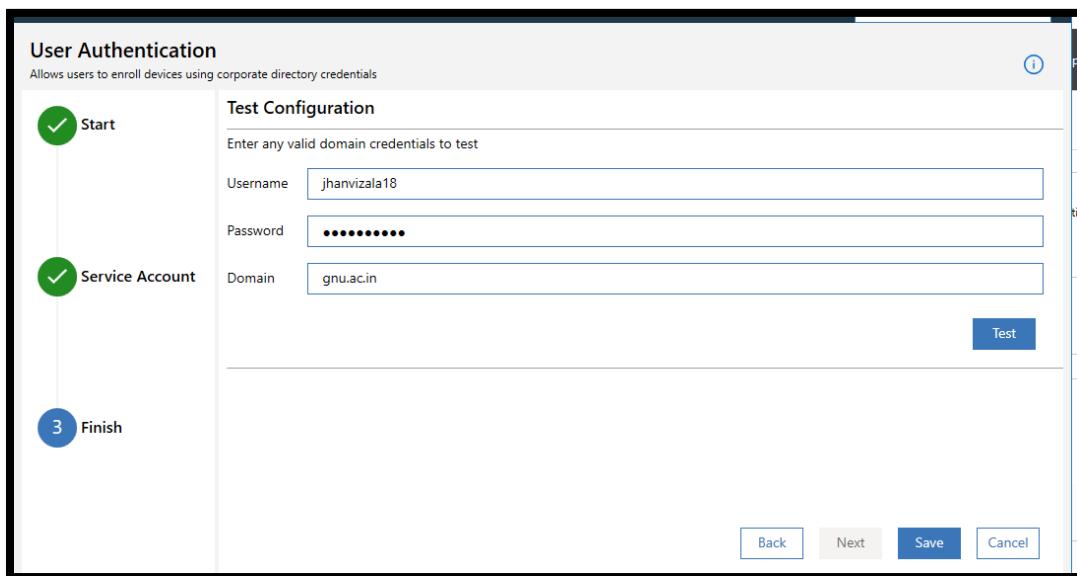
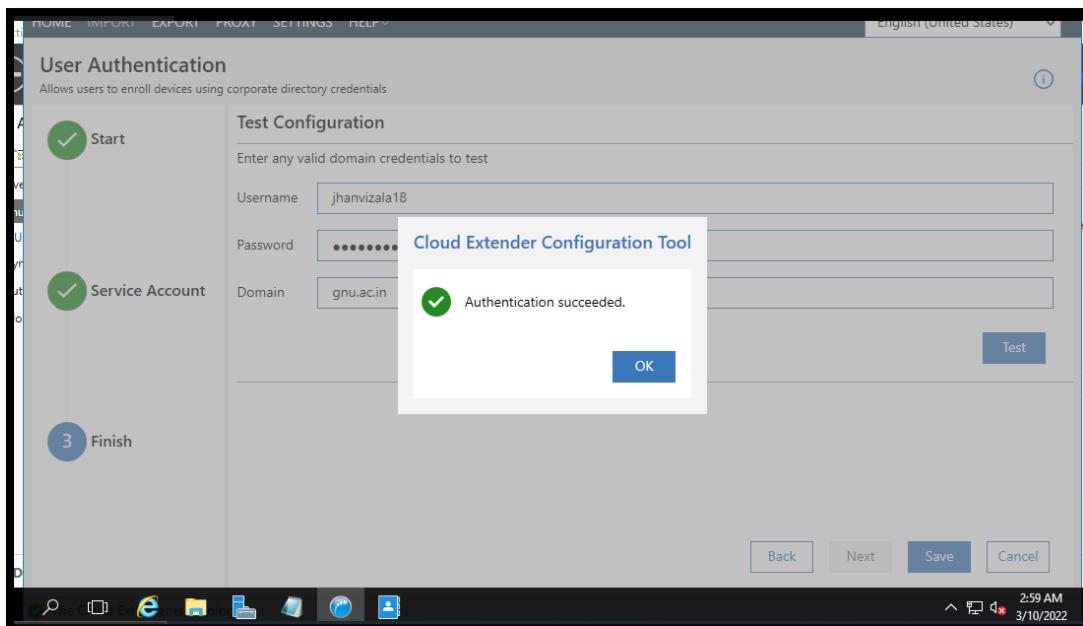
- Select User Authentication in the Cloud Extender Configuration Tool.
- Click Next after selecting the authentication mode you want to configure: Active Directory or LDAP.
- Complete the service account configuration.



