How Application Groups Feature Works

Last Modified on 23/02/2024 1:56 pm EET

Application Groups can be used to automatically update applications that have been installed from Company Portal through **available** type deployment. For this feature to function, an additional consent from a Global Administrator is required:

1. Configure additional permissions for Application Groups feature
2. Configure Application Groups Feature

Process once the feature is fully configured and an application is deployed into Company Portal:

1. User installs an application created by CSM for Intune from Company Portal
2. Application is installed to user's workstation
    - Application install status is reported to Intune. Application Groups feature uses device install status to determine what devices are going to be added to the selected Azure AD group
3. The workstation is automatically added into the Azure AD group corresponding the installed application. This relationship is specified in CSM for Intune Application Groups settings
    - Workstations are added to Azure AD groups once a day
4. All upcoming versions of the application will be automatically installed into user's workstation through **required** type deployment

- If you delete a workstation from Azure AD group that's used in Application Groups, and uninstall the matching application from the workstation, Application Groups feature might re-add the workstation to the Azure AD group due to reporting delays. This will cause the app to be re-installed to the workstation.
- If you'd like to exclude a specific device from a application group, you need to create a separate application specific Azure AD group for devices to be excluded from deployments. Add the device to the new group, and add the group to the application's deployment process in CSM portal by using **exclude** mode. Read more from here.