

Proget Documentation

1. [Home](#)
2. [Proget Console](#)
3. [Administrator guide](#)
4. [Login](#)
5. [Dashboard](#)
6. [My Card](#)
7. [Devices](#)
8. [Attributes](#)
9. [Certificates](#)
10. [Audit Logs](#)
11. [Backups](#)
12. [Settings](#)
13. [Dependency graph](#)
14. [Users](#)
15. [Add user from Microsoft Entra ID](#)
16. [Add user from LDAP](#)
17. [Add local user](#)
18. [User Backups](#)
19. [Activations](#)
20. [Manual](#)
21. [Automatic](#)
22. [Templates](#)
23. [Template configuration](#)
24. [Custom EULA](#)
25. [EULA configuration](#)
26. [Devices](#)
27. [Activations](#)
28. [Android Enterprise Device Owner](#)
29. [Service password](#)
30. [Android Enterprise Profile Owner \(COPE\)](#)
31. [Service password](#)
32. [Android](#)
33. [Service password](#)
34. [iOS \(Supervised mode\)](#)
35. [macOS](#)
36. [Windows](#)

- 37. [Devices tabs](#)
- 38. [Details](#)
- 39. [Policy](#)
- 40. [Profiles](#)
- 41. [Applications](#)
- 42. [Location](#)
- 43. [Backups](#)
- 44. [Audit log](#)
- 45. [Tasks](#)
- 46. [Dependency graph](#)
- 47. [File Manager](#)
- 48. [Reports](#)
- 49. [Export](#)
- 50. [User accounts](#)
- 51. [System bug reports](#)
- 52. [Photos during device lock](#)
- 53. [Users](#)
- 54. [Groups](#)
- 55. [Group Priorities](#)
- 56. [Selected group](#)
- 57. [Manage filter](#)
- 58. [Proget Query Language \(PQL\)](#)
- 59. [Apps](#)
- 60. [Add application](#)
- 61. [Single Android app](#)
- 62. [Single Android app from file](#)
- 63. [Single iOS app](#)
- 64. [Policies](#)
- 65. [Android Enterprise Device Owner](#)
- 66. [Android Enterprise Profile Owner](#)
- 67. [Android](#)
- 68. [iOS](#)
- 69. [macOS](#)
- 70. [Windows](#)
- 71. [Profiles](#)
- 72. [ActiveSync](#)

- 73. [APN](#)
- 74. [Android Enterprise configuration](#)
- 75. [Samsung configuration](#)
- 76. [iOS configuration](#)
- 77. [Apple Business Manager](#)
- 78. [Apple Update](#)
- 79. [Application rules](#)
- 80. [Android Enterprise - work space](#)
- 81. [Android Enterprise - private space](#)
- 82. [iOS \(Supervised mode\)](#)
- 83. [Backup](#)
- 84. [Business contacts](#)
- 85. [Business documents](#)
- 86. [Certificate](#)
- 87. [File](#)
- 88. [Template](#)
- 89. [SCEP](#)
- 90. [Certificate mapping](#)
- 91. [Connectivity](#)
- 92. [Custom Apple Configuration](#)
- 93. [Geofencing](#)
- 94. [IMAP/POP](#)
- 95. [Kiosk](#)
- 96. [Android](#)
- 97. [Single App](#)
- 98. [Multi App](#)
- 99. [iOS](#)
- 100. [Location](#)
- 101. [MTP](#)
- 102. [SCEP](#)
- 103. [Shared device](#)
- 104. [VPN](#)
- 105. [Proget IPsec](#)
- 106. [IPsec](#)
- 107. [IKEv2](#)
- 108. [L2TP](#)

- 109. [Custom SSL](#)
- 110. [Wallpaper](#)
- 111. [Wi-Fi](#)
- 112. [Labels](#)
- 113. [Audit logs](#)
- 114. [Tasks](#)
- 115. [Service](#)
- 116. [Update](#)
- 117. [Service history](#)
- 118. [Service password](#)
- 119. [Security](#)
- 120. [Reports](#)
- 121. [List](#)
- 122. [Generate report](#)
- 123. [Configuration](#)
- 124. [Add report configuration](#)
- 125. [Settings](#)
- 126. [Access control](#)
- 127. [Allowed SIM Cards](#)
- 128. [List](#)
- 129. [Manage Allowed SIM Cards](#)
- 130. [Operations](#)
- 131. [Audit and logging](#)
- 132. [Certificate Manager](#)
- 133. [CAs](#)
- 134. [User certificates](#)
- 135. [External certificates](#)
- 136. [Connector](#)
- 137. [Gateway](#)
- 138. [General](#)
- 139. [LDAP](#)
- 140. [Microsoft Entra ID](#)
- 141. [Users configurations](#)
- 142. [Settings](#)
- 143. [Roles](#)
- 144. [Add Role](#)