- 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 the MaaS360 Portal Home page, select **Setup > Cloud Extender Settings**.

**Default Cloud Extender Policy**

Last Published: 03/31/2022 06:51 UTC [Version:1] Current Status: Needs Publish

**Cloud Extender Settings**

- Health Check Alerts** (selected)
- Exchange ActiveSync
- IBM Traveler and IBM Connections Cloud
- Health Check Configuration

**Enable Cloud Extender Health Check Alerts**: Yes

**Configure Alert and Notification Settings**

**Alert Notification Settings**

**Subscribe to email notifications**: Yes

**Send email notifications for**: All Alerts

**Email addresses to be notified**: jhanvizala18@gnu.ac.in

**Subscribe to SMS notifications**: No

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

**Default Cloud Extender Policy**

Last Published: 03/31/2022 06:51 UTC [Version:1] Current Status: Needs Publish

**Cloud Extender Settings**

- Health Check Configuration**
- Exchange Alerting
- IBM Traveler Alerting
- User Authentication Alerting** (selected)
- AD User Visibility Alerting
- Certificate Integration Alerting
- Email Notifications

**User Authentication Alerting**

**Invalid credentials**

**Subscribe to notifications**: Yes

**Critical Alert**: Yes

**Authentication taking more than configured limit**

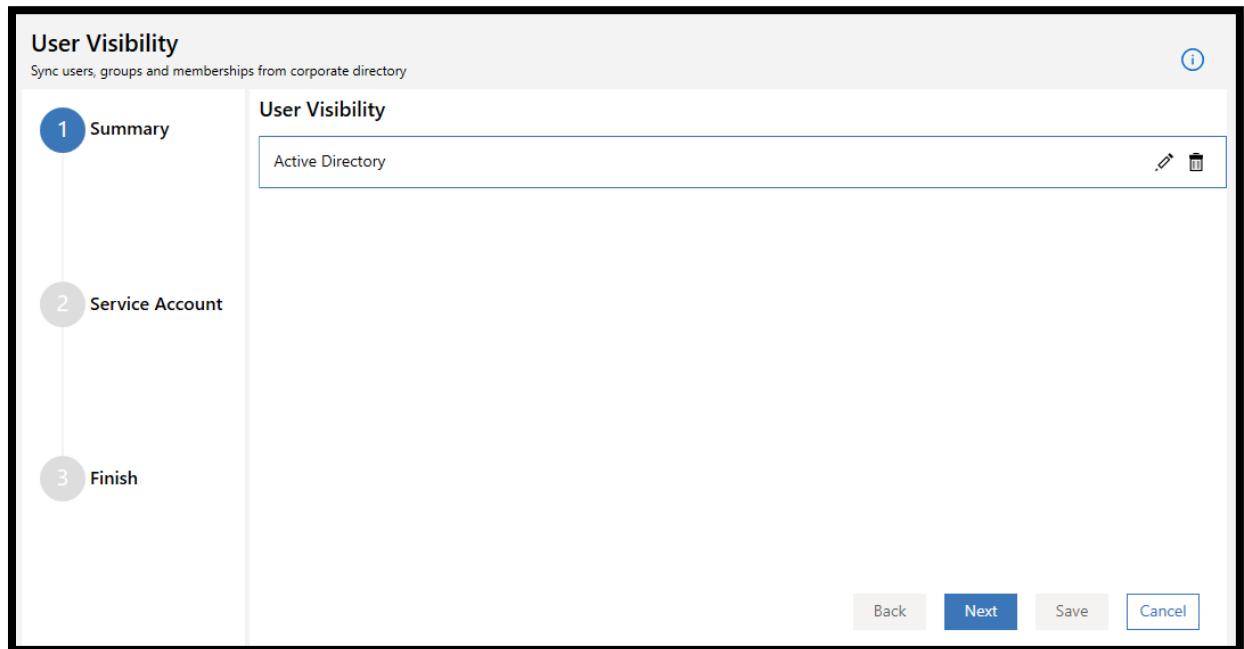
**Subscribe to notifications**: Yes

Username: drishitmotwani18@gnu.ac.in | Account ID: 40047141 | Last Login: Friday, April 8, 2022 12:29:08 PM UTC| [PRIVACY AND LEGAL](#)

