



2021.0

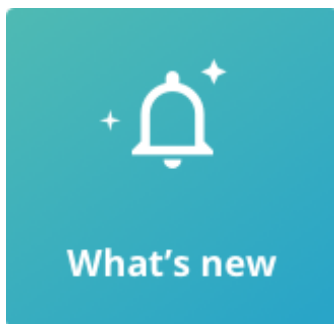
Administrator Guide

Contents

| | |
|---|----|
| 1. Administrator Guide for WorkZone Mobile 2021.0 | 4 |
| 2. What's new | 5 |
| 3. About WorkZone Mobile | 9 |
| 4. WorkZone Mobile feature overview | 10 |
| 5. Architecture | 13 |
| 6. Security considerations | 15 |
| 7. Installing WorkZone Mobile | 16 |
| 8. Microsoft Intune | 17 |
| 8.1 WorkZone Mobile requirements to Microsoft Enterprise Mobility Suite infrastructure | 18 |
| 8.2 Create a group of WorkZone users | 21 |
| 8.3 Publishing WorkZone Web services in Azure Application Proxy | 21 |
| 8.4 Creating a native API for WorkZone Mobile | 28 |
| 8.5 Publishing the WorkZone Mobile iOS app on Microsoft Intune (Azure Portal) | 32 |
| 8.6 Publishing the WorkZone Mobile Android app on Microsoft Intune (Azure Portal) | 38 |
| 8.7 Set up security and access from mobile devices | 46 |
| 8.8 Push notification certificates for iOS | 58 |
| 9. Citrix XenMobile | 60 |
| 9.1 WorkZone Mobile requirements to Citrix XenMobile infrastructure | 60 |
| 9.2 Wrap the WorkZone Mobile app using Citrix MDX Toolkit | 63 |
| 9.3 Publish WorkZone Mobile in Citrix XenMobile | 71 |
| 10. Document formats supported in preview | 78 |
| 11. Known issues | 80 |
| 12. Terms and conditions | 82 |

1. Administrator Guide for WorkZone Mobile 2021.0

This guide describes the WorkZone architecture that WorkZone Mobile is part of, security considerations, how to install WorkZone Mobile, and other information relevant for a WorkZone administrator.



[Support matrix](#)

[WorkZone Mobile feature overview](#)

Related product documentation

- [WorkZone Mobile User Guide](#)

2. What's new

WorkZone Mobile 2021.0

- Instructions for Intune users on how to [set up security and access from mobile devices](#) are updated to include multi-factor authentication (step 14), [setting up multi-factor authentication](#), and [logging in to edit the Office documents](#).
- Feature overview updates: chat enhancements. See [Feature overview](#).

WorkZone Mobile 2020.3 Feature overview updates

- New chat enhancements.
- WorkZone Mobile version for Intune (iOS) now supports editing WorkZone documents with Microsoft Office 365.

See [Feature overview](#).

WorkZone Mobile 2020.2

- Chat module added to [Feature overview](#).
- New task rank and view task as a single PDF file features (under **Task** module) are now available for Android version. See [Feature overview](#).

WorkZone Mobile 2020.1

No changes in this release.

WorkZone Mobile 2020.0

No changes in this release.

WorkZone Mobile 2019.3

- [WorkZone Mobile feature overview](#) updated with the new task rank and view task as a single PDF file features.
- [WorkZone Mobile requirements to Citrix XenMobile infrastructure](#) are updated.
- Instructions on [publishing WorkZone Mobile in Citrix](#) are updated to include MDX 19.X version.

WorkZone Mobile 2019.2

- The WorkZone Mobile app can now run on Android 8.X
- Guidance on how to configure [Publishing the WorkZone Mobile Android app on Microsoft Intune](#) has been added to the guide.

WorkZone Mobile 2019.1

A version of WorkZone Mobile can now be installed and managed through Microsoft Intune. See the WorkZone Mobile [feature overview](#) for an overview of the features that KMD WorkZone for Intune supports.

WorkZone Mobile 2019.0

No changes in this release.

WorkZone Mobile 2018.2

No changes in this release.

WorkZone Mobile 2018.1

- You can now deploy WorkZone Mobile through Citrix XenMobile. See [Citrix XenMobile](#).

WorkZone Mobile 2018 (1283)

- An overview of which features are available on iOS and Android and on which device type. See WorkZone Mobile [WorkZone Mobile feature overview](#).
- You can now find instructions on how to deploy WorkZone Mobile using Microsoft Intune. See [Microsoft Intune](#).

WorkZone Mobile 2017 (4.5.3)

No changes.

WorkZone Mobile 2017 (4.5.2)

No changes.

WorkZone Mobile 2017 (4.5.1)

No changes.

WorkZone Mobile 2017 (4.5.0)

No changes.

WorkZone Mobile 2017 (4.3.1)

No changes.

WorkZone Mobile 2017 (4.3.0)

No changes.

WorkZone Mobile 2017 (4.2.0)

- WorkZone Mobile requires that WorkZone Mobile with policies is installed to be able to open documents in PDF format in the document viewer. See [Installing WorkZone](#)

Mobile.

- Supported document formats for document preview have been updated, see [Document formats supported in preview](#).

3. About WorkZone Mobile

WorkZone Mobile is a mobile client in the WorkZone case and document management suite. WorkZone Mobile allows the user to work with tasks, meetings, cases and documents from mobile devices. WorkZone Mobile runs on both iOS and Android platforms. For an overview of which features are supported on which platform, see [WorkZone Mobile feature overview](#).

For an overview of what users can do with WorkZone Mobile, see [Getting started with WorkZone Mobile](#) in the WorkZone Mobile User Guide.

4. WorkZone Mobile feature overview

The table below provides an overview of the WorkZone Mobile features that are available on each platform.

Important: Please note that features marked by an asterisk (*) are currently not supported by WorkZone for Citrix XenMobile. Features marked by two asterisks (**) are currently not supported by WorkZone for Microsoft Intune and Citrix XenMobile.

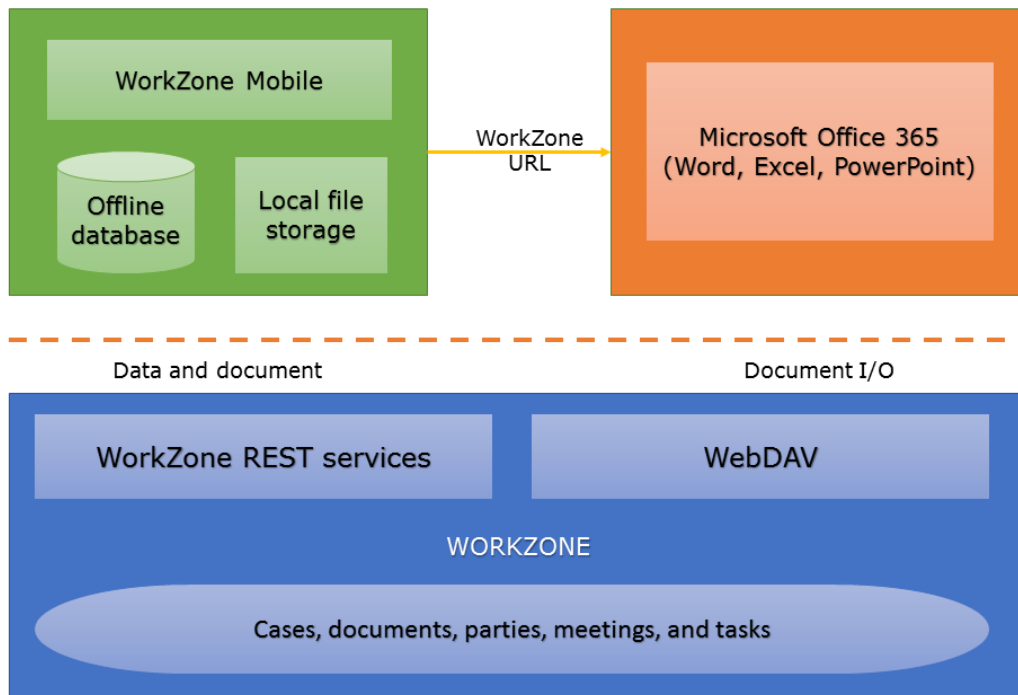
| | iOS | Android |
|-------------------------------------|-----|---------|
| Authentication | | |
| NTLM | X | X |
| OAuth | X | X |
| Basic | X | X |
| Task module | | |
| Task list | X | X |
| Task list sorting | X | X |
| Task detail view | X | X |
| Task ranking | X | X |
| Task – edit content | X | X |
| Task – preview document | X | X |
| Task – edit documents in PDF format | X | X |
| Task – view task as a PDF | X | – |
| Task – edit documents Office 365 * | X | – |
| Meeting module | | |

| | iOS | Android |
|--|-----|---------|
| Meeting list | X | X |
| Meeting list filtering | X | X |
| Meeting detail view | X | X |
| Meeting – preview document | X | X |
| Meeting – edit document in PDF format | X | X |
| Meeting – edit document in Office 365 * | X | – |
| Meeting - annotate document copies | X | X |
| Chat module | | |
| View existing chats | X | X |
| Reply to existing chats | X | X |
| Create new chats for existing tasks | X | X |
| Add or remove chat participants | X | X |
| Preview chat documents | X | X |
| View chat documents metadata | X | X |
| Browsing WorkZone documents from Office | | |
| Open and edit WorkZone documents from Office 365 * | X | X |
| Settings module | | |
| Settings module | X | X |
| URL in device settings (without MDM) | X | – |
| Notifications | | |

| | iOS | Android |
|---|-----|---------|
| Notifications * | X | - |
| MDM/MAM Support | | |
| Device Wide VPN | X | X |
| Citrix XenMobile - Micro VPN | X | - |
| Microsoft - Enterprise Mobility Suite | X | X |
| MDM settings on device (Server, redirect URI, client ID, and user name) | X | - |
| Password change | | |
| Support for password change at expiration ** | X | X |
| Help module | | |
| Online Help | X | X |

5. Architecture

The drawing below illustrates how WorkZone Mobile interacts with WorkZone and Microsoft Office 365.



- **WorkZone** is the back-end case and document management system. WorkZone stores and manages data on cases, documents, parties, meetings, and tasks. The data is exposed through standard REST services and WebDAV.
- **WorkZone Mobile** is a client. It fetches data through the WorkZone REST services and stores current meetings, tasks, and their related documents locally on the device for improved performance and offline scenarios. Data and documents that are no longer relevant are removed automatically from the app storage. WorkZone Mobile interacts with other apps and allows scenarios for copying documents to other apps, and most importantly it supports scenarios for editing documents directly from Office 365. The editing is done through parsing a WebDAV URL to Word, Excel, or PowerPoint.
- **Microsoft Office 365 – Office** is used for mobile document editing of WorkZone documents. This is done using direct access to WorkZone WebDAV services. Office

365 gets the WebDAV URL from WorkZone Mobile, and then Office 365 and WorkZone WebDAV services handle the document I/O (check-out, save, check-in). Note that only Office formats supported by Office 365 mobile apps work.

6. Security considerations

As most organizations apply WorkZone Mobile to scenarios for documents of high security and confidentiality, it is very important to understand the level of security in the APP and the surrounding infrastructure.

- **Authentication** – WorkZone Mobile supports authentication using OAuth (Azure ADFS), NTLM (Windows Integrated), and Basic authentication. The recommended setup is either OAuth or NTLM depending on the network setup.
- **Authorization** – The WorkZone back-end ensures correct access to resources for the users that are logged in. See [Register security](#) in the WorkZone Configuration Management Online Help.
- **Network transport** – HTTP and HTTPS are supported. It is recommended to use TLS 1.2. The highest level of TLS supported depends on the devices used in iOS the TLS version 1.2 for Android its TLS version 1.2.
- **Data security** – The WorkZone Mobile database and file storage is protected by the security on the device, both iOS and Android. Please refer to [iOS Security](#) guidelines and [Android Security](#) guidelines. It is important that a device runs with the correct security configuration enforced by a Mobile Device Management (MDM) system.
- **Logging** – All user actions are logged in the WorkZone Mobile back-end. See [Use logs and deletion logs](#) for more about the use logs and deletion logs in the WorkZone Operations Guide.
- **Multifactor authentication** - Multifactor authentication can be enabled in the MDM system.

7. Installing WorkZone Mobile

Prerequisites:

- WorkZone PDF with policies must be installed. WorkZone Mobile uses the WorkZone PDF Crawler module of WorkZone PDF to open documents in PDF format in the document viewer.

If you do not install WorkZone PDF Crawler, documents will open in Quick Look.

See the [WorkZone Installation Guide](#) for information about installing WorkZone PDF and the WorkZone PDF Crawler module.

- WorkZone 365 or WorkZone for Office must be installed, if you want to view on your mobile device your WorkZone meetings created in Outlook using WorkZone 365 or WorkZone for Office. See [Install WorkZone 365](#) and [Install WorkZone for Office](#) instructions in the WorkZone Installation Guide.

Install WorkZone Mobile

WorkZone Mobile must be installed through a mobile device management (MDM) system. An MDM system manages an organization's mobile devices from a central place. It handles deployment of apps, security, and monitoring of mobile devices used by the organization. Examples of MDM systems are Microsoft Intune and Citrix ZenMobile.

8. Microsoft Intune

You can use Microsoft Intune to get the following solutions:

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)

The Microsoft Intune solution is relevant if you have a Microsoft infrastructure strategy. It is a component of:

- Microsoft's Enterprise Mobility Suite + Security (EMS) suite
- Microsoft Office 365 Enterprise.

WorkZone is designed to integrate with other parts of the EMS platform, for example, Azure Active Directory or Azure Information Protection.

Tip: For an overview of Intune, see [Microsoft Intune](#).

Before you begin

Before you begin, please check the [WorkZone Mobile requirements to Microsoft Enterprise Mobility Suite infrastructure](#).

Microsoft Office 365 is required, if you want to edit documents using WorkZone Mobile.

Configure WorkZone Mobile in Microsoft Azure Portal

When the requirements to the infrastructure are fulfilled, you can move on to setting up and configuring WorkZone Mobile in Microsoft Azure Portal.

When you have completed the configuration steps below, you have set up a two-factor authentication.

- The first factor is that only the selected user groups or users in Azure Active Directory are able to authenticate.

- The second factor is that only users with mobile devices that are marked as "In compliance" by Intune MDM are authenticated.

The following step by step procedures guide you through the configuration in Microsoft Azure Portal:

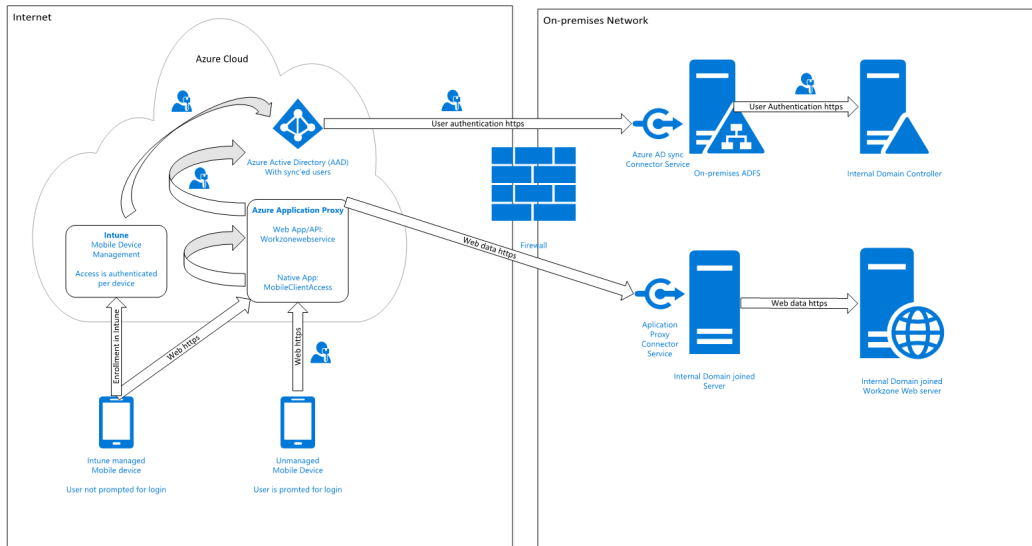
- [Publishing WorkZone Web services in Azure Application Proxy](#)
- [Creating a native API for WorkZone Mobile](#)
- [Publishing the WorkZone Mobile iOS app on Microsoft Intune \(Azure Portal\)](#)
- [Set up security and access from mobile devices](#)

8.1 WorkZone Mobile requirements to Microsoft Enterprise Mobility Suite infrastructure

Some configuration of an organization's infrastructure actions must take place to allow WorkZone Mobile access to on-premise WorkZone through Microsoft Enterprise Mobility Suite,

- [Synchronization of internal users to Azure Active Directory](#)
- [Azure Application Proxy with a Proxy Connector service installed](#)
- [Azure Web App publication of internal WorkZone services](#)
- [InternalWorkZone must run with HTTPS](#)
- [Intune deployment of WorkZone Mobile and Microsoft Office 365](#)

The diagram below shows a conceptual overview of the components in the infrastructure and how they are set up to support WorkZone Mobile with Microsoft Enterprise Mobility Suite (EMS). The number of real servers, firewalls, load balancers, and so on varies depending on how the environment is set up for a specific organization.



Synchronization of internal users to Azure Active Directory

You can do this in several different ways but to be able to use **Multifactor Authentication**¹, and thereby also conditional access, the only supported solution is to federate your internal domain using an on-premises **ADFS**² solution. This means that user login requests are forwarded to an internal ADFS service. Furthermore, it means that there are no passwords or password hashes in Azure. This is also the only solution that offers users the full single sign-on experience across internal systems, for example Microsoft Office 365 apps.

Azure Application Proxy with a Proxy Connector service installed

Azure Application Proxy pre-authenticates users in Azure Active Directory and provides access to underlying applications, in this case the internal WorkZone web service. A Proxy Connector service is installed on an internal server, which is in the same domain as the resources that are to be exposed, in this case the internal WorkZone web server.

¹Multi-factor authentication (MFA) is an authentication method that requires the use of at least two verification methods at user login, for example user name and password and a client certificate.

²Active Directory Federation Services

When the Azure Application Proxy service approves a request, it connects to the internal Proxy Connector, and requests it to access the internal resource (the WorkZone web server) on behalf of the current user, and send data back to the user/device on the other side of the Azure Application Proxy service.

Azure Web App publication of internal WorkZone services

The internal WorkZone web site must be published using Azure Application Proxy as a Web App/API type, so that it can be accessed externally with the same URL as the internal clients use on the domain. Furthermore, it requires that WorkZone is set up to use the HTTPS.

You set it up so that it is required that users are pre-approved with Azure Active Directory before they get access to the internal resources. As a second factor, besides user name and password, you can add a so-called Conditional Access Policy in Azure that only allows access if the user uses a device, which is managed by Intune. This means that you can use the actual device as the second factor.

It is also possible to use other built-in two-factor features in Azure Active Directory, for example sms code or voice call. This will, however, add an extra step to the user's login process.

InternalWorkZone must run with HTTPS

To publish a web service using Azure Application Proxy, HTTPS is required and as WorkZone does not support HTTPS off-loading, the underlying WorkZone server must also use HTTPS.

Flexible management of security

Because you use Azure Active Directory, you also have access to all the options for managing access. When Microsoft releases new features, you will also be able to use these features to manage the access to the WorkZone Mobile app.

Intune deployment of WorkZone Mobile and Microsoft Office 365

To get the full benefit of WorkZone Mobile, it must be deployed along with Office 365, which offers the possibility to edit Office documents.

8.2 Create a group of WorkZone users

Create a group of users to provide them access to the WorkZone mobile app.