- 145. [SMTP](#)
- 146. [Default configuration](#)
- 147. [Basic authentication](#)
- 148. [Modern authentication \(Google\)](#)
- 149. [Modern authentication \(Microsoft 365\)](#)
- 150. [Theme](#)
- 151. [Updates](#)
- 152. [Integrations](#)
- 153. [Android Enterprise](#)
- 154. [Android zero-touch](#)
- 155. [Apple Business Manager](#)
- 156. [Apple Push Notification Service](#)
- 157. [Apps and Books](#)
- 158. [Microsoft Entra ID Applications](#)
- 159. [Samsung KME](#)
- 160. [File Manager](#)
- 161. [Changelog](#)
- 162. [Known Issues](#)
- 163. [Proget Mobile App](#)
- 164. [Changelog](#)
- 165. [Known issues](#)
- 166. [Proget Notifier App](#)
- 167. [Changelog](#)
- 168. [Proget File Manager App](#)
- 169. [Changelog](#)
- 170. [Proget Remote App](#)
- 171. [Changelog](#)
- 172. [Proget Geofencing App](#)
- 173. [Changelog](#)
- 174. [Proget Backup App](#)
- 175. [Changelog](#)
- 176. [Proget File Sharing App](#)
- 177. [Changelog](#)
- 178. [Proget OpenVPN App](#)
- 179. [Changelog](#)
- 180. [FAQ](#)

Important information

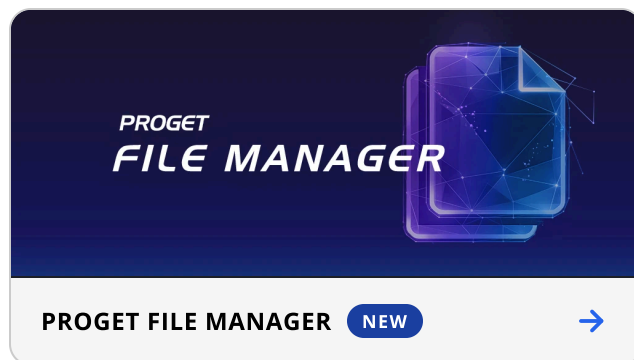
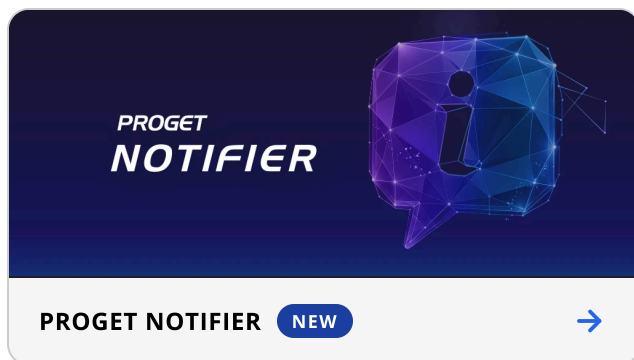
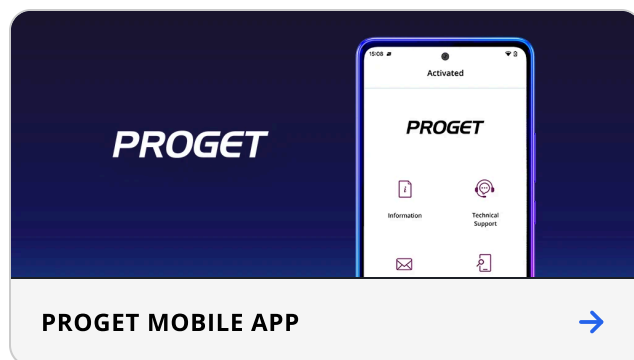
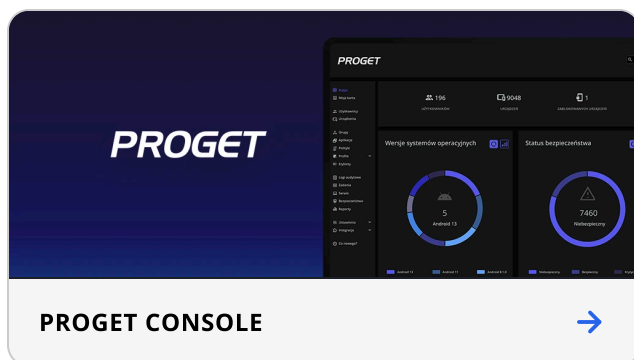
✓ **Proget Console**
Version 2.20.4