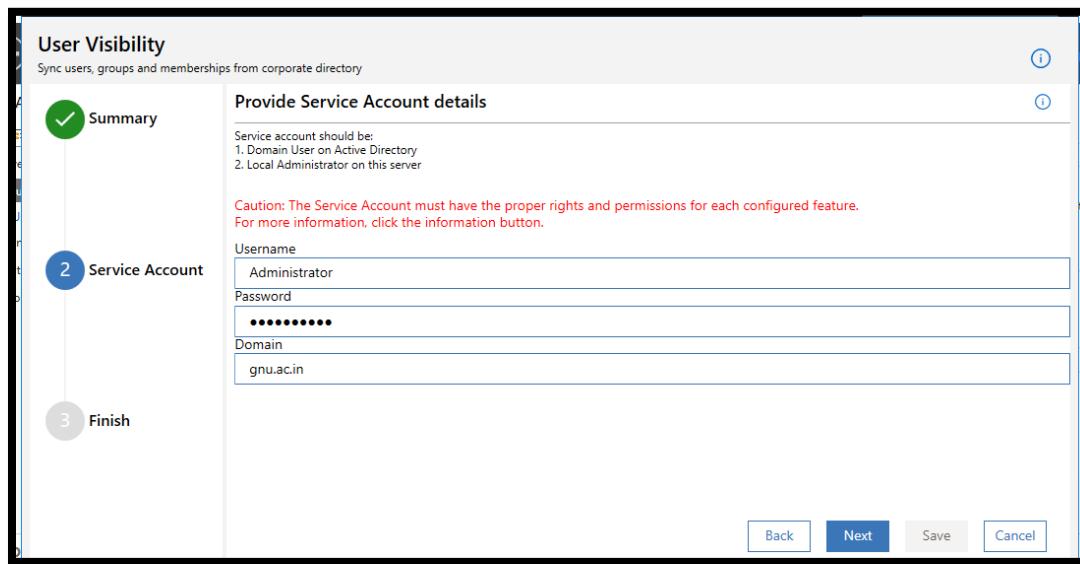
[Cookie Preferences](#)