1. Go to **Azure Active Directory** and click **Groups**.
2. Click **+ New group**.
3. Specify the following parameters:
 - **Group type** – Select *Security*.
 - **Group name** – Type *EMS_Licensed_Users*.
 - **Membership type** – Select *Assigned*.
4. Click **Create**.
5. Go to the newly created group and click **Members**.
6. Click **+ Add members** and specify users whom you want to add to the group.
7. Click **Select**.

8.3 Publishing WorkZone Web services in Azure Application Proxy

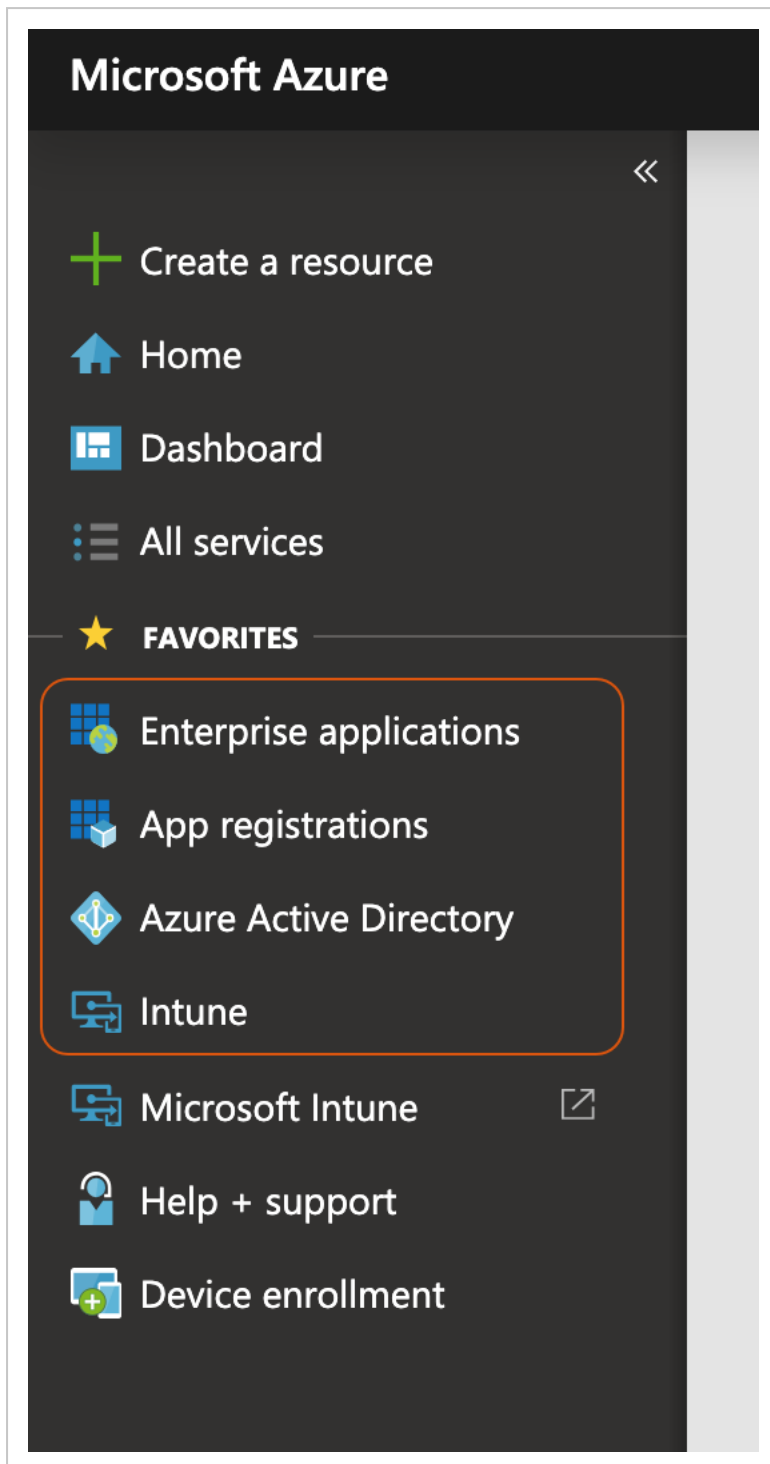
Prerequisites:

WorkZone Mobile 2021.0

- The Azure Application Proxy is set up with an internal Proxy service.
- The necessary rights are set up.
- The internal on-premises domain is synced with the Azure Active Directory.
- The certificate for the external URL in place.

Log in to the [Microsoft Azure portal](#).

The example shows the most frequently used Azure features.



Register the WorkZone Mobile app

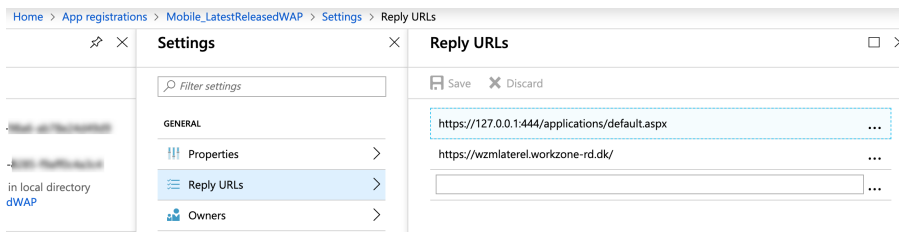
1. Go to the **Azure Active Directory** tab.
2. Click **App registrations**.

3. On the **App registration** page, click **New application registration**.
4. Enter a name for the WorkZone Mobile app.
5. Select **Web app / API** in the **Application type** field.
6. Enter the URL of WorkZone Mobile in the **Sign-on URL** field. This is the URL of the server. Users use it to sign in and use WorkZone Mobile.

The 'Create' dialog box contains the following fields:

- Name:** Mobile_LatestReleasedWAP
- Application type:** Web app / API
- Sign-on URL:** https://wzmlaterel.workzone-rd.dk/

Tip: See where to find the correct URL of the server:



7. Click **Create**.

Enable users to sign in

1. Click **Enterprise applications > All applications**.
2. Select the WorkZone Mobile app with the name you specified above.
3. Click **Properties**.

- Make sure to enable the **Enabled for users to sign-in?** and **User assignment required?** settings.

WorkzoneAzureWAP (connectzone.dk) - Properties
Enterprise Application

Save Discard

Enabled for users to sign-in? Yes No

Name

Publisher

Homepage URL

Logo

User access URL

Application ID

Object ID

User assignment required? Yes No

- Click **Save**.
- Click **Users and groups**.
- Click **Add user** to assign users or groups of users that will have access to WorkZone Mobile.

Home > App registrations > Mobile_LatestReleasedWAP > Mobile_LatestReleasedWAP - Users and groups

Mobile_LatestReleasedWAP - Users and groups
Enterprise Application

+ Add user Edit Remove Update Credentials Columns

The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

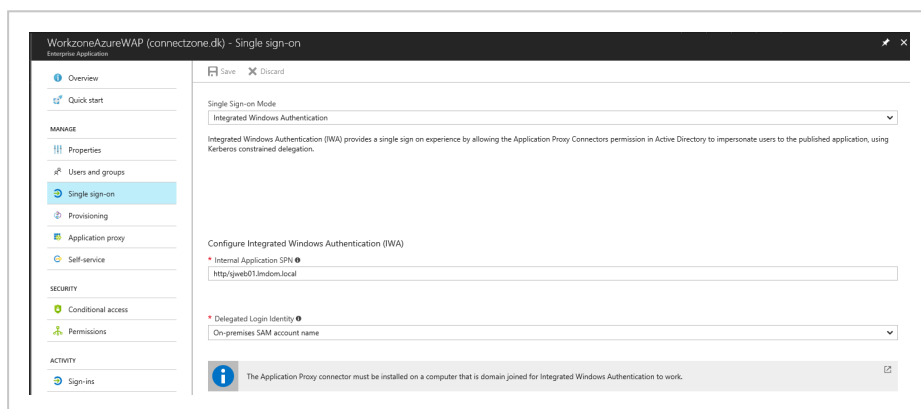
First 100 shown, to search all users & groups, enter a display name.

| DISPLAY NAME | OBJECT TYPE | ROLE ASSIGNED |
|-----------------------|-------------|----------------|
| EM EMS_Licensed_Users | Group | Default Access |

- Click **Single sign-on**.

9. Specify the following settings:

- Select **Integrated Windows Authentication** in the **User Sign-on Mode** field.
- Enter the **SPN**¹ of the internal WorkZone Mobile app in the **Internal Application SPN** field.
- Select **On-premises SAM**² **account name** in the **Delegated Login Identity** field.



9. Click **Save**.

10. Click **Application proxy**.

11. Make sure to enable the following settings (**1**):

- Enter the internal URL to access WorkZone Mobile from inside your network in the **Internal Url** field.

The URL must match the external URL.

- Enter the external URL to access WorkZone Mobile from outside your network in the **External Url** field.

The URL must match the internal URL.

¹Service Principal Name

²Security Application Manager

- Select **Azure Active Directory** in the **Pre Authentication** field.
- In the Connector Group, select LatestReleased.

Note: It is highly recommended to add at least three connectors. **(2)**

- Under **Translate URLs in**, disable the settings **(3)**:
 - **Headers**
 - **Application Body**

Mobile_LatestReleasedWAP - Application proxy
Enterprise Application

« Save Discard

Test Application
Click here to verify application configuration.

Basic Settings

1 * Internal Url

External Url

Pre Authentication

2 Connector Group

We recommend at least two active connectors in each group. Click here to download a new connector or manage your connector groups.

Additional Settings

Backend Application Timeout

Use HTTP-Only Cookie

Use Secure Cookie

Use Persistent Cookie

3 **Translate URLs In**

Headers

Application Body

4 **Certificate**
Click here to view your certificate

To access your application using a custom domain you must configure a CNAME entry in your DNS provider which points 'wzmlaterel.workzone-rd.dk' to 'wzmlaterel-wzmworkzonerd.msappproxy.net'

12. Select a certificate for the external URL **(4)**. Under **Certificate**, click **Click here to view your certificate** to view or upload the certificate.
13. Click **Save**.

8.4 Creating a native API for WorkZone Mobile

Log in to the [Microsoft Azure portal](#).

Register the native API

1. Click **App registrations**. It must be the same place as your WorkZone web app publication is created.
2. On the **App registration** page, click **New application registration**.
3. Enter a name for the WorkZone Mobile app, for example, WorkZoneMobileNative.
4. Select **Native** in the **Application type** field.
5. Enter the URL of your WorkZone web app publication in the **Redirect URI** field.

Create

* Name ⓘ

Mobile_LatestReleasedNative ✓

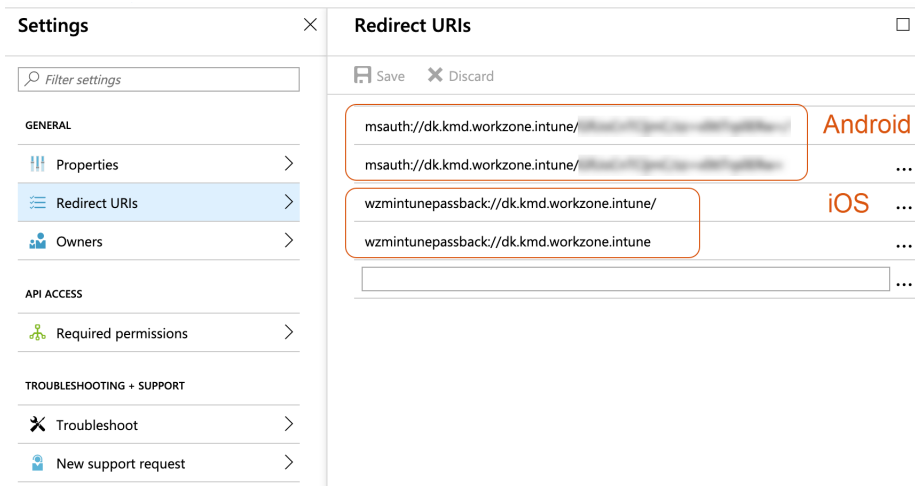
Application type ⓘ

Native ✓

* Redirect URI ⓘ

wzmintunepassback://dk.kmd.workzone.intune ✓

Tip: To avoid issues with the third-party applications integrity, it is recommended to add another Redirect URI with slash in the end.

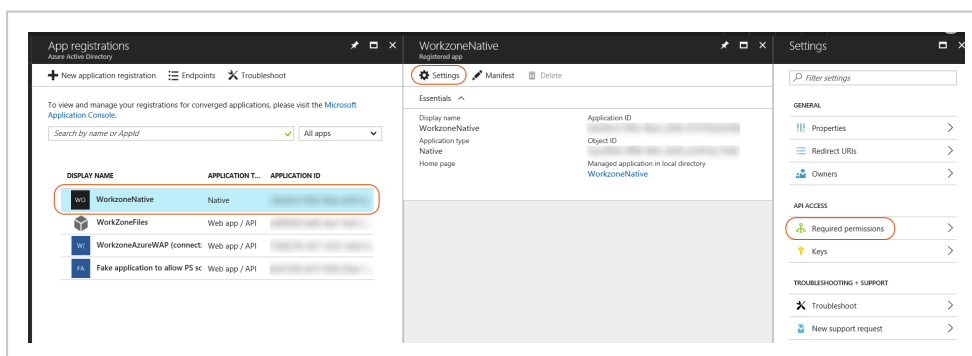


Notes:

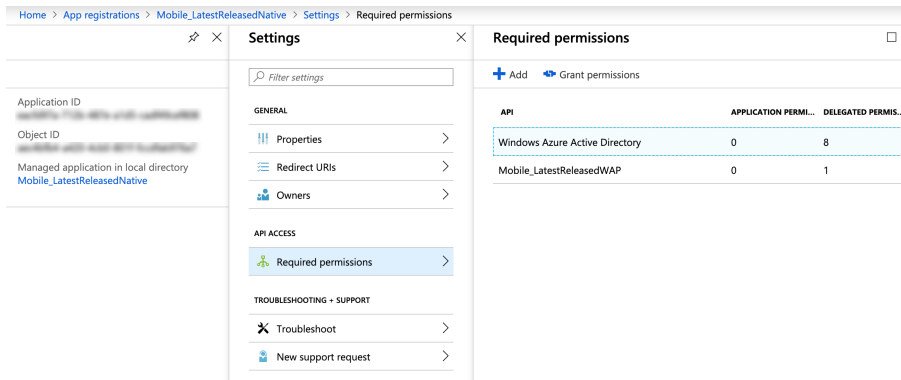
- According to vendors limitations, each platforms (iOS and Android) must have specific URI format. Please follow the format illustrated on the picture.
- For the Android platform, use [Android Debug Bridge](#).

Add permissions

1. Select the app you just created and click **Settings > Required permissions**.

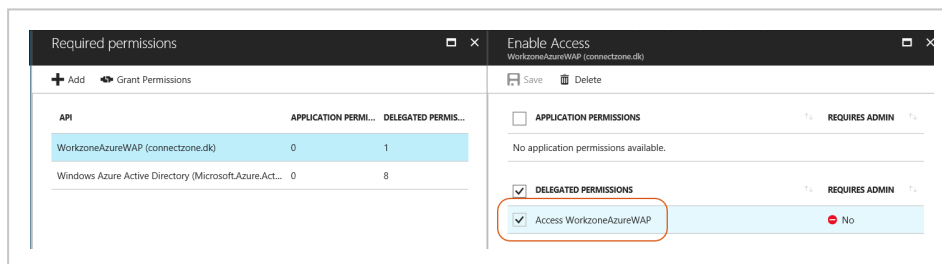


2. On the **Required permissions** page, click **Add > Select an API**.

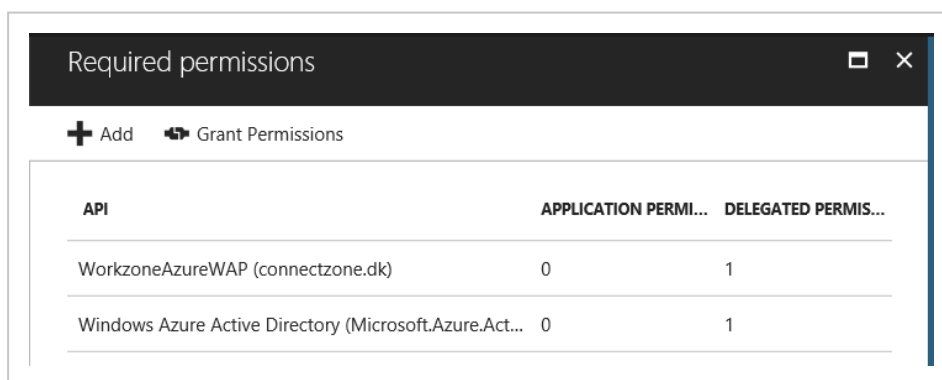


Note: If you only see the Microsoft API, you need to type in the **Search** field, and then other results will be listed.

3. Select your published web app for WorkZone, and click the **Select** button.
4. On the **Enable access** page, select the **Access <Your published web app>**, click the **Select** button.



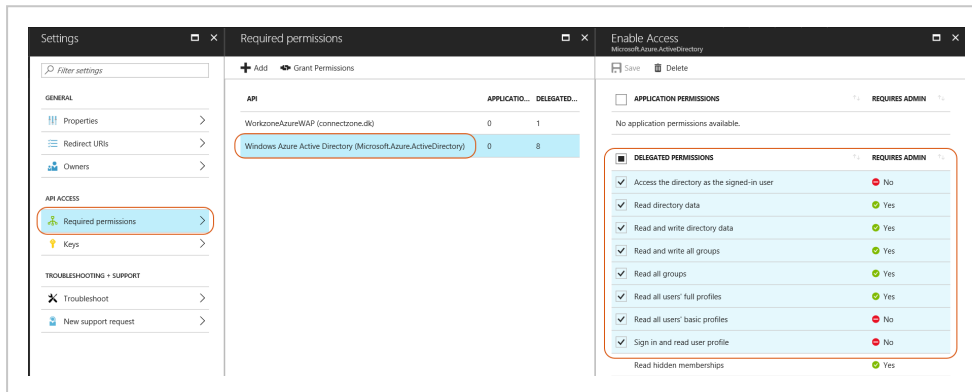
5. Click **Done**.



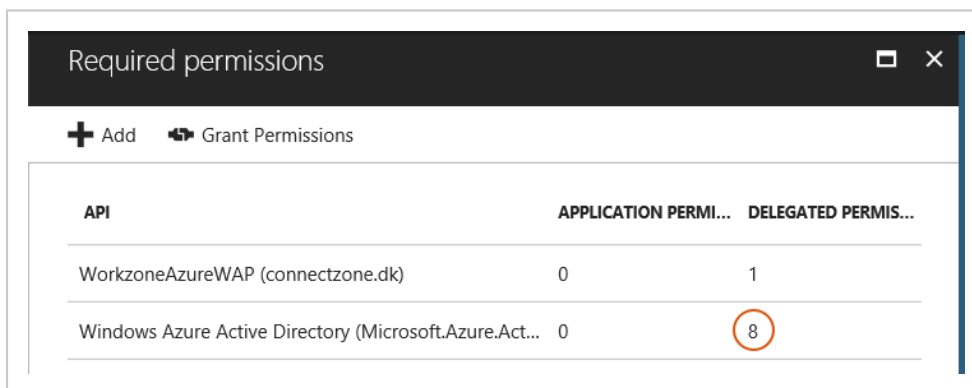
The next step is to add specific permissions to the Windows Azure Active Directory.