✓ **Proget Mobile App**
Version 2.20.3

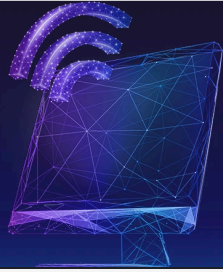
✓ **Proget Notifier**
Wersja 1.0.0

✓ **Proget File Manager**
Wersja 0.1.1

Applications



PROGET
REMOTE



PROGET REMOTE



PROGET
GEOFENCING



PROGET GEOFENCING



PROGET
BACKUP



PROGET BACKUP



PROGET
FILE SHARING



PROGET FILE SHARING



PROGET
OPENVPN

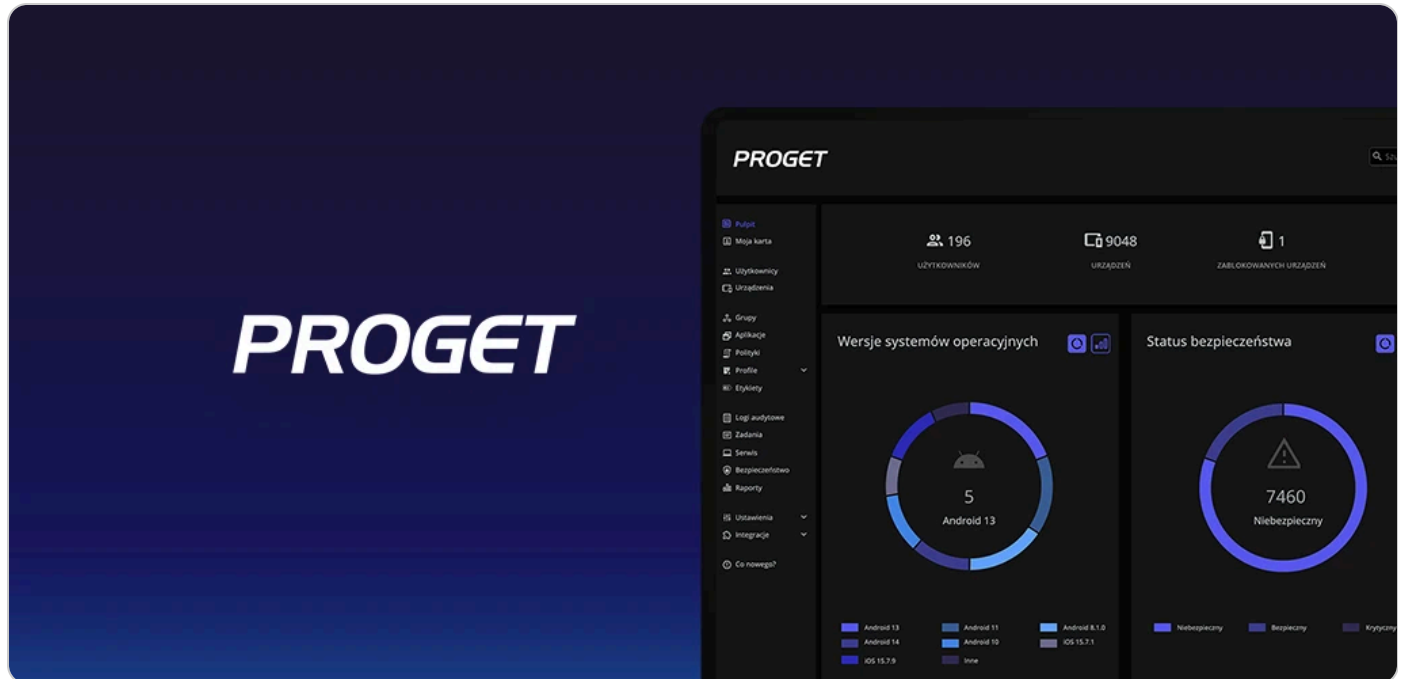


PROGET OPENVPN



Proget Console

Updated: Feb 13, 2025



Administrator guide



Changelog



Known Issues

Administrator guide

Updated: Jul 16, 2026

Administrator guide contains information about the administrator console that will help you get familiar with our system. Here you will find a description of our system and its features to help you get started using our product.



Login

Log in to the console via domain, local, or Microsoft Entra ID



Dashboard

Overview of users, devices, notifications, and device locations



My Card

User details, assigned devices, and available user actions



Users

Manage users and add them via Entra ID, LDAP, or locally



Activations

Manual, automatic, template-based, and custom EULA device activation



Devices

Table of devices activated on the server with their details



Groups

Groups for assigning policies, profiles, and apps to