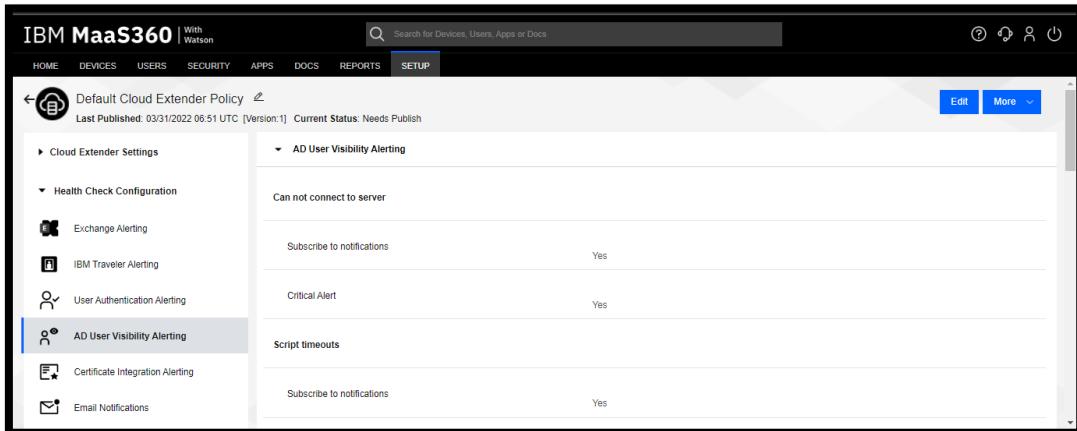
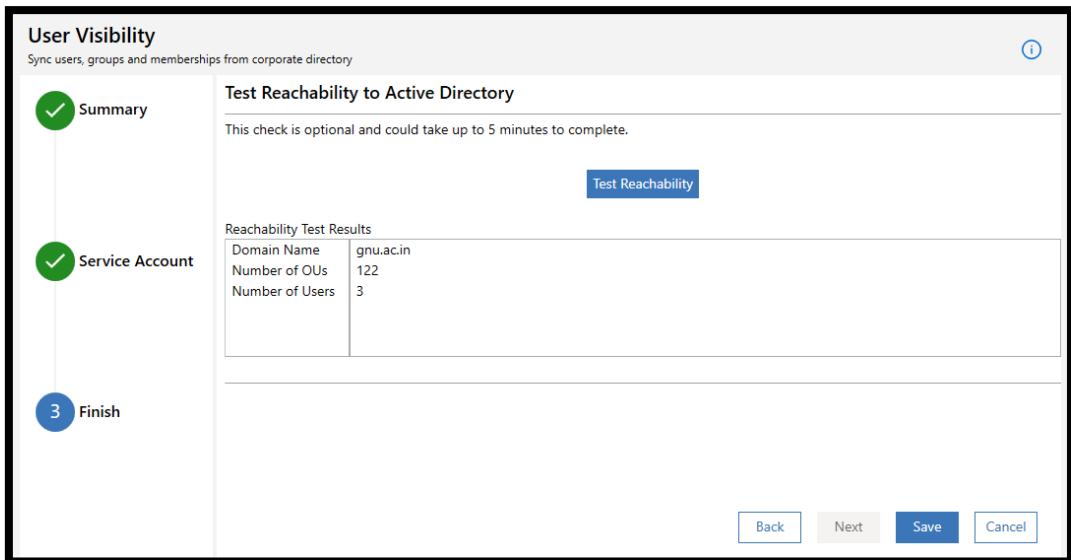
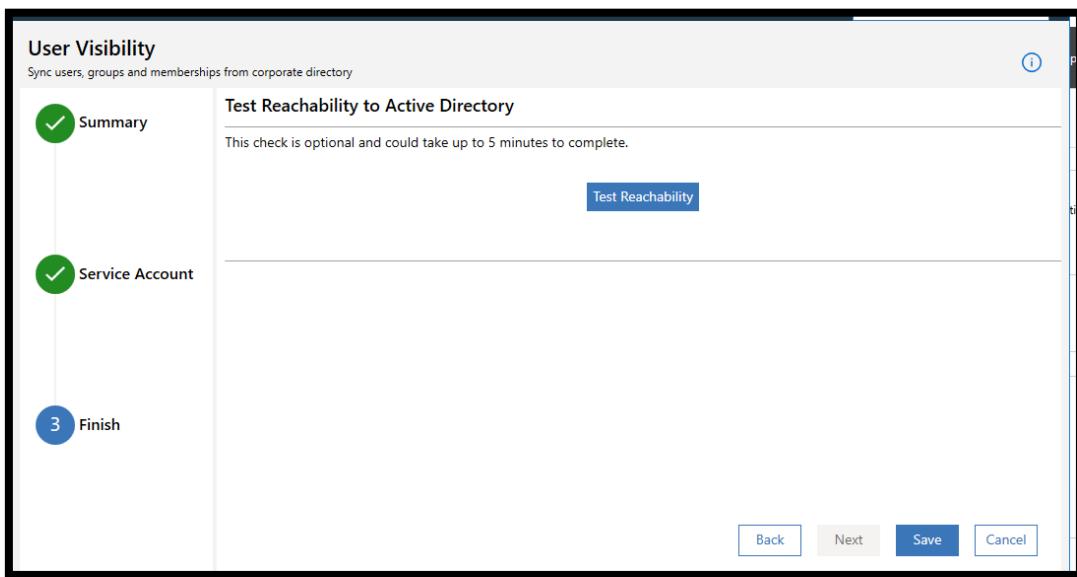
### 6.10.2 User Visibility:

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



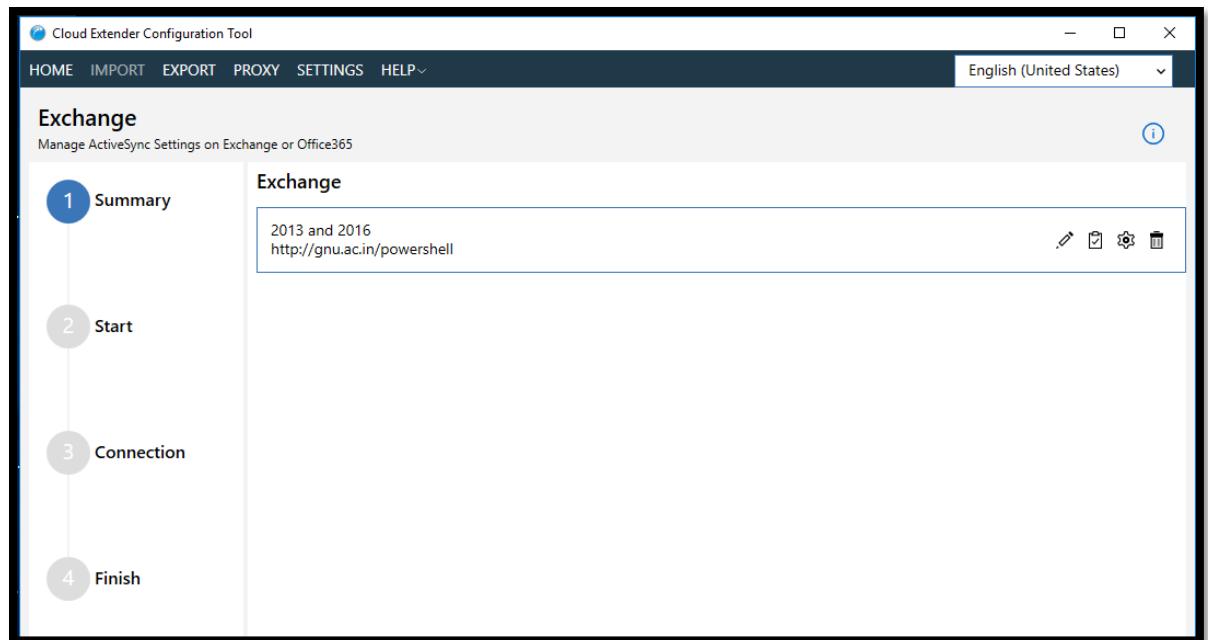
- Choose Basic to see a list of all users and groups in the directory.
- To see if your service account can discover domains, object users (OU), and users, run a reachability test.