Add permissions to the Windows Azure Active Directory

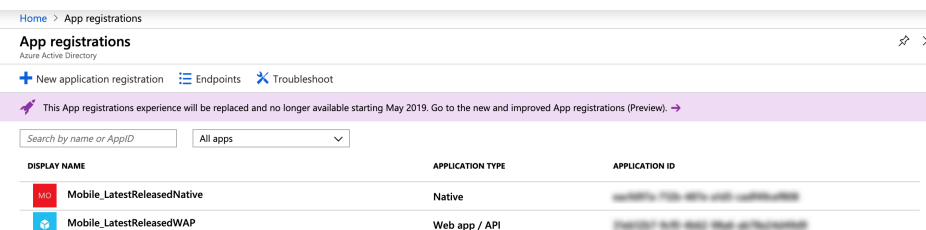
1. Select the app you just created and click **All settings** > **Required permissions**.
2. On the **Required permissions** page, click **Windows Azure Active Directory**.
3. Under **Delegated permissions**, select all the check boxes except the last one.



4. Click **Save**.



5. Click **Grant Permissions**. If prompted, click **Yes**, **OK**, or **Accept**.



8.5 Publishing the WorkZone Mobile iOS app on Microsoft Intune (Azure Portal)

Prerequisites:

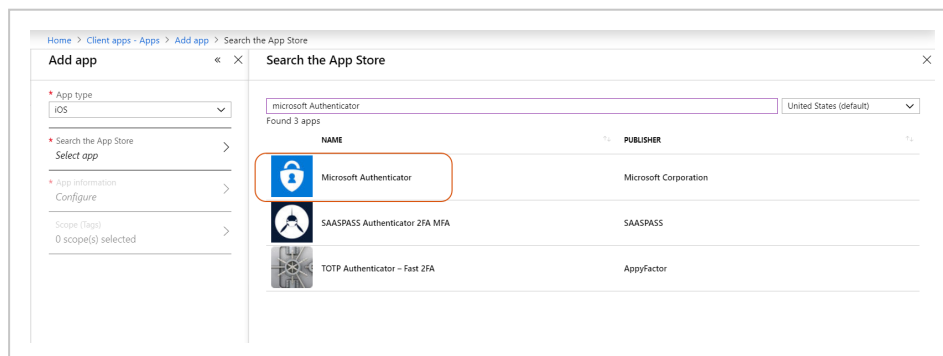
- Internal domain users are synced to Azure Active Directory and user groups with access to WorkZone Mobile exist.
- Conditional access policies are created. See [Set up security and access from mobile devices](#).
- Intune is set up so that mobile devices are managed and the devices are marked as "in compliance" by Intune.

Log in to the [Microsoft Azure portal](#).

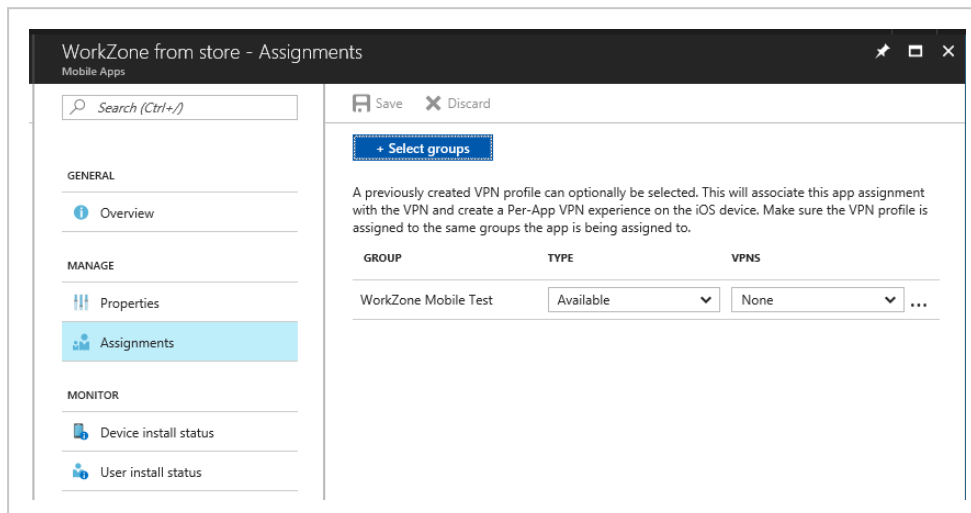
Add the Microsoft Authenticator app

Publish the Microsoft Authenticator app to make it available on the Company Portal. Users can then easily download it and use to log in to WorkZone.

1. Go to **Microsoft Intune**.
2. Click **Client apps > Apps**.
3. Click **Add**. In the **App type** field, select **Store app > iOS**.
4. Click **Search the App Store**.
5. Enter **Microsoft Authenticator** in the search field and select **Microsoft Authenticator** among the available options.



6. Click **Select** and then click **Add**.
7. Click **Assignments**, and select the Azure Active Directory groups or users who should get WorkZone Mobile in their Company Portal.

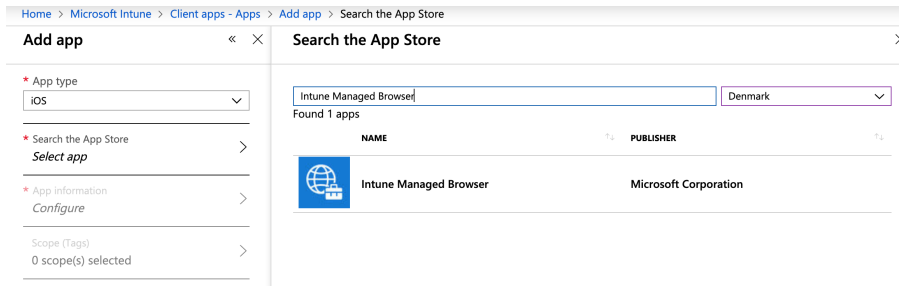


8. Click **Save**.

Add the Intune Managed Browser app and the Microsoft Office apps

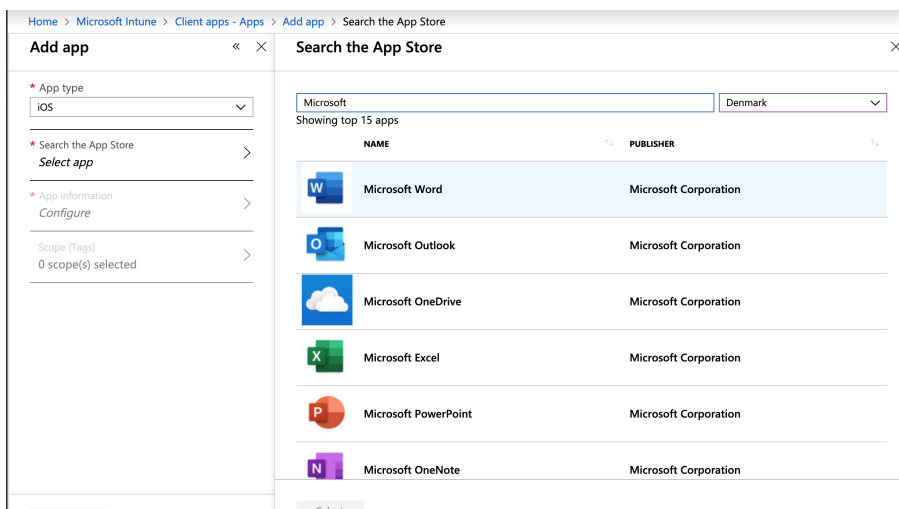
Optionally, you can add the **Intune Managed Browser** app and a number of Microsoft Office apps to improve user experience with the WorkZone Mobile application.

1. Go to **Microsoft Intune**.
2. Click **Client apps > Apps**.
3. Click **Add**. In the **App type** field, select **Store app > iOS**.
4. Click **Search the App Store**.
5. Enter **Intune Managed Browser** in the search field and select the application.



6. Click **Select** and then click **Add**.

7. Enter **Microsoft** in the search field and select the applications that you want to add.

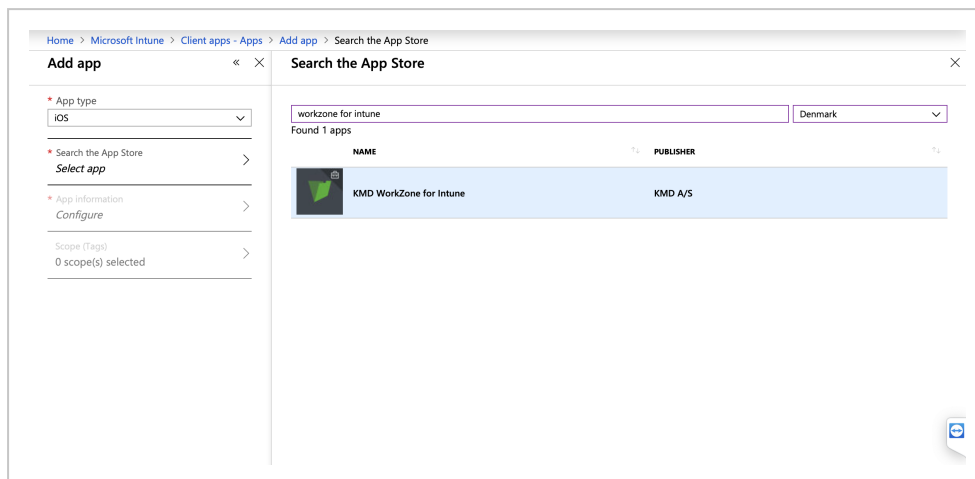


8. Click **Select** and then click **Add**.

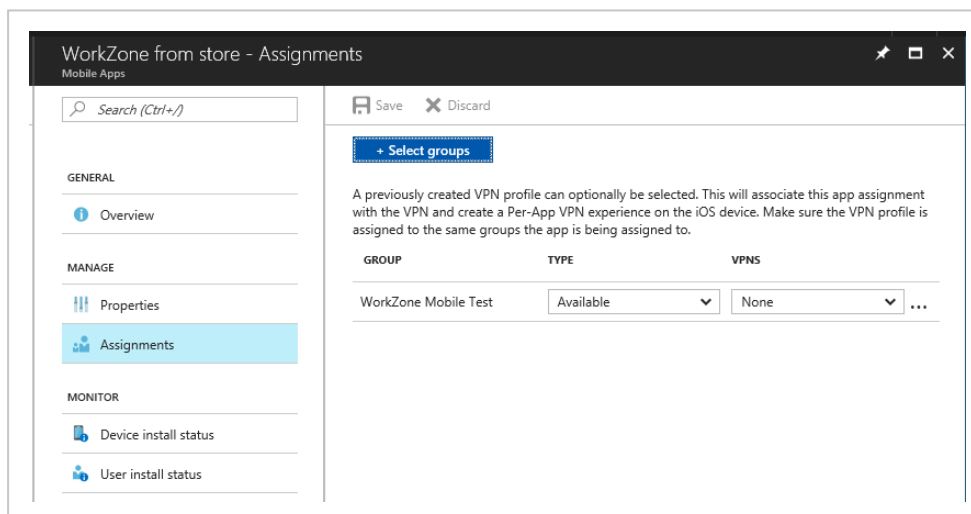
Add the WorkZone Mobile app

1. Go to **Microsoft Intune**.
2. Click **Client apps > Apps**.
3. Click **Add**. In the **App type** field, select **Store app > iOS**.
4. Click **Search the App Store**.
5. Select **Denmark** among countries and type "WorkZone for Intune" in the search field. Search for **WorkZone for Intune** and select **KMD WorkZone for**

Intune published by **KMD A/S**, and click **OK**.



6. Click **Select** and then click **Add**.
7. Click **Assignments**, and select the Azure Active Directory groups or users who should get WorkZone Mobile in their Company Portal.

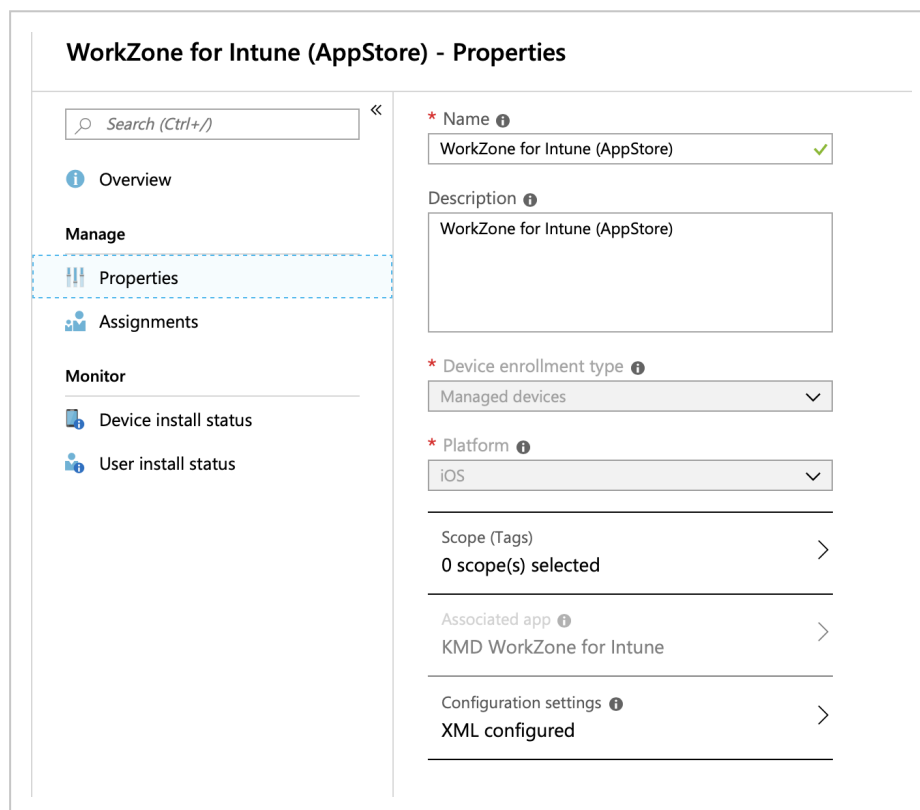


8. Click **Save**.

Create an App configuration policy for iOS

WorkZone Mobile supports pushing certain connection settings to the mobile devices through Intune. This is done by creating an app configuration policy and assign the policy to the app users.

1. In Intune, click **Client apps > App configuration policies**.
2. Click **Add**, and fill in the required information. See an example below.
 - Select **Managed devices** in the **Device enrollment type** field.
 - Select **iOS** in the **Platform** field.
 - Click **Associated app**, and select the WorkZone Mobile app that you just created.



3. Click **OK**.
4. Click **Configuration settings** and select **Enter XML data** in the **Configuration settings format** field.
5. Copy and paste the code below.

```
<dict>
  <key>mamserverurl</key>
  <string>[URL to your WorkZone server]</string>
```

```

<key>mamredirecturi</key>

<string>[Redirect URI of the native WorkZone app]</string>

<key>mamclientid</key>

<string>[ClientID]</string>

<key>mamuserprincipalname</key>

<string>{{userprincipalname}}</string>

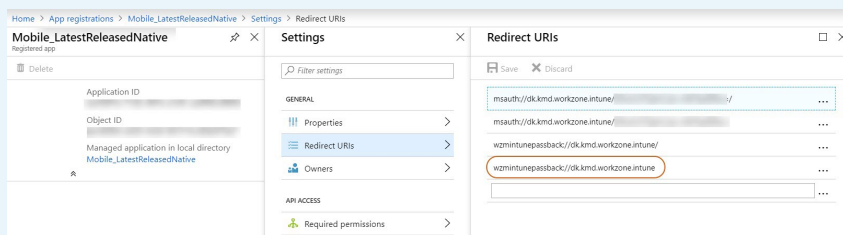
</dict>

```

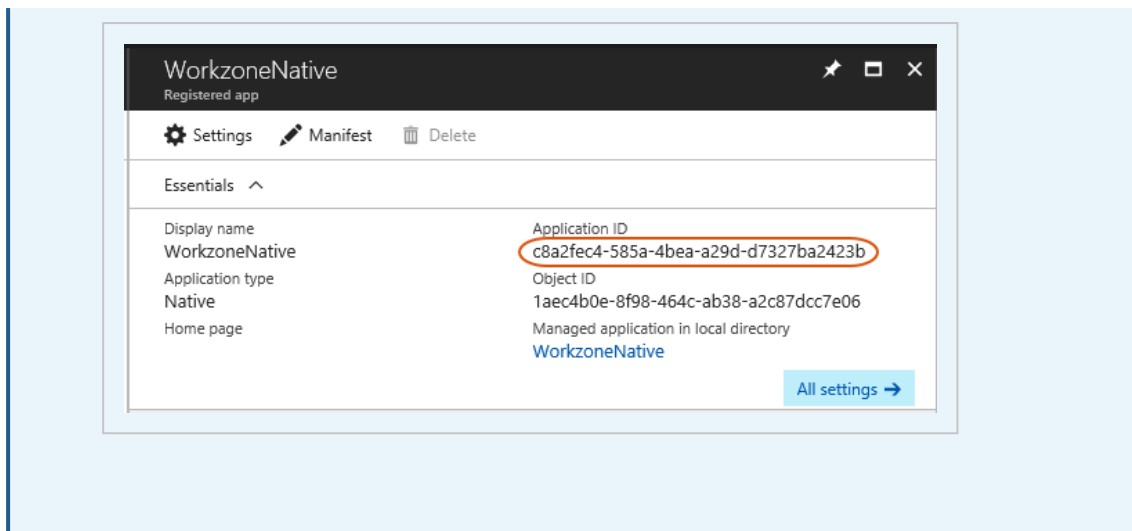
Where you need to replace the URLs and `ClientID` with the ones from your environment.

Tips:

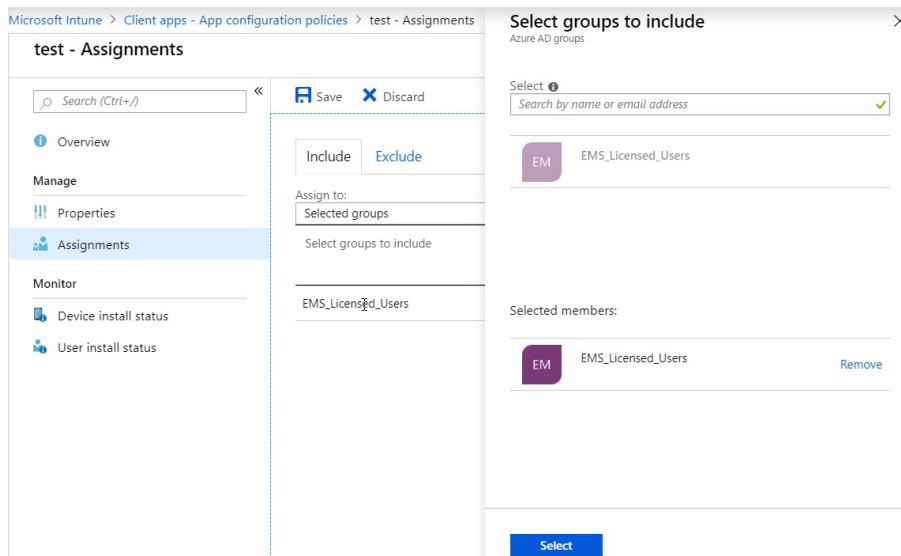
- It is recommended to copy the exact value of Redirect URI from the [Native API](#).



- You can find the `ClientID` under **Azure Active Directory > App registrations > [Name of your Workzone Mobile Native app]** where it is called **Application ID**.



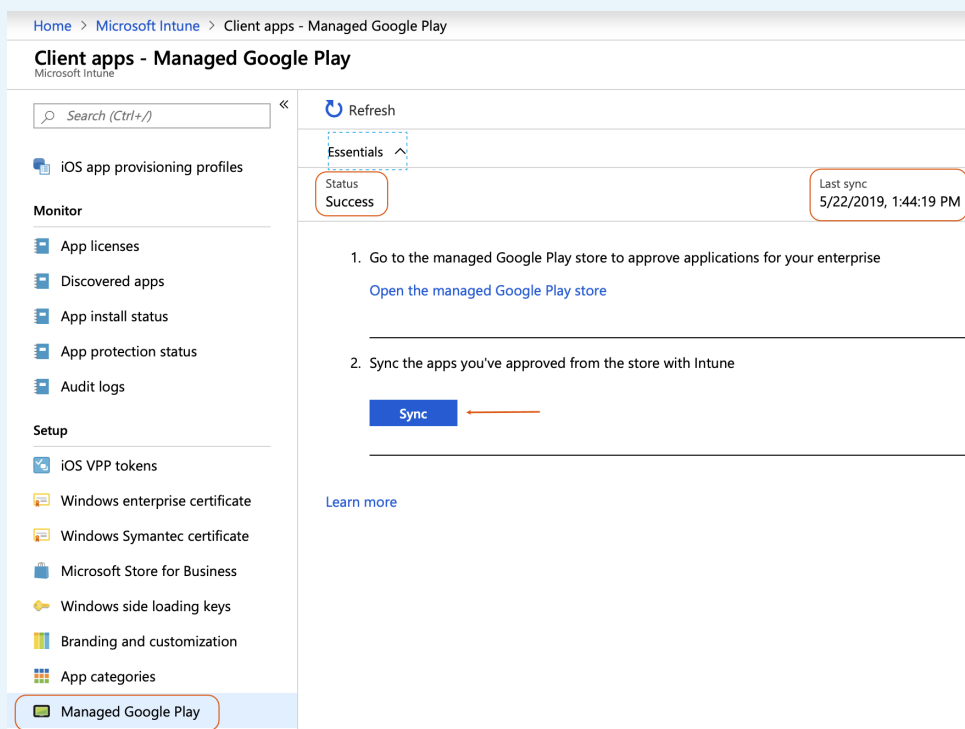
6. When you have completed the setup, click **OK**.
7. Click **Add** or **Save** to apply the policy.
8. Click **Assignments**. Select **Selected groups** in the **Assign to** list. Click **Select groups to include** and select *EMS_Licensed_Users*. Click **Select** and then **Save**.



8.6 Publishing the WorkZone Mobile Android app on Microsoft Intune (Azure Portal)

Prerequisites:

- Internal domain users are synced to Azure Active Directory and user groups with access to WorkZone Mobile exist.
- Conditional access policies are created. See [Set up security and access from mobile devices](#).
- Intune is set up so that mobile devices are managed and the devices are marked as "in compliance" by Intune.
- **Managed Google Play** account must be synchronized:

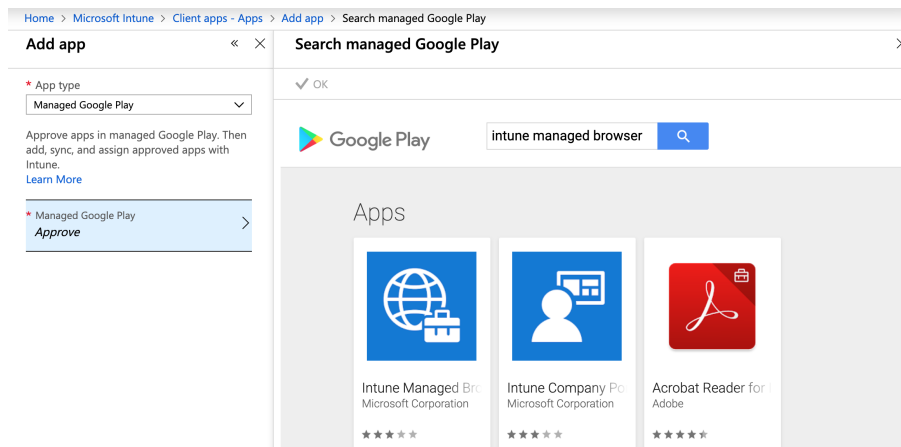


Log in to the [Microsoft Azure portal](#).

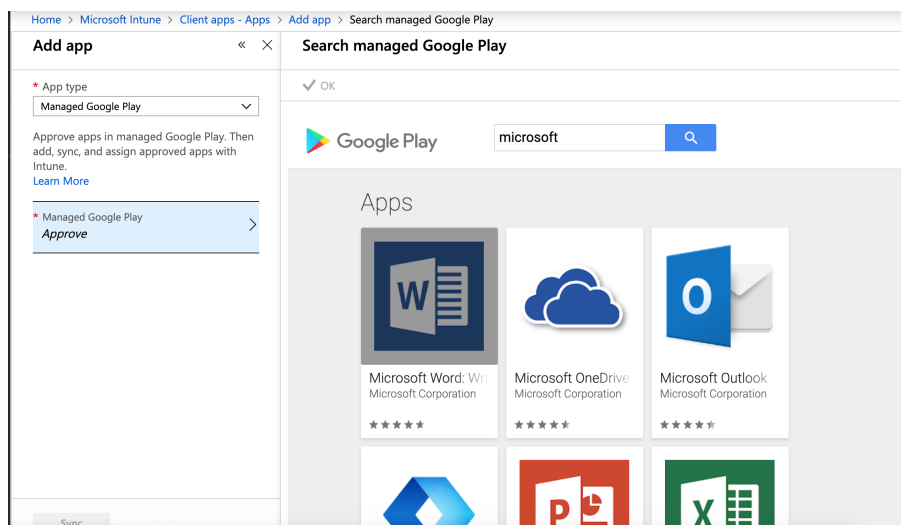
Add Microsoft Authenticator, Intune Managed Browser, and the Microsoft Office apps

Optionally, you can add the **Microsoft Authenticator** app, the **Intune Managed Browser** app, and a number of Microsoft Office apps to improve user experience with the WorkZone Mobile application.

1. Go to **Microsoft Intune**.
2. Click **Client apps > Apps**.
3. Click **Add**. In the **App type** field, select **Store app > Managed Google Play**.
4. Click **Managed Google Play / Approve** in the menu.
5. Enter **Microsoft Authenticator** in the search field and select **Microsoft Authenticator** among the available options.
6. Click **Select** and then click **Add**.
7. Enter **Intune Managed Browser** in the search field and select the application.



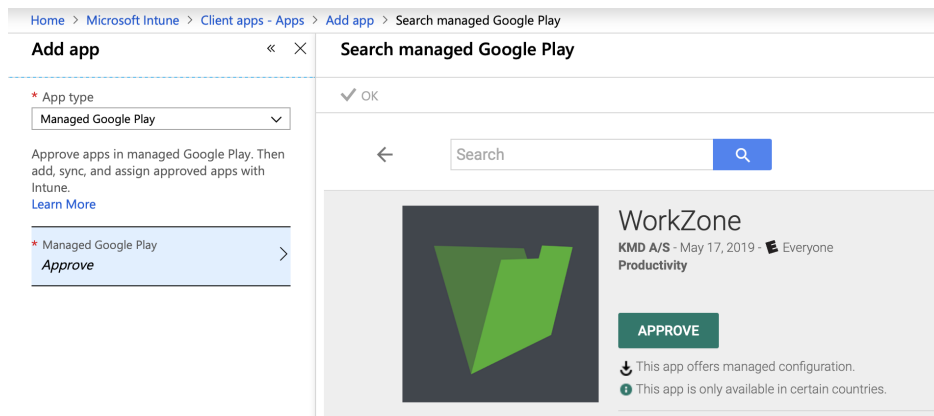
8. Click **Select** and then click **Add**.
9. Enter **Microsoft** in the search field and select the applications that you want to add.



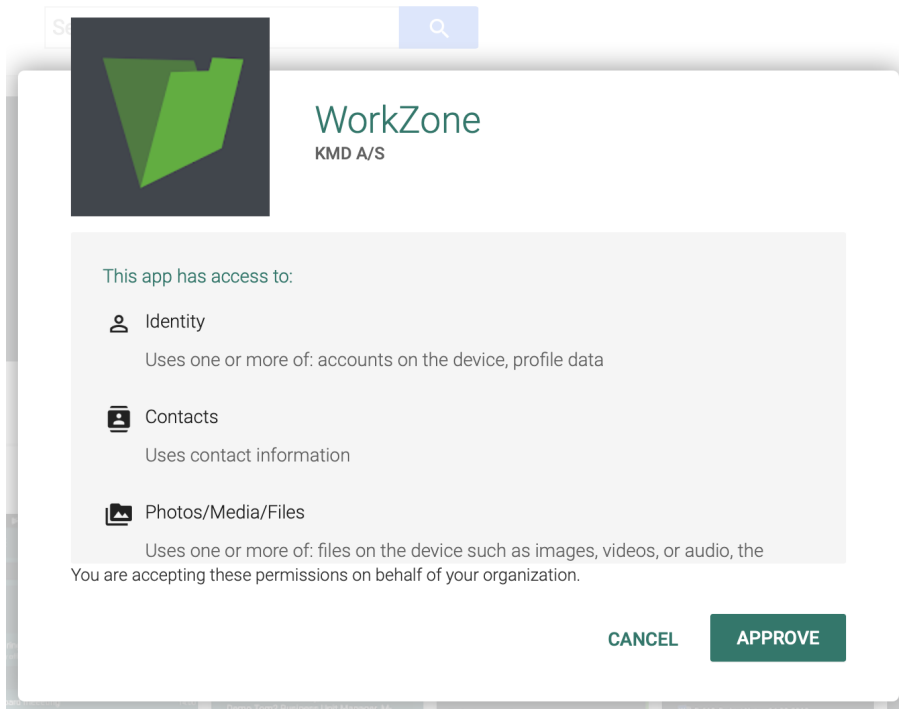
10. Click **Select** and then click **Add**.

Add the WorkZone Mobile app

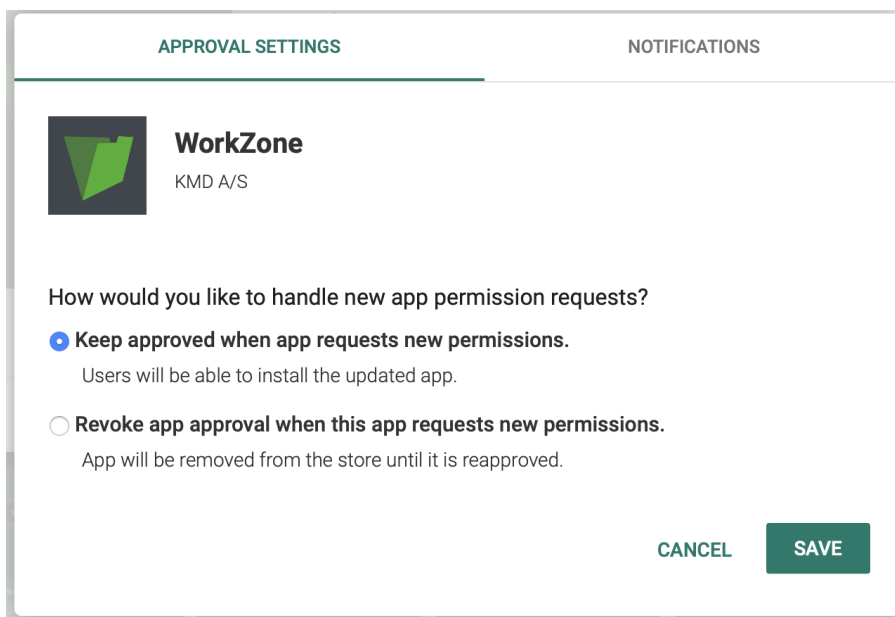
1. Go to **Microsoft Intune**.
2. Click **Client apps > Apps**.
3. Click **Add**. In the **App type** field, select **Store app > Managed Google Play**.
4. Click **Managed Google Play** in the menu.
5. Enter **WorkZone** in the search field and select **WorkZone** published by **KMD A/S**.
6. Click **Approve**.



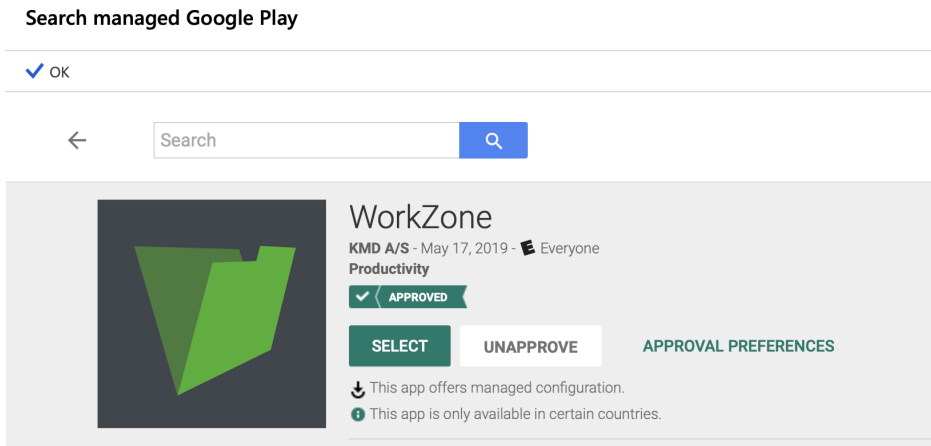
7. Click **Approve**.



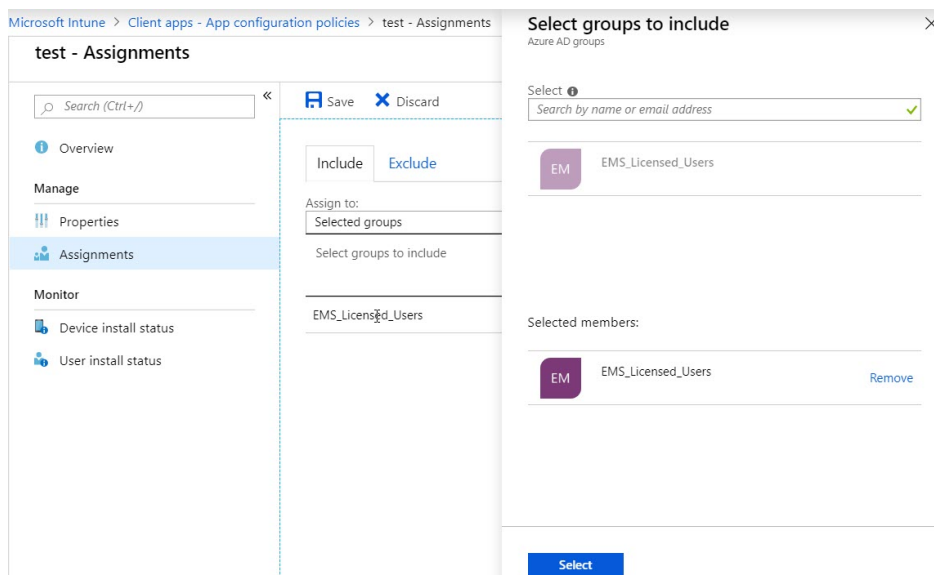
8. Select the following setting and click **Save**.



9. Click **OK**.



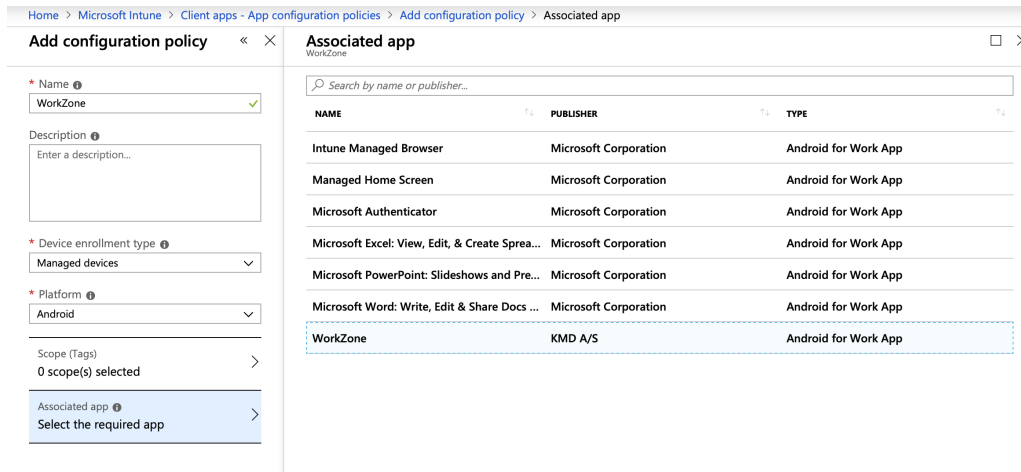
10. Click the **Sync** button.
11. Click **Assignments**. Select **Selected groups** in the **Assign to** list. Click **Select groups to include** and select *EMS_Licensed_Users*. Click **Select** and then **Save**.



Create an App configuration policy for Android

WorkZone Mobile supports pushing certain connection settings to the mobile devices through Intune. This is done by creating an app configuration policy and assigning the policy to the app users.

1. In Intune, click **Client apps > App configuration policies**.
2. Click **Add**, and fill in the required information (see an example below). In the **Associated app**, select the WorkZone. Click **OK**.



3. Click **Configuration settings** and select **Enter JSON data** in the **Configuration settings format** list. Adjust your data.

```
{
"kind": "androidenterprise#managedConfiguration",
"productId": "app:dk.kmd.workzone",
"managedProperty": [
{
"key": "mamserverurl",
"valueString": "[URL to your WorkZone server]"
},
{
"key": "mamredirecturi",
"valueString": "msauth://dk.kmd.workzone/XXXXXXXXXXXXXXXXXX"
},
{

```

```

"key": "mamclientid",

"valueString": "[ClientID]"

},

{

"key": "mamuserprincipalname",

"valueString": "{{userprincipalname}}"

}

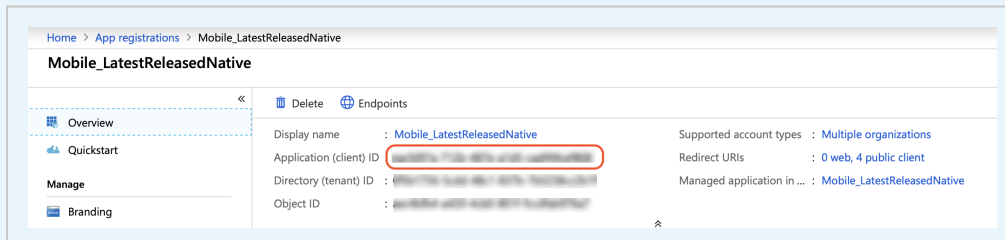
]

}

```

Tips:

- You can find the `ClientID` under **Azure Active Directory > App registrations > [Name of your Workzone Mobile Native app]** where it is called **Application (client) ID**.



- It is recommended to copy the exact value of the Redirect URI from the **Native API**.

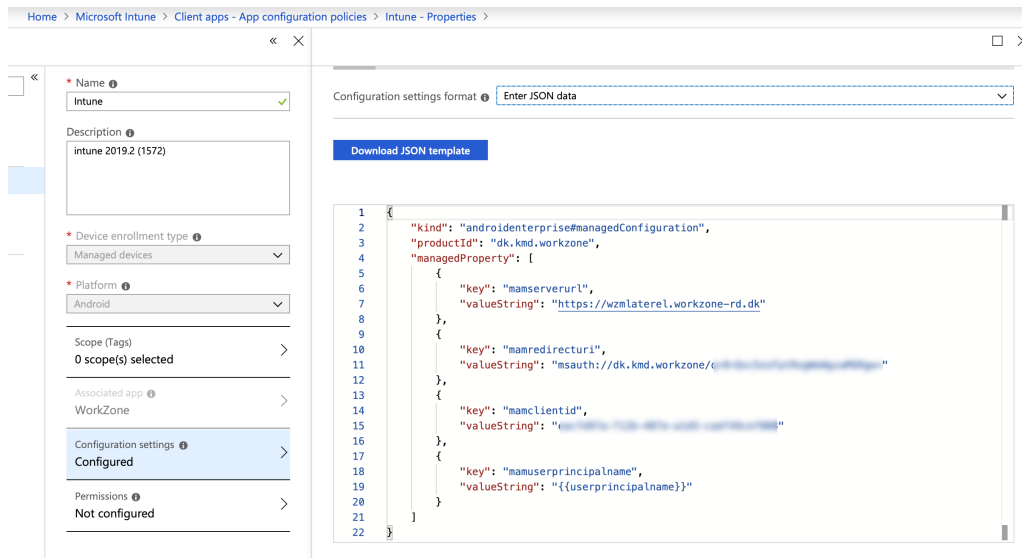
Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs.