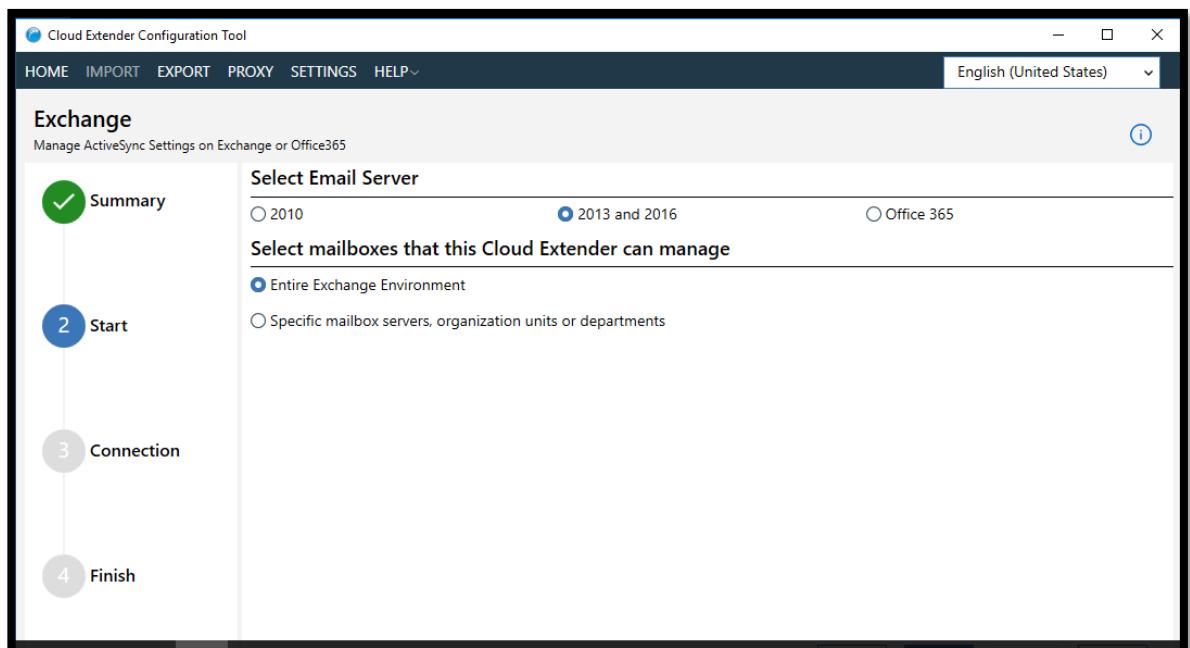


### 6.10.3 Configure Exchange:

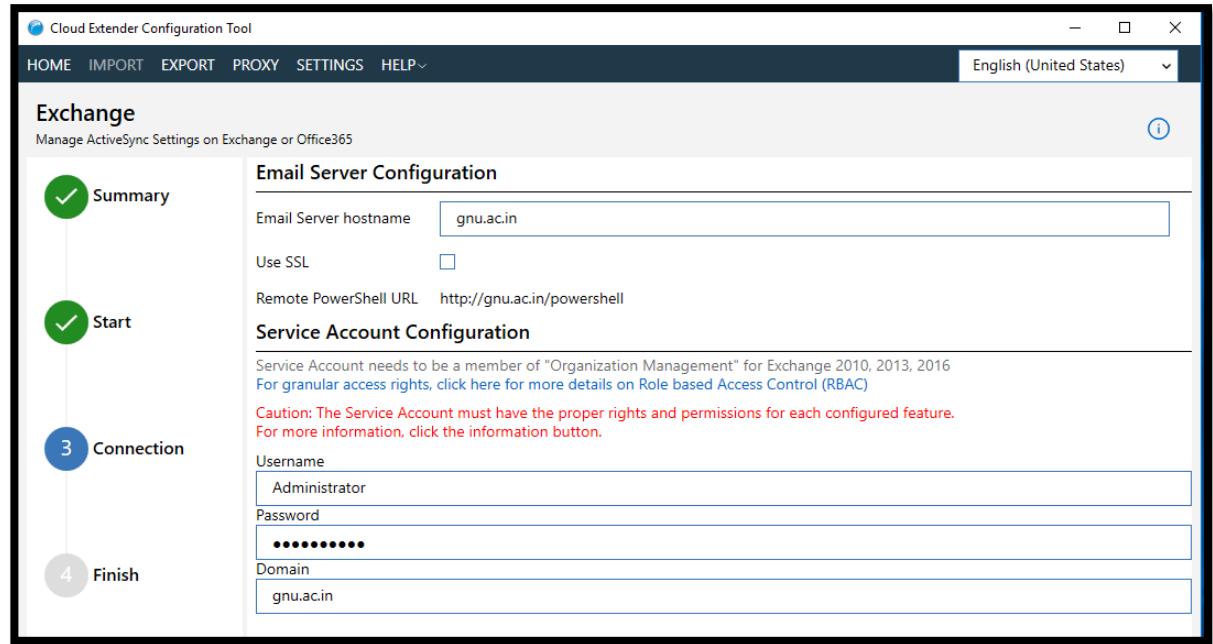
- Open the Cloud Extender Configuration Tool and select **Exchange**.
- Select the version of Exchange that you are using, and click **Next**.



- 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

The screenshot shows the 'Basic Information' step of the 'Create API role' wizard. It includes fields for 'Role Name\*' (API role) and 'Role Description\*', and a section for selecting mode of creation ('Select From Existing' or 'Create new'). A 'Next' button is at the bottom.

**1. Basic Information**

Role Name\*

Role Description\*

**2. Select Mode of Creation**

Select From Existing

Create new

**Next**

### b. Adding Web services access keys

The screenshot shows a list of permissions under 'Right to Access'. The 'Web Service - Access Keys' checkbox is selected and highlighted in grey, indicating it has been chosen.

Right to Access	Category	Description
<input type="checkbox"/> Apps - Read-only	App Distribution	View only access to Apps.
<input type="checkbox"/> Distribute Apps	App Distribution	Ability to distribute Apps.
<input type="checkbox"/> Manage Apps	App Distribution	Ability to add, change or delete Apps.
<input type="checkbox"/> Manage Apps Only No Distribution	App Distribution	Allow access for only managing apps, but not distributing them
<input type="checkbox"/> App Attributes - All Access	App Management	Provides user with the ability to manage custom Attributes
<input type="checkbox"/> Installed Apps - Read-only	App Management	Provides user with the ability to view installed apps workflow.
<input checked="" type="checkbox"/> Web Service - Access Keys	Auth Management	Ability to manage Web Service Access keys
<input type="checkbox"/> Action History	Device Management	Ability to view a global action history across all devices.
<input type="checkbox"/> Approve Device	Device Management	Ability to approve a blocked or quarantined device (ActiveSync/Traveler).
<input type="checkbox"/> Block Device	Device Management	Ability to block an approved or quarantined device (ActiveSync/Traveler).
<input type="checkbox"/> Bulk Upload Custom Attributes	Device Management	Ability to bulk upload a file to set custom attributes.
<input type="checkbox"/> Buzz Device	Device Management	Ability to buzz a device through a Device View action.
<input type="checkbox"/> Change Compliance Rule Set	Device Management	Ability to change a compliance rule set through a Device View action.
<input type="checkbox"/> Change Device Policy	Device Management	Ability to change a device policy through a Device View action.