[Learn more about adding support for web, mobile and desktop clients](#)

| TYPE | REDIRECT URI | |
|----------------------------------|---|--|
| Public client (mobile & desktop) | msauth://dk.kmd.workzone/[redacted] | |
| Public client (mobile & desktop) | msauth://dk.kmd.workzone/[redacted] | |
| Public client (mobile & desktop) | wzmintunepassback://dk.kmd.workzone.intune | |
| Public client (mobile & desktop) | wzmintunepassback://dk.kmd.workzone.intune/ | |

Example:



4. Click **OK**.
5. Click **Add**.
6. Click **Assignments**. Select **Selected groups** in the **Assign to** list. Click **Select groups to include** and select *EMS_Licensed_Users*. Click **Select** and then **Save**.

8.7 Set up security and access from mobile devices

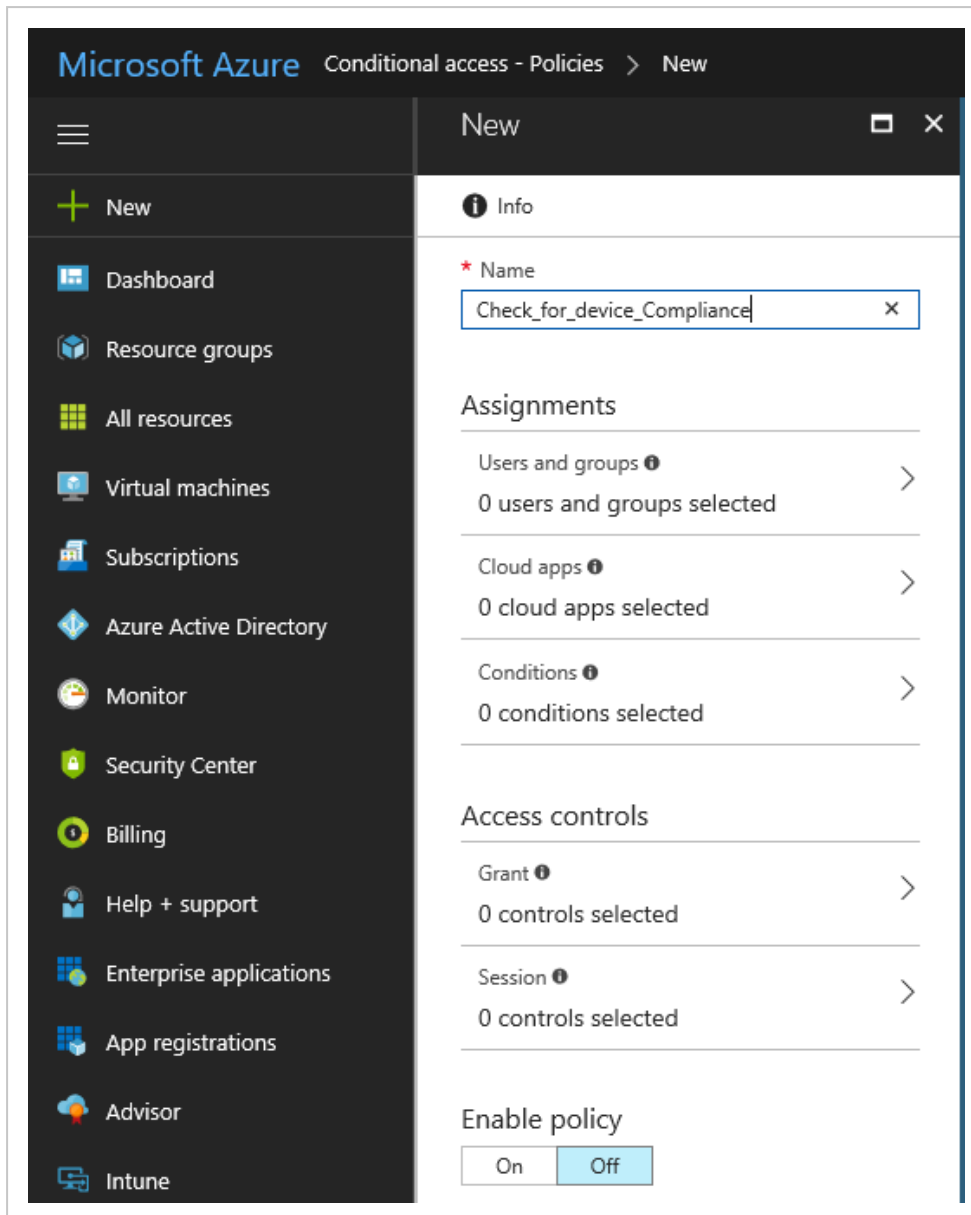
To secure the access to the WorkZone Mobile web services that are used by WorkZone Mobile, it is recommended to configure conditional access, which will only allow access from compliant mobile devices.

Prerequisites: Mobile devices are managed by Intune and compliance policies are configured and enabled on the devices.

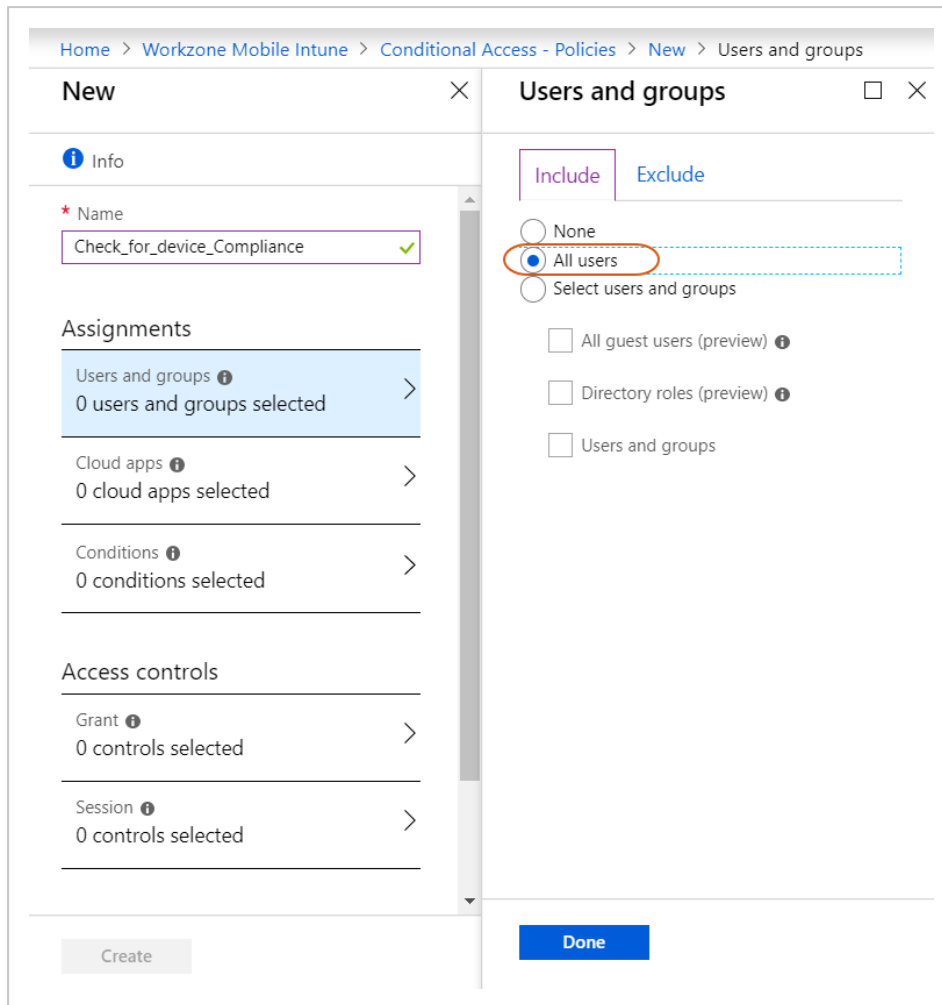
Log in to the [Microsoft Azure portal](#).

Create a new policy

1. Click **Azure Active Directory** on menu, or use search to find it easily.
2. Under **Security**, click **Conditional Access > New policy**.
3. Enter a name of the policy in the **Name** field. In the example below, the policy is named *Check_for_device_Compliance*.

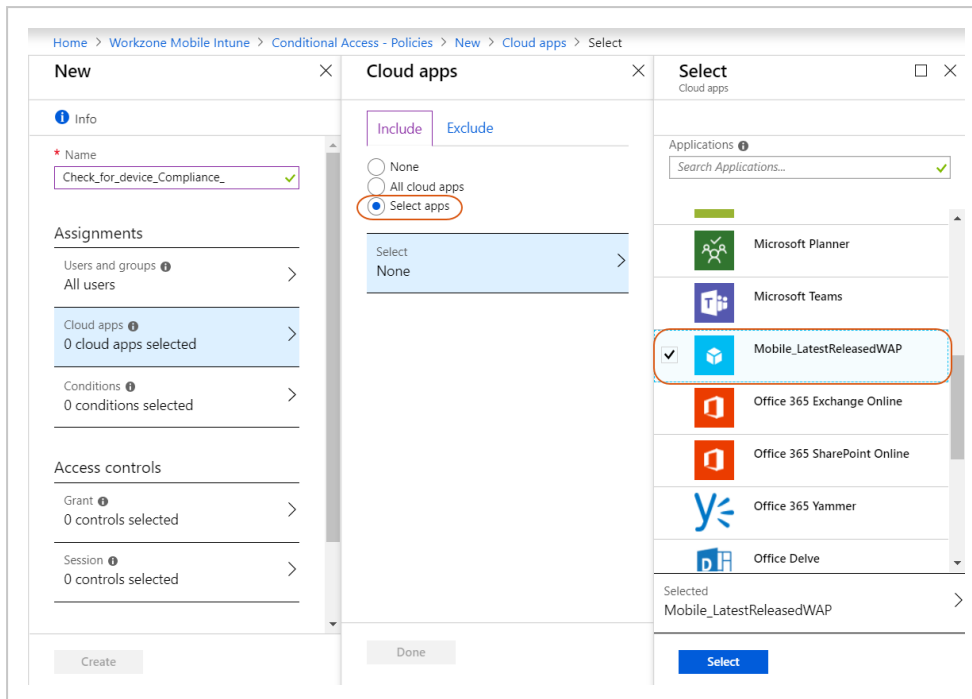


4. Under **Assignments**, click **Users and groups**. Select **All users** on the **Include** tab and click **Done**. This ensures that all users will be checked.

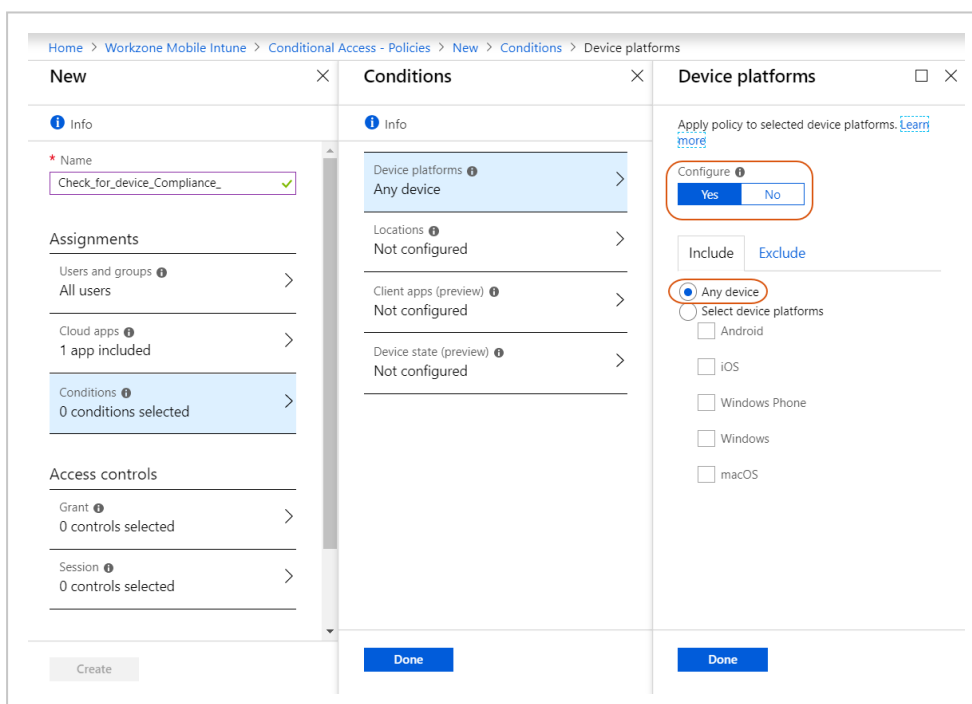


5. Click **Cloud apps**, and click **Select apps** on the **Include** tab.
6. Click **Select** to expand the list of applications. Select the WorkZone Mobile app that you [have created](#) earlier. Click the **Select** button and then click **Done**.

Tip: See how to [publish WorkZone Web services](#) in Azure Application Proxy.

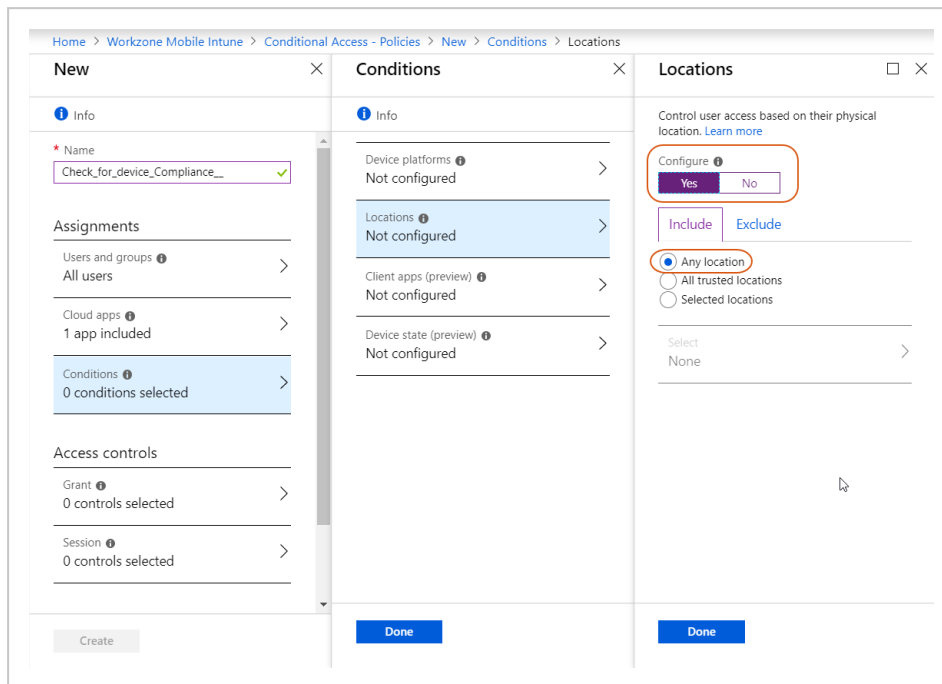


7. Click **Conditions** > **Device platforms**, and click **Yes** to enable **Configure**.
8. Select **Any device** and then **Done**. This ensures that all platforms will be checked.

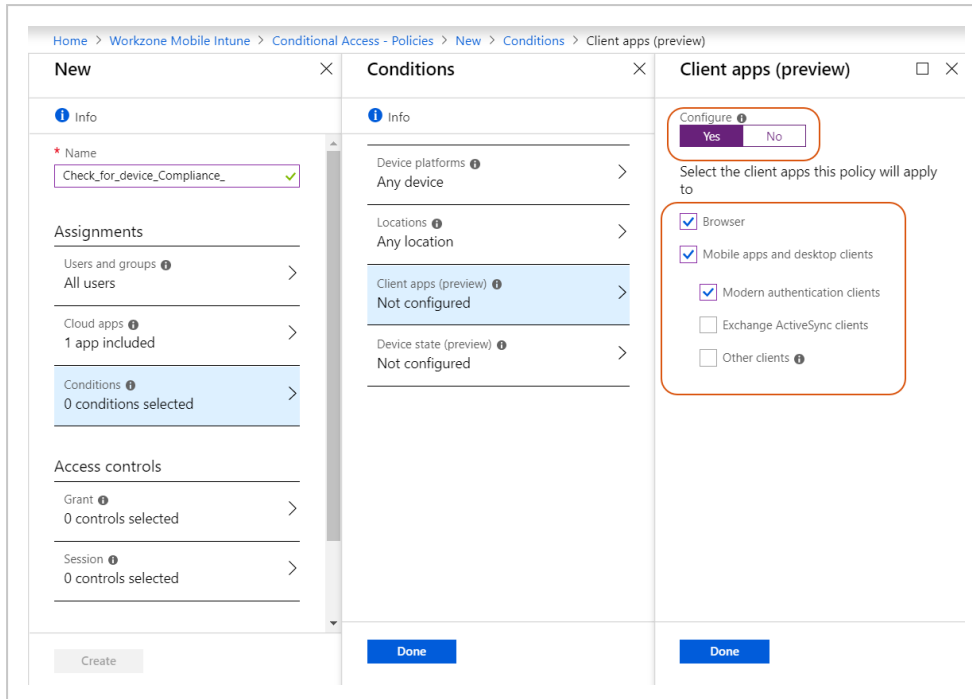


9. Click **Locations** and click **Yes** to enable **Configure**.

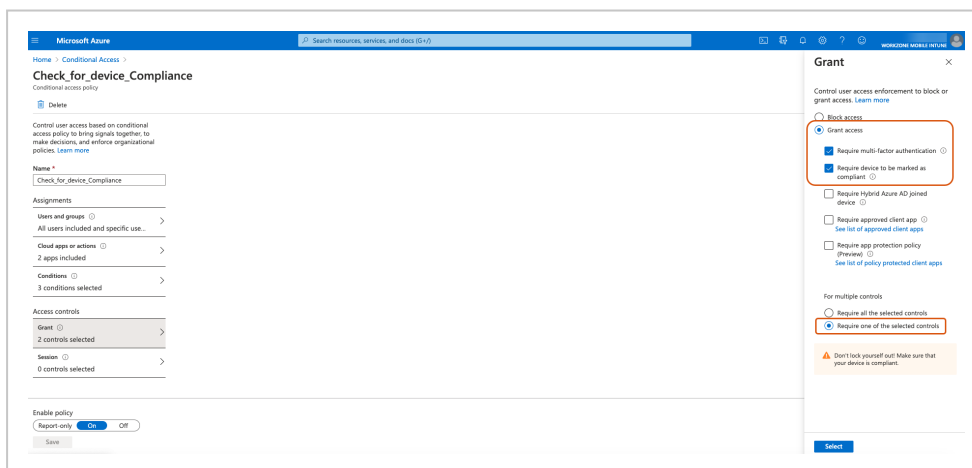
10. Select **Any location** on the **Include** tab and click **Done**. It ensures that all locations will be checked.



11. Click **Client apps**, and click **Yes** to enable **Configure**.
12. Select **Select client apps**, and then select the **Browser, Mobile apps and desktop clients**, and **Modern authentication clients** check boxes. Click **Done**.