IBM MaaS360 | With Watson

HOME DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Manage Roles

Role Name	Role Description	Last Updated By	Last Updated Date
API role	API role	yamanaka@au1.ibm.com	04/04/2022 05:50 UTC

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

360 | With Watson

USERS SECURITY APPS DOCS REPORTS SETUP

Keys

How to use access keys, click here

App ID
40047141_LFZFPPrz
40047141_FvZh0a

Jump To Page Displaying 1 - 2 of 2 Records Show 25

Generate Access Key

Type\* MaaS360 Web Services

Key Name\* Maas

Copy To Customer

Generate

Access Key Details

Generate Access Key

Status	PlatformID	*	3
Inact	Version		1.0
Activ	App ID		40047141_LFZFPPrz
Recor	Access Key		d4zewhfkq6

Close

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

The screenshot shows the IBM MaaS360 interface with the 'SETUP' tab selected. A POST request is being configured:

- Parameter:** billingId, Value: 40047141
- body:**

```
<?xml version="1.0"?>
<authRequest>
<maaS360AdminAuth>
<platformID>3</platformID>
<billingID>40047141</billingID>
<password>IBMProject@28</password>
<userName>drishtimotwani18@gnu.ac.in</userName>
<appId>40047141_FvZjh0a</appId>
<appVersion>1.0</appVersion>
<appAccessKey>tsLFSDyn9</appAccessKey>
<maaS360AdminAuth>
</authRequest>
```

Below the body, it says "Parameter content type: application/xml". There are "Try it out!" and "Hide Response" buttons.

The screenshot shows the response from the previous API call:

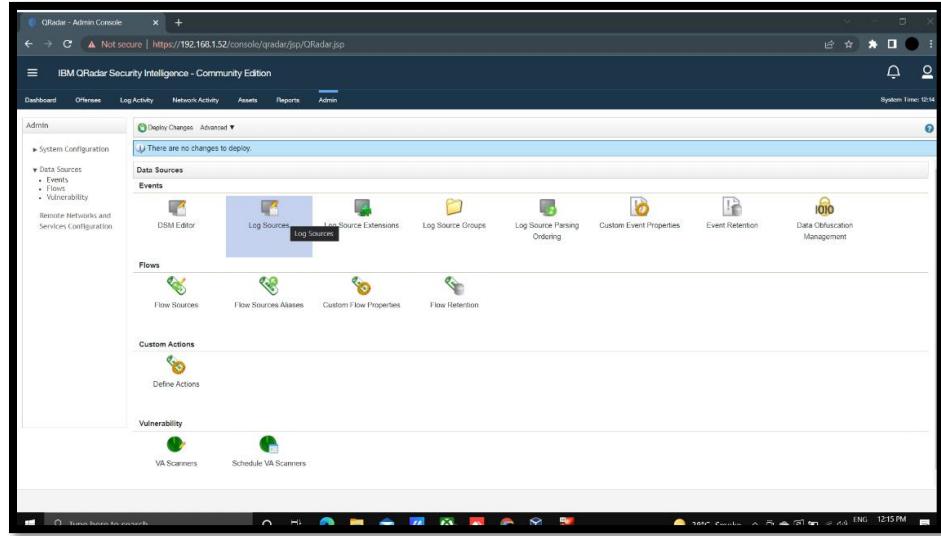
- Response Body:**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<authResponse>
<authToken>b0600dd0-df2c-49f1-aa52-49af4c112744-Ga3jSm2</authToken>
<errorCode>0</errorCode>
</authResponse>
```

- Response Code:** 200
- Response Headers:**