13. Under **Access controls**, click **Grant** and then select **Grant access**.
14. Select the **Require multi-factor authentication** and **Require device to be marked as compliant** checkboxes. For multiple controls, select the **Require one of the selected controls** option. Click **Select**.



Tip: To use multi-factor authentication, you must first set it up on your mobile device and link to your account your mobile phone number or app token. See [Set up multi-factor authentication](#).

- Click **On** to enable the policy and then **Create**. The created policy now appears as **Enabled**.

| POLICY NAME | ENABLED | |
|---|---------|-----|
| Baseline policy: Require MFA for admins (Preview) | | ... |
| Check_for_device_Compliance | ✓ | ... |

Set up multi-factor authentication

- Go to <https://aka.ms/mfasetup>.
- On the **Additional security verification page**, under **Set up one or more of these options**, select the **Authentication phone** checkbox and enter your phone number to use for authentication.
- Select the **Authenticator app or Token** checkbox.

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. [View video to know how to secure your account](#)

what's your preferred option?
We'll use this verification option by default.

Notify me through app

how would you like to respond?
Set up one or more of these options. [Learn more](#)

Authentication phone

Office phone Extension

Alternate authentication phone

Authenticator app or Token

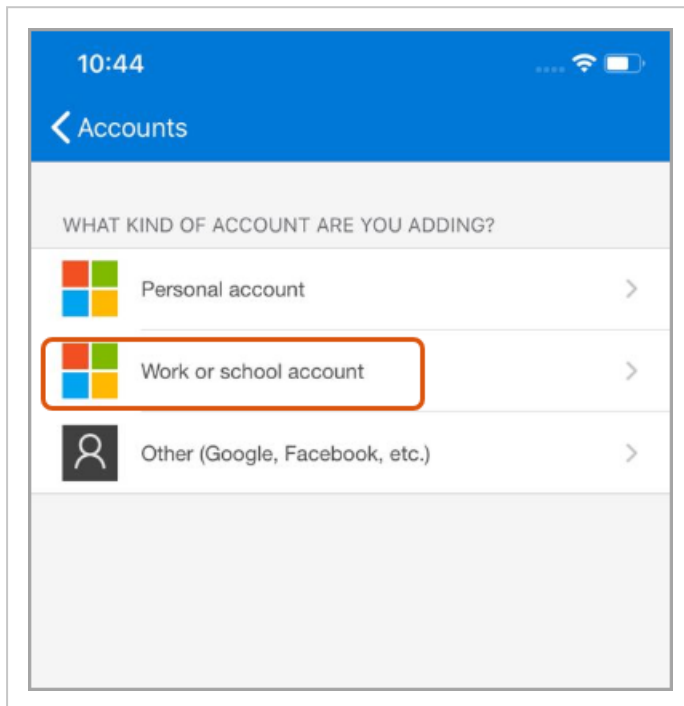
Authenticator app - iPhone

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

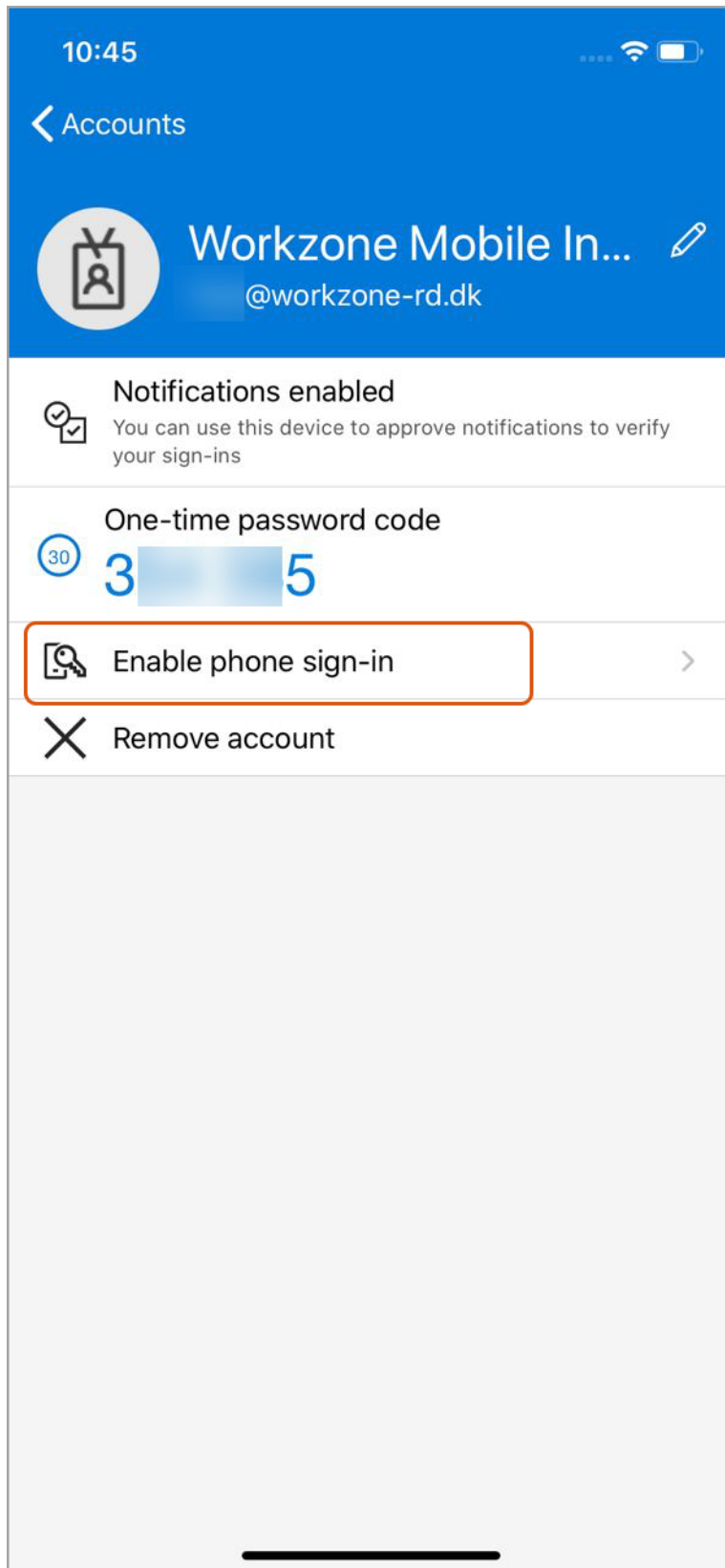
- A QR-code will appear on the screen. Scan it with your mobile device using the **Authenticator** app.
 - If your account is already added to the **Authenticator** app, select it from the app.

-Or-

- If your account is not added to the **Authenticator** app yet, add it. Under **What kind of account are you adding?**, select **Work or School account**.



5. After you have scanned the QR-code, your account will be displayed with the single sign tokens.
 - To simplify logging in, select **Enable phone sign-in**. This will allow you to log in using Face ID or TouchID, instead of entering the log-in codes.

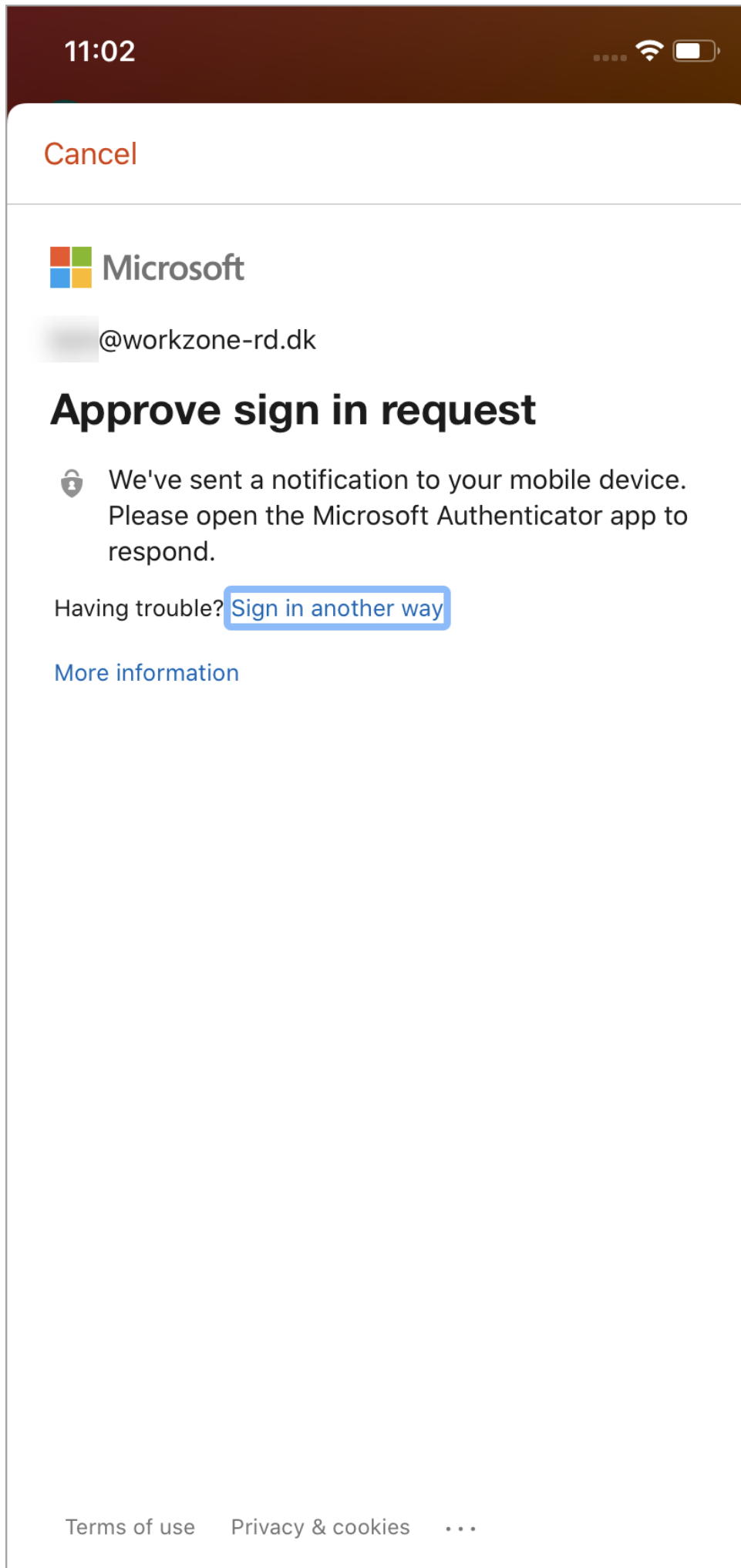


Log in to edit the Office documents

Before you start editing Office documents, you will need to confirm your login.

- After entering your user name and password, confirm your login via previously selected option: by phone, authentication code, Face ID or Touch ID, or notification code in the

Authenticator app.

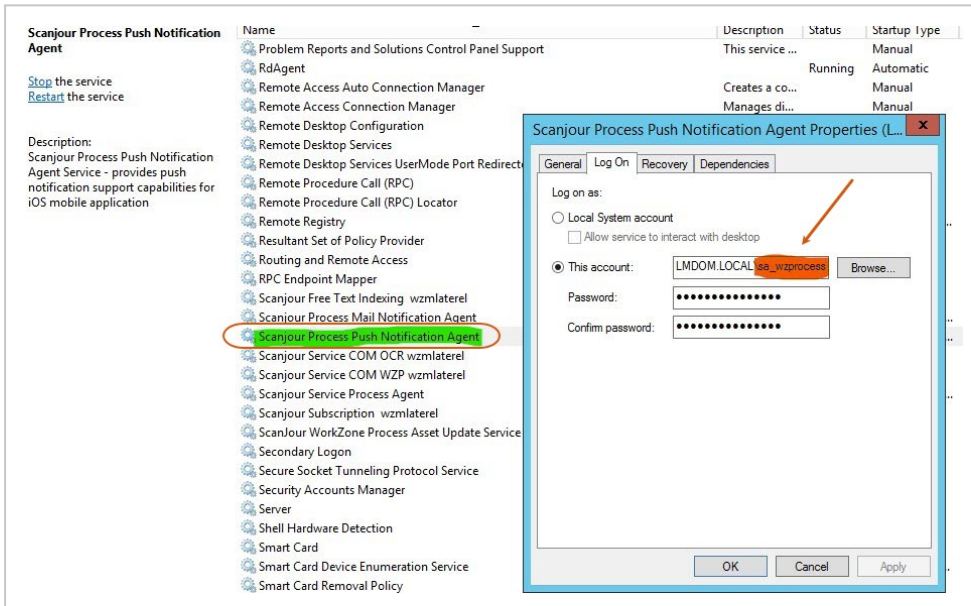
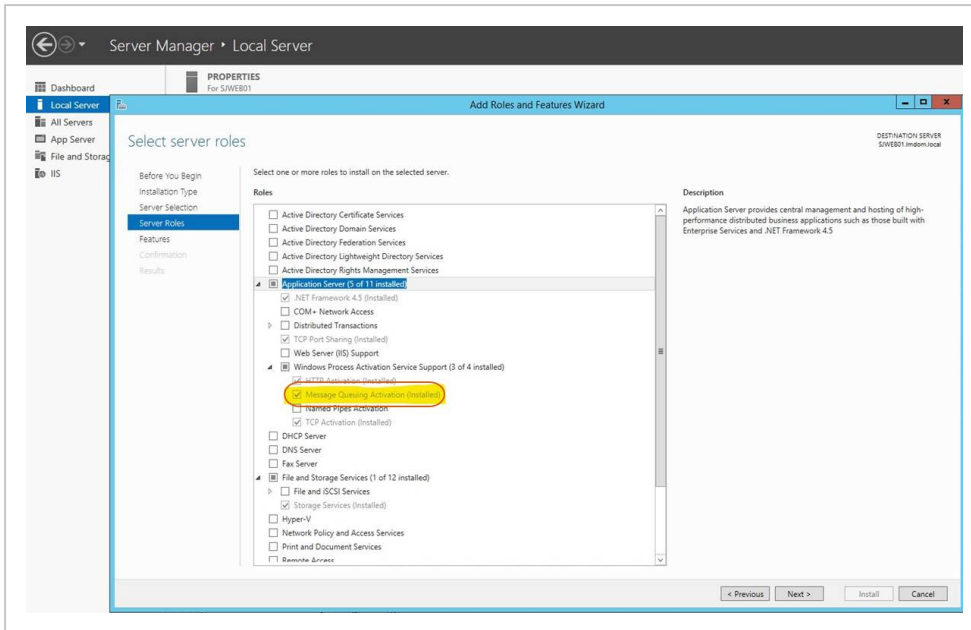


- After logging in, you can select to remain logged in all the time. In this case your login will be remembered during your next sessions (by default, your login will be remembered for 90 days, but this period can be changed during the initial setup of the Intune environment).

8.8 Push notification certificates for iOS

To enable push notifications feature for iOS devices, proceed with the following steps:

1. [Generate](#) the Apple Push Notification Services (APNS) certificate.
2. Configure push certificates in the [Administrator Guide for WorkZone Process](#).
3. Ensure that you have the following settings adjusted:



9. Citrix XenMobile

Citrix XenMobile is Citrix's **MDM**¹ solution.

Before you begin

Before you begin, please check the [WorkZone Mobile requirements to Citrix XenMobile infrastructure](#).

Configure WorkZone Mobile in Citrix XenMobile

When the requirements to the infrastructure are fulfilled, you can move on to setting up and configuring WorkZone Mobile in Citrix XenMobile.

This guide will be updated regularly with guidance on how to configure and manage WorkZone Mobile in XenMobile.

- [Wrap the WorkZone Mobile app using Citrix MDX Toolkit](#)
- [Publish WorkZone Mobile in Citrix XenMobile](#)

More information

For an overview of XenMobile, see [XenMobile page on the Citrix web site](#).

9.1 WorkZone Mobile requirements to Citrix XenMobile infrastructure

To allow WorkZone Mobile access to on-premise WorkZone through Citrix XenMobile, some configuration of your organization's infrastructure is required. You need to:

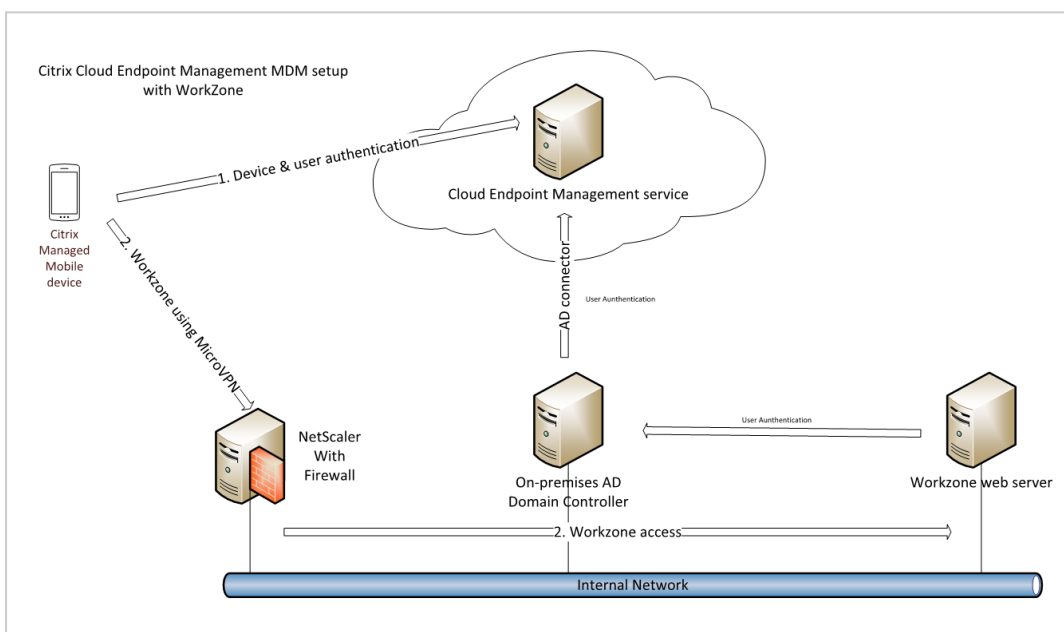
- Set up on-premises XenMobile server or Citrix Cloud Endpoint Management to manage organization's mobile devices.

¹Mobile Device Management

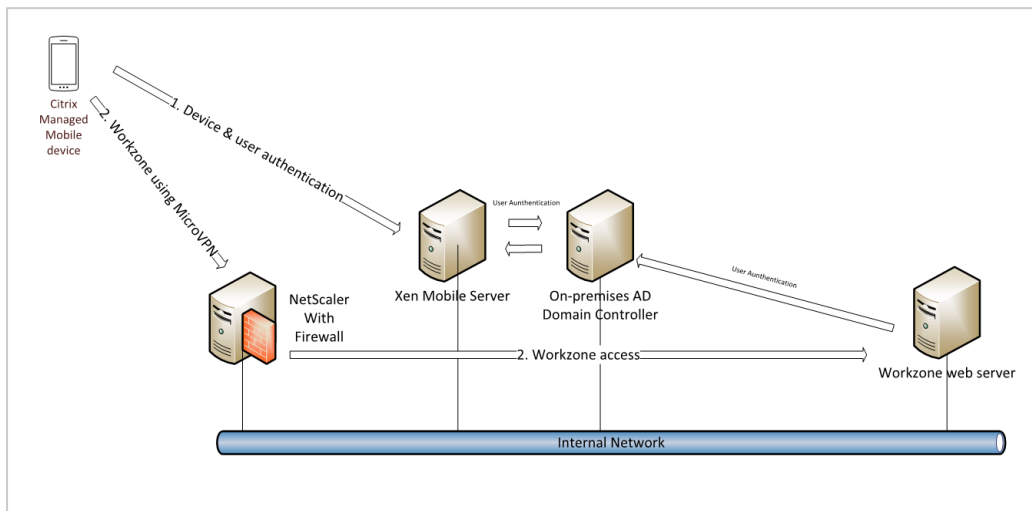
- Establish a Citrix NetScaler with MicroVPN to an internal WorkZone web server.
- Make the WorkZone Mobile app available in Citrix Secure Hub.

The diagram below shows a conceptual overview of the components in the infrastructure and how they are set up to support WorkZone Mobile with Citrix XenMobile. The number of real servers, firewalls, load balancers, and so on, varies depending on how the environment is set up for a specific organization.

Cloud solution



On-premises solution



Citrix XenMobile or Cloud Endpoint Management

You must set up an on-premises XenMobile server or use Citrix Cloud Endpoint Management to manage the mobile devices that should have access to the internal WorkZone web server. For users to have a consistent experience with user names and passwords, it is recommended to allow XenMobile access to look up and approve access in the same internal domain (Active Directory) that holds the WorkZone users. This is done by setting up the Citrix Active Directory Connector.

Citrix NetScaler

You need to set up a MicroVPN tunnel rule that allows mobile devices to access the internal WorkZone web server on port 80 for http, or port 443 for https, depending on the WorkZone setup.

WorkZone Mobile app uses NTLM, and does currently not support Single Sign-on with Citrix NetScaler. If Single Sign-On (SSO) is enabled on your NetScaler, you need to create a policy that disables SSO towards the WorkZone web server.

Publishing the WorkZone Mobile on Citrix XenMobile

You need to wrap the WorkZone Mobile app using Citrix MDX Toolkit before you can manage it in XenMobile. See [Wrap the WorkZone Mobile app using Citrix MDX Toolkit](#).

Tip: You can deploy the app using delivery groups.

9.2 Wrap the WorkZone Mobile app using Citrix MDX Toolkit

The steps below describe how to wrap the WorkZone Mobile app so that it can be managed in Citrix XenMobile.

[Wrap WorkZone Mobile for iOS](#)

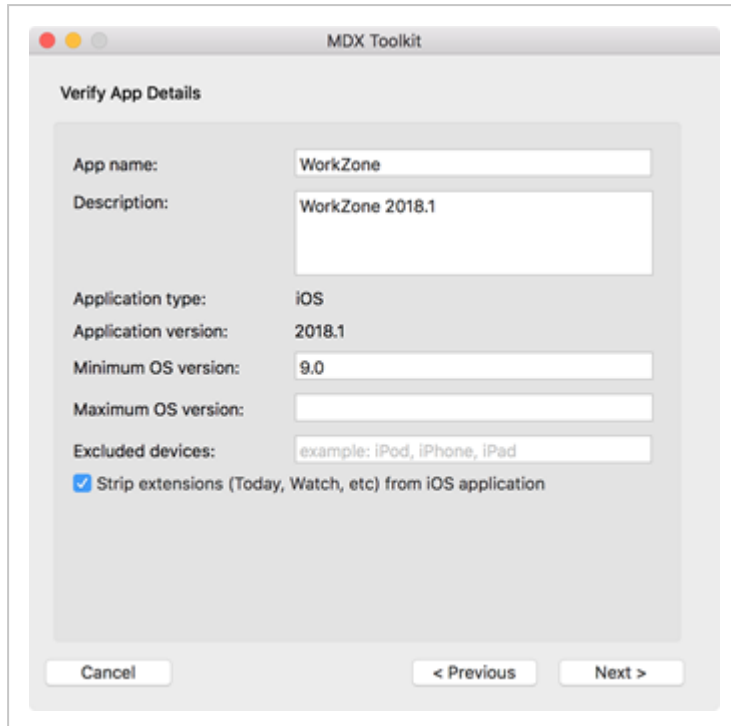
[Wrap WorkZone Mobile for Android](#)

Wrap WorkZone Mobile for iOS

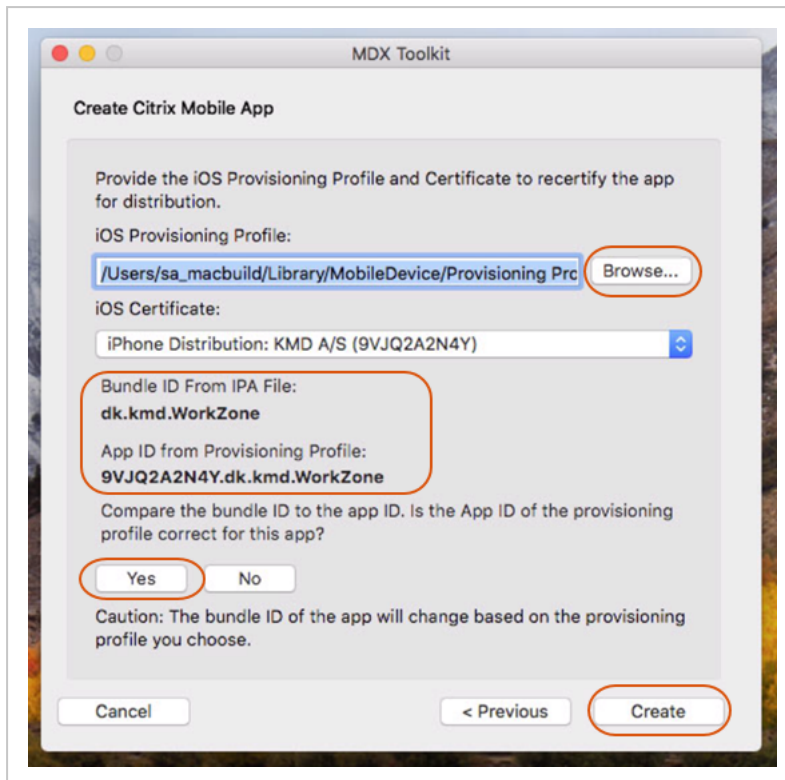
Prerequisites:

- Citrix MDX Toolkit is installed.
- Application binary - an IPA file. Contact your WorkZone responsible to get the file.
- Files used for signing the application, such as a provisioning profile, a signing certificate, or a private key.
- Latest Xcode is installed with command line tools.

1. Launch Citrix MDX Toolkit, and click **Next** on the **Welcome to the MDX Toolkit for Enterprise Deployment** page.
2. On the **Select the Input Package** page, click **Browse**, and then navigate to the IPA file, you want to wrap.
3. Click **Next**, the data on this page is pre-filled with information from the IPA file.



4. Change the **App name**, **Description**, and other fields. The settings you specify here will be shown in Citrix Store.
5. Leave the **Strip extensions** check box selected.
6. Click **Next**.
7. On the **Create Citrix Mobile App** page, click **Browse** and navigate to the provisioning profile that will be used to sign the application.
8. Select the iOS certificate from the list.
9. Verify the Bundle ID from the IPA file, and from the provisioning profile. If they are correct, click **YES**, and then **Create**.



- Now, select the folder where you want to store the wrapped application, the MDX file, and click **Create**.

The MDX file is now created and you can upload it to XenMobile for publishing to devices.

Please refer to the Citrix documentation for more information:

[Wrapping iOS mobile apps](#)

[Other requirements for wrapping iOS mobile apps](#)

Wrap WorkZone Mobile for Android

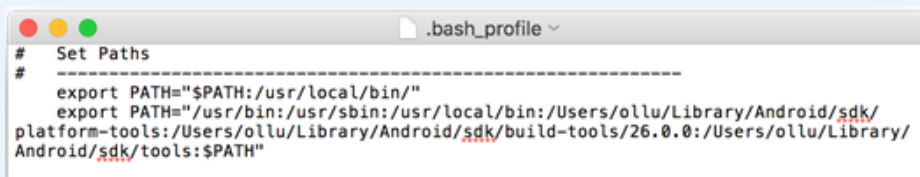
Prerequisites:

- Android SDK (API level 26)
- Verify that the **.bash_profile** exists and contains the full paths for the appropriate folders under android-sdk.

Verify and create a .bash_profile

1. Start up Terminal.
2. Type `cd ~/` to go to your home folder.
3. If you do not have **.bash_profile** in your home folder, type `touch .bash_profile` to create a new file.
4. Type `open -e .bash_profile` to open it in TextEdit, add paths, and save.
5. Type `source .bash_profile` to reload and update the **.bash_profile**.

Example:



```
# Set Paths
# -----
export PATH="$PATH:/usr/local/bin/"
export PATH="/usr/bin:/usr/sbin:/usr/local/bin:/Users/ollu/Library/Android/sdk/platform-tools:/Users/ollu/Library/Android/sdk/build-tools/26.0.0:/Users/ollu/Library/Android/sdk/tools:$PATH"
```

- Citrix MDX Toolkit is installed.

In **Applications > Citrix > MDX Toolkit**, open the **android_settings.txt** file, and then add the full path for the following folders:

- Android SDK
- Android SDK > tools
- Android SDK > platform-tools
- Android SDK > build-tools > [version]

Example:

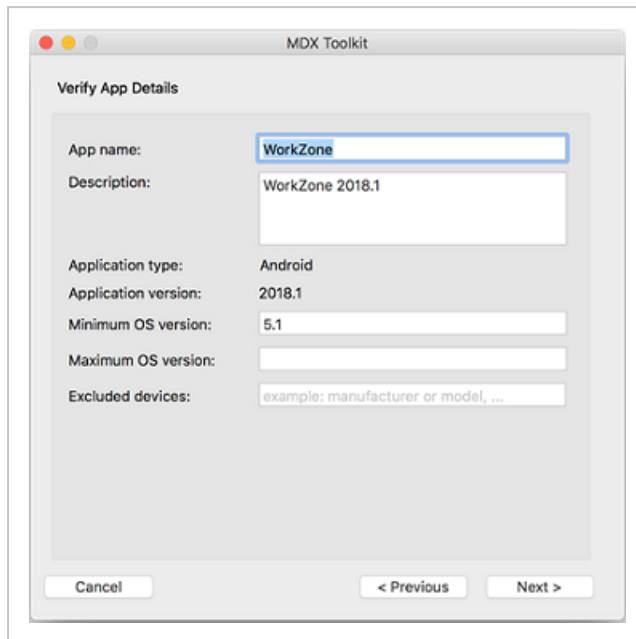
```

android_settings.txt — Locked
// For Android wrapping, not iOS
//
// Created by Citrix Systems on 06/02/14.
// Copyright (c) 2014 Citrix Systems, Inc. All rights reserved.
//
// This file is intended for modifying the environment variables on
// your machine for the purposes of Citrix application wrapping without
// affecting the rest of your environment.
//
// Please ensure all wrapping prerequisites are downloaded and installed
// before continuing. A sample is given for you. Please find the correct
// locations on your machine and add them to the path below. Please
// separate paths with your OS specific separators,
// i.e. (":" - Unix, ";" - Windows)
//
// Sample Unix Path:
// PATH = /Users/Sample/Downloads/android-sdk-macosx/platform-tools:/Users/Sample/
Downloads/android-sdk-macosx/build-tools/19.1.0:/Users/Sample/Downloads/android-sdk-
macosx/tools
//
// To use this file, please delete the comments, "//", and append the correct
// paths to the PATH variable below.
//
//PATH = /usr/bin:/usr/sbin
//
PATH = /usr/bin:/usr/sbin:/usr/local/bin:/Users/ollu/Library/Android/sdk:/Users/ollu/
Library/Android/sdk/platform-tools:/Users/ollu/Library/Android/sdk/build-tools/26.0.0:/
Users/ollu/Library/Android/sdk/tools:/Users/ollu/Library/Android/sdk/build-tools

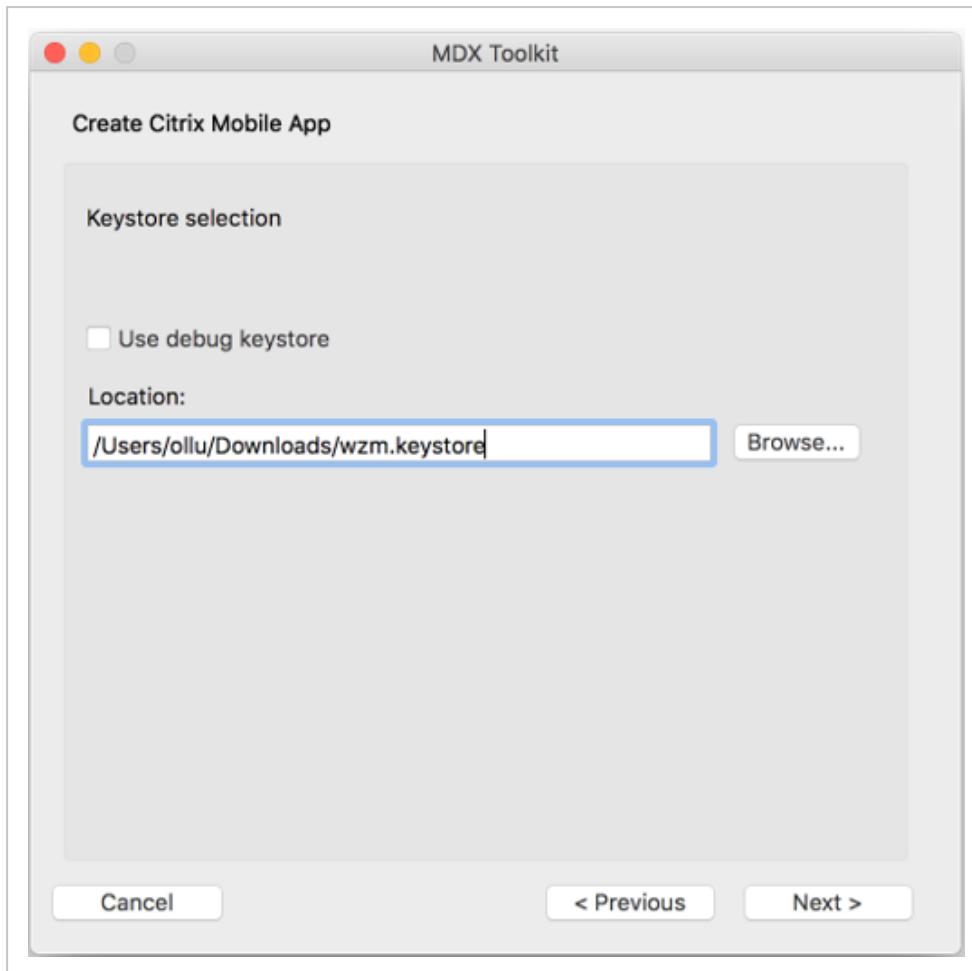
```

- Application binary - an APK file. Contact your WorkZone responsible to get the file.
- Files used for signing the application, such as a valid keystore, a signing certificate, or a private key.

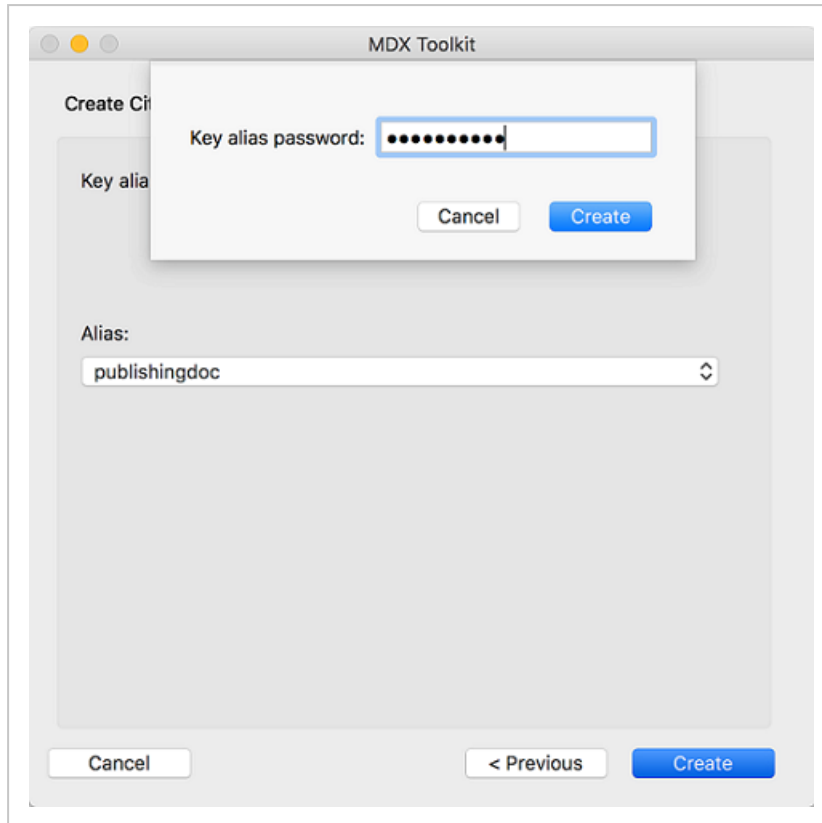
1. Launch Citrix MDX Toolkit, and click **Next** on the **Welcome** page.
2. On the **Select the Input Package** page, click **Browse**, and then navigate to the APK file, you want to wrap.
3. Click **Next**. The data on this page is pre-filled with information from the APK file.



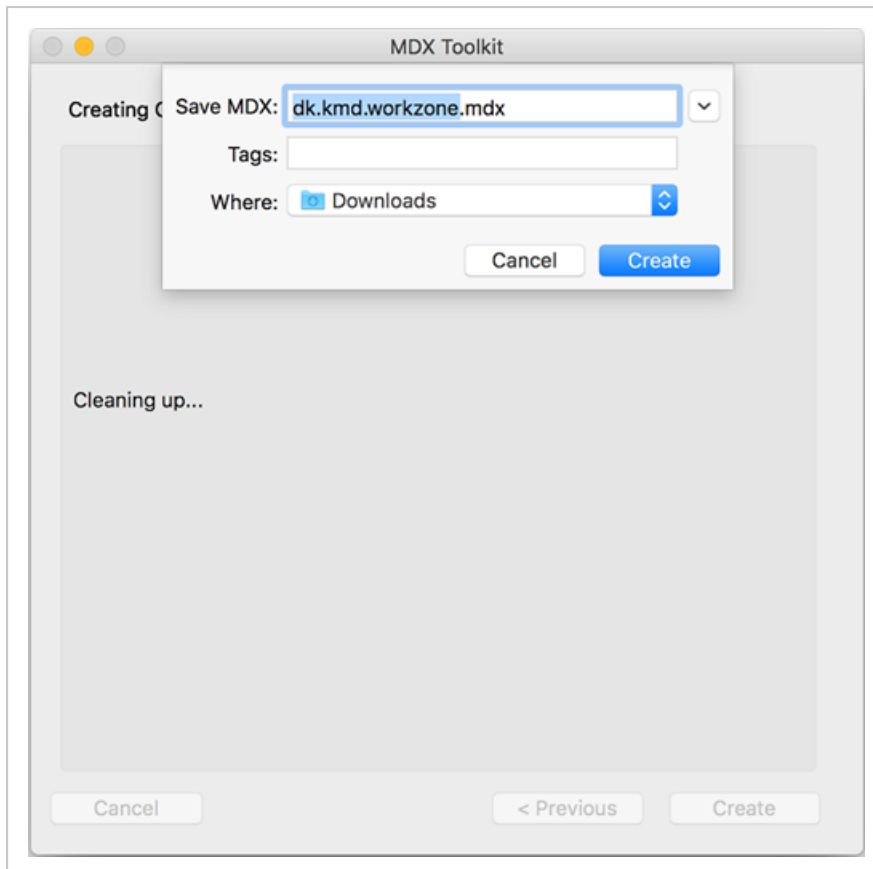
4. Change the **App name**, **Description**, and other fields. The settings you specify here will be shown in Citrix Store.
5. Click **Next**.
6. On the **Create Citrix Mobile App** page, click **Browse** and navigate to the keystore that will be used to sign the application.