```
{
  "content-length": "175",
  "content-type": "application/xml",
  "x-rate-limit-max": "250000",
  "x-rate-limit-remaining": "249940",
  "x-rate-limit-resetwindow": "1627"
}
```

g. To integrate with QRadar go to log sources



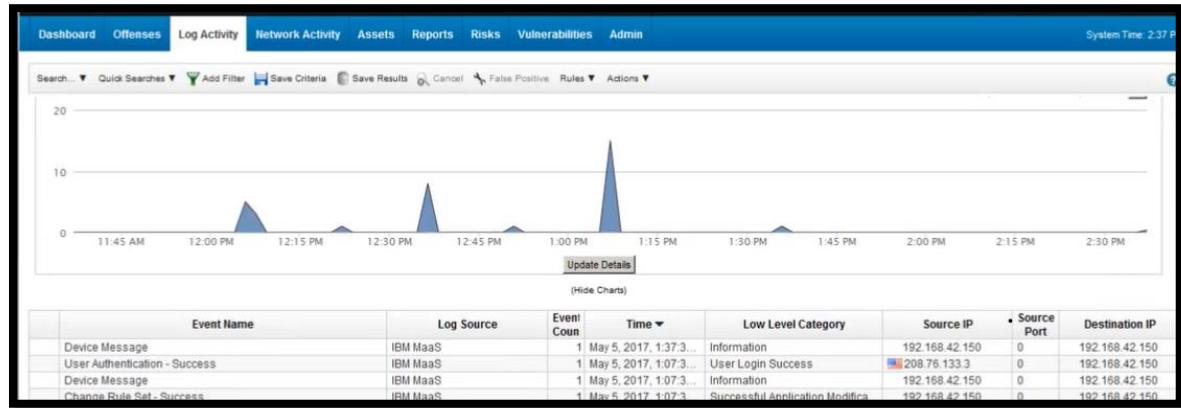
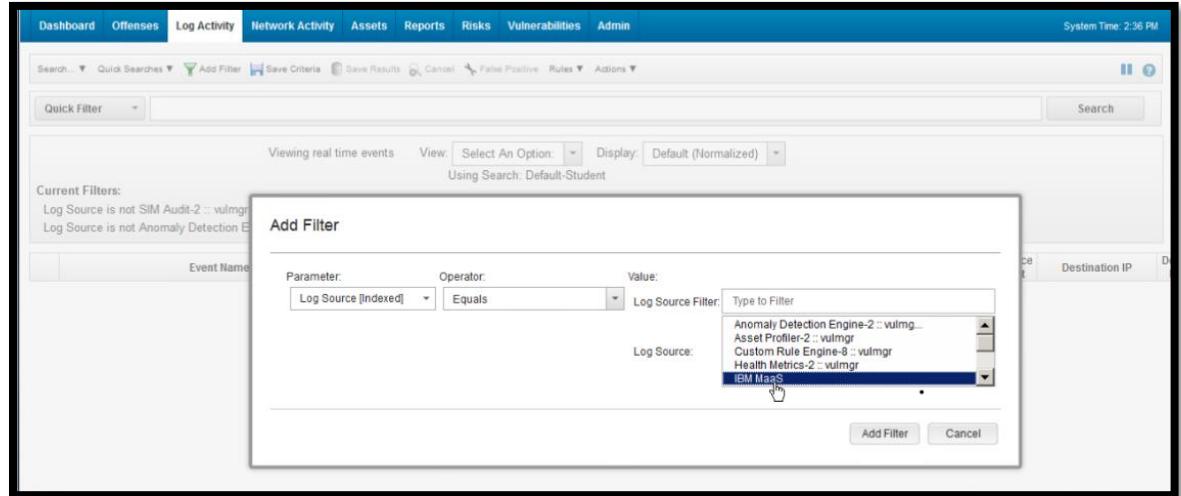
h. Create a new source

A screenshot of a web-based configuration form titled "Edit a log source". The form fields are as follows:

- Log Source Name: IBM MaaS
- Log Source Description: log from IBM MaaS360
- Log Source Type: IBM Fiberlink MaaS360
- Protocol Configuration: IBM Fiberlink REST API
- Log Source Identifier: Maas
- Login URL: https://services.m4.maas360
- Username: drish@mitwani18@gnu.ac.in
- Password: (redacted)
- Password Confirm: (redacted)
- Secret Key: (redacted)
- App ID: 40047141\_LFZFPz
- Billing ID: 40047141
- Platform: 3
- App Version: 1.0
- Use Proxy: (checkbox)
- Automatically Acquire Server Certificate(s): No
- EPS Throttle: 5000
- Recurrence: 15M
- Enabled: (checkbox, checked)

The status bar at the bottom right shows a green progress bar.

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>