7. Click **Next**, enter the password to the keystore, and then click **Next**.
8. Back on the **Create Citrix Mobile App** page, click **Create** without making any changes.
9. Enter the key alias password, and then click **Create**.



10. Select the folder where you want to store the wrapped application, the MDX file, and click **Create**.



The MDX file is now created and you can upload it to XenMobile for publishing to devices.

Please refer to the Citrix documentation for more information:

[Wrapping Android mobile apps](#)

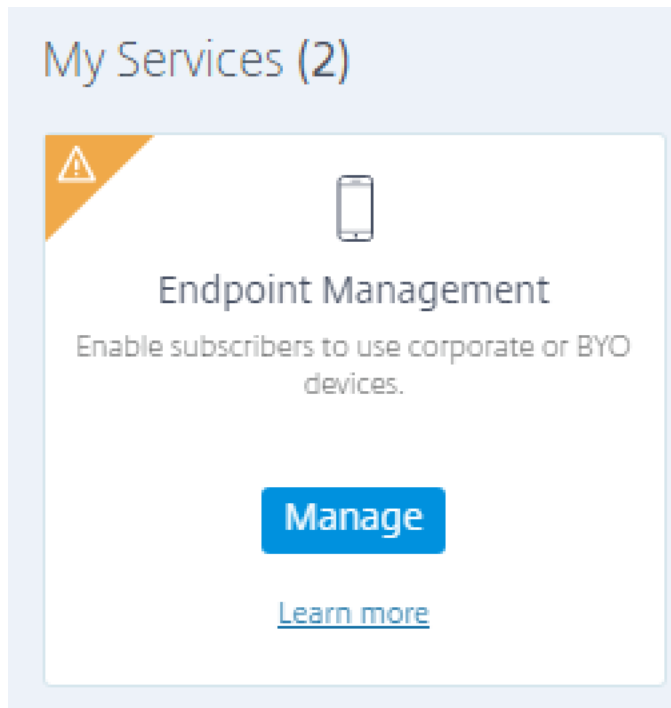
[Other requirements for wrapping Android mobile apps](#)

[Manage your own key and keystore](#)

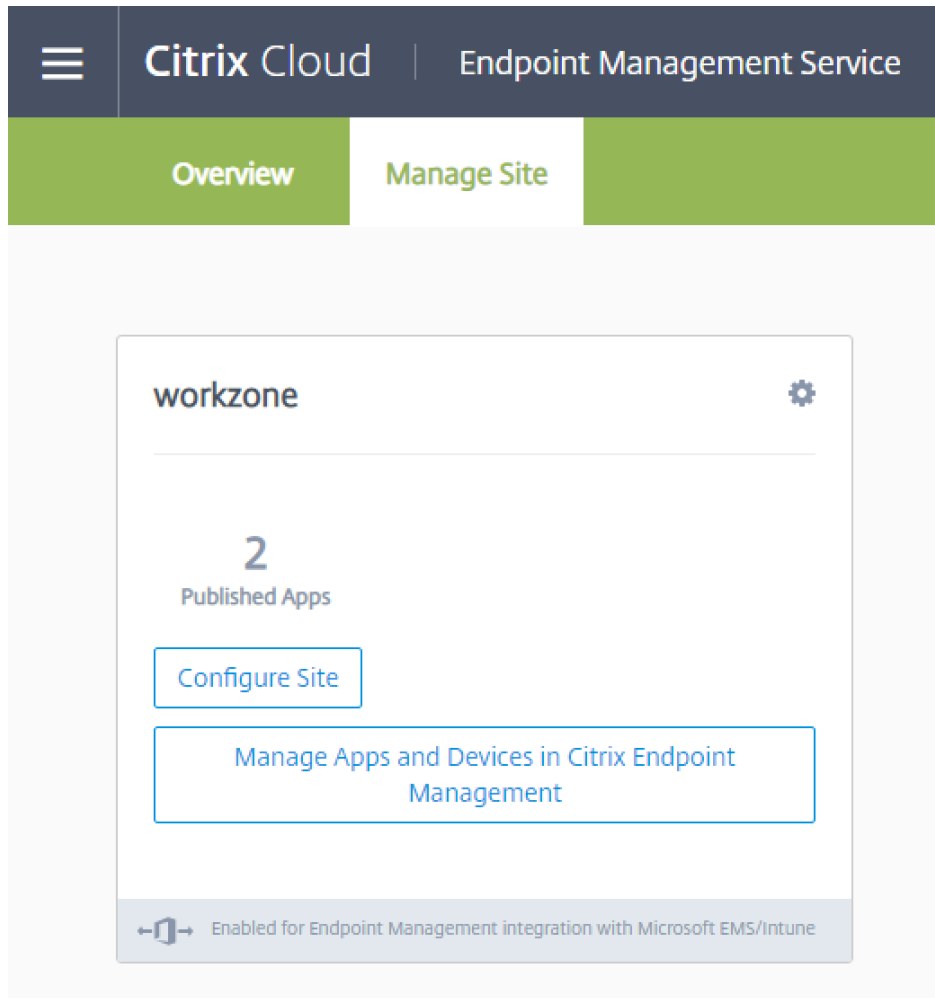
9.3 Publish WorkZone Mobile in Citrix XenMobile

The procedure below walks you through the basic steps of how to publish the WorkZone Mobile app through Citrix XenMobile. Depending on your organization's setup, you may need to specify more XenMobile settings than are described below. Please refer to the Citrix documentation for more information.

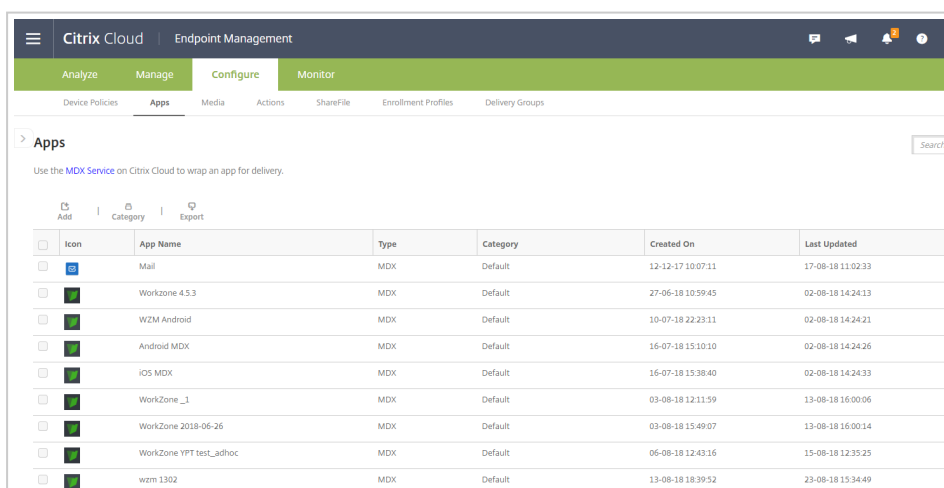
1. In Citrix XenMobile, click **Manage** under **Endpoint Management**.



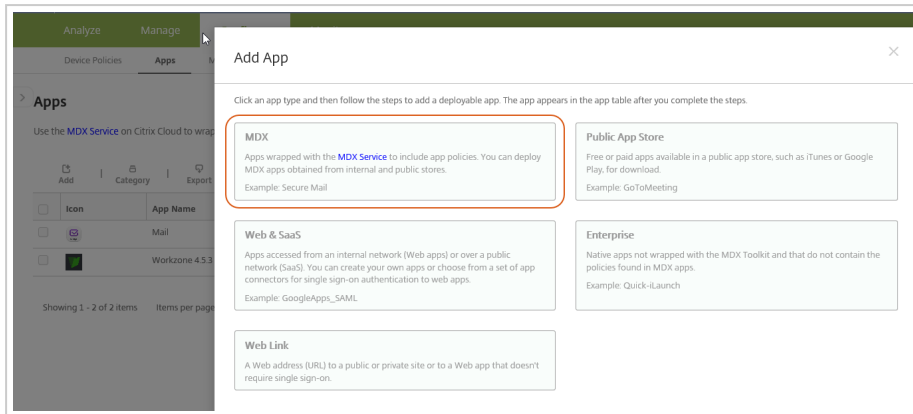
2. Click **Manage Apps and Devices in Citrix Endpoint Management**.



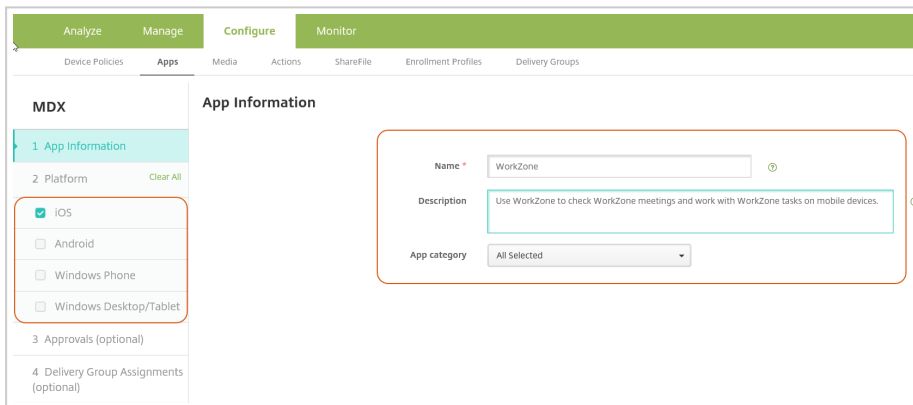
3. Click **Configure > Apps**.



4. Click **Add > MDX**.



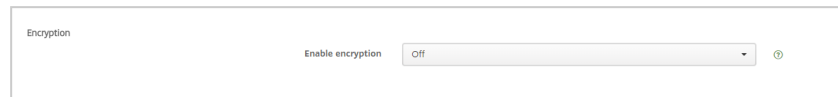
5. Clear the check boxes that are not relevant for the current publication. In this example, only iOS is selected. Fill in information about the app. The information that you enter here is only for internal use.



6. Click **Next**.
7. On the **iOS MDX App** page, click **Upload**, and select the wrapped app file (the .MDX file).
8. Click **Next**. Note that it takes a while to upload the file. When the upload is complete, a number of settings appear on the **iOS MDX App** page.
9. Fill in the policy and security settings as needed.

- For MDX Toolkit 10.X: Ensure that the following values are selected:

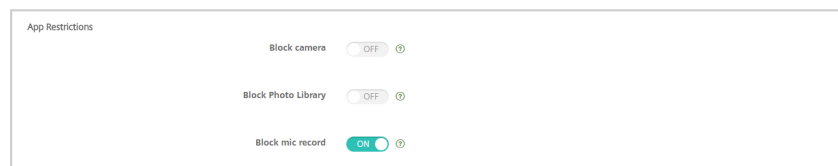
- **Encryption:** Set **Enable encryption** to **Off**.



Encryption

Enable encryption

- **App Restrictions:** Set **Block camera** and **Block Photo Library** to **OFF**. This means that WorkZone Mobile users will be able to add photos to tasks using the camera and the photo library on their devices.



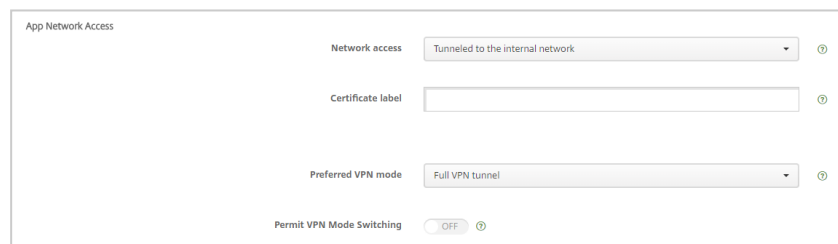
App Restrictions

Block camera

Block Photo Library

Block mic record

- **App Network Access:** Set **Network access** to **Tunneled to the internal network** and **Preferred VPN mode** to **Full VPN tunnel**.



App Network Access

Network access

Certificate label

Preferred VPN mode

Permit VPN Mode Switching

- For MDX Toolkit 19.X: Ensure that the following values are selected:

- **Encryption:** Set **Encryption Type** to **Platform encryption with compliance enforcement, Non-compliant device behavior** to

Allow app, and Enable MDX encryption to On.

Encryption

Encryption Type: Platform encryption with compliance enforce... ⓘ

Non-compliant device behavior: Allow app ⓘ

Enable MDX encryption: On ⓘ

Database encryption exclusions: ⓘ

File encryption exclusions: ⓘ

- **App Restrictions:** Set **Block camera** and **Block Photo Library** to **OFF**. This means that WorkZone Mobile users will be able to add photos to tasks using the camera and the photo library on their devices.

App Restrictions

Block camera: OFF ⓘ

Block Photo Library: OFF ⓘ

Block mic record: ON ⓘ

- **App Network Access:** Set **Network access** to **Tunneled - Full VPN**, **micro VPN session required** to **Use Previous Settings**, and **micro VPN session required grace period (minutes)** to **0**.

App Network Access

Network access: Tunneled - Full VPN ⓘ

micro VPN session required: Use Previous Settings ⓘ

micro VPN session required grace period (minutes): 0 ⓘ

Certificate label: ⓘ

Exclusion List: ⓘ

10. Click **Next**. Optionally, apply an approval workflow on the **Approvals (Optional)** page, and then click **Next**.

11. On the **Delivery Group Assignment (Optional)** page, optionally select the delivery group that you want to deploy the app to.
12. Click **Save** to publish the WorkZone Mobile app.

10. Document formats supported in preview

In WorkZone Mobile, users can preview documents that are attached to tasks or meetings. When the user taps a document title, the document viewer displays the documents in PDF format.

The following document formats can be previewed on iOS devices:

- Microsoft Office documents (Office '97 and newer)
- Microsoft Project files
- Microsoft Visio files
- Emails
- XLSM files
- Rich Text Format (RTF) documents
- PDF files
- Text files whose uniform type identifier (UTI) conforms to the public.text type
- Comma-separated value (csv) files
- AutoCAD files
- Apache OpenOffice files
- Zip files

On iOS devices

- Microsoft Excel documents, image files, txt files, and xml documents open in Quick Look as the display quality is better than the PDF format.
- Documents that cannot be converted to PDF, for example video and audio files, open in the original format.

On Android devices

- Documents that cannot be converted to PDF, for example video and audio files, cannot be previewed.

11. Known issues

Click an issue below to see a description and a possible workaround.

After upgrading the WorkZone products to next version, the Meeting module disappears from WorkZone Mobile.

To solve the issue, advise the user to re-log in on WorkZone Mobile.

A delay during the WorkZone for Intune loading and switching between tasks

- When you log in for the first time after the WorkZone for Intune installation, the authentication delay might take around 3 minutes.
- When you have selected another task, you might see the previous task on your screen for around 20 seconds more.

This is the expected behavior since the system requires some time to process these actions. Please wait until it has finished.

WorkZone Mobile app for Intune stops connecting

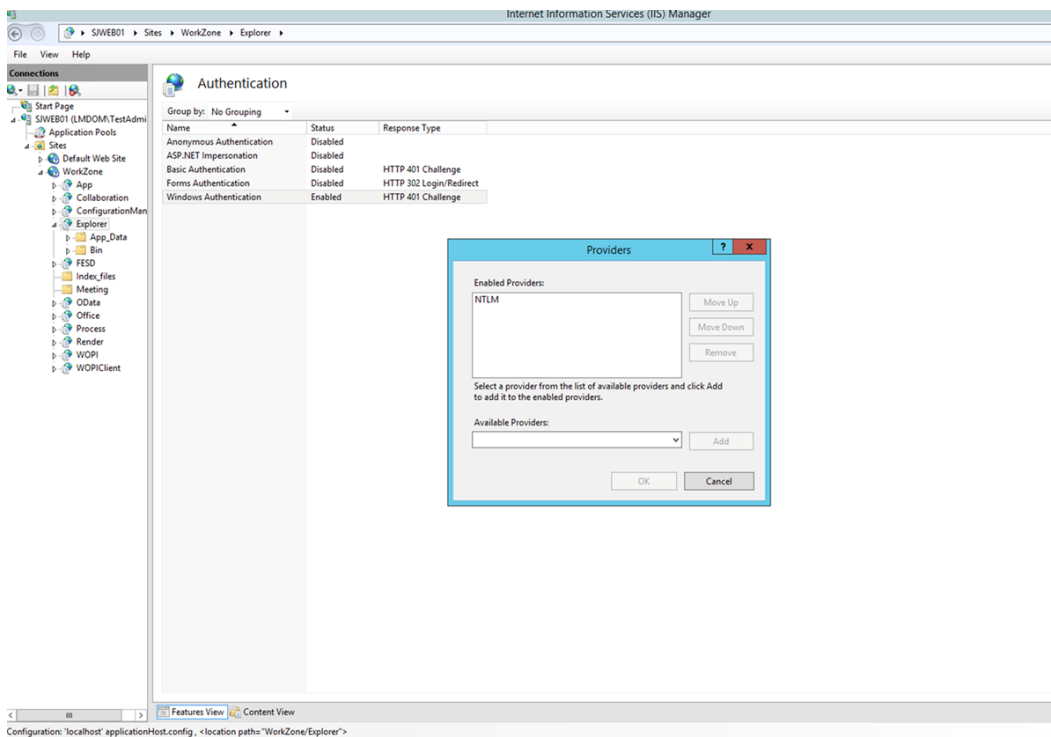
After some time the WorkZone Mobile application stops connecting, returning the "Not connected/Ikke tilsluttet" error message. Attempts to restart the application result with the "Connect/Tilslut" error message.

Check the Wi-Fi settings on user's device. Ensure that the user uses your regular internet connection (that is, the connection previously used to successfully connect to WorkZone).


Office app fails to get the WorkZone documents (unmanaged App Store iOS version only)

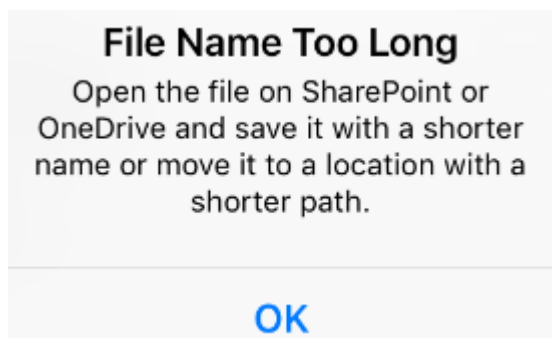
If Office app fails to open the WorkZone documents, advise the user to reset the Office app from the device settings. If the issue persists, verify that WorkZone Explorer Authentication

providers (located under **Internet Information (IIS) Manager > Sites > WorkZone > Explorer > Windows Authentication > Providers**) only contain **NTLM**.



Documents cannot be exported if the file name is too long

When users click  in the document viewer, they may get the following error message:



12. Terms and conditions

Intellectual property rights

This document is the property of KMD. The data contained herein, in whole or in part, may not be duplicated, used or disclosed outside the recipient for any purpose other than to conduct business and technical evaluation provided that this is approved by KMD according to the agreement between KMD and the recipient. This restriction does not limit the recipient's right to use information contained in the data if it is obtained from another source without restriction set out in the agreement between KMD and the recipient or by law.

Disclaimer

This document is intended for informational purposes only. Any information herein is believed to be reliable. However, KMD assumes no responsibility for the accuracy of the information. KMD reserves the right to change the document and the products described without notice. KMD and the authors disclaim any and all liabilities.

Copyright © KMD A/S 2020. All rights reserved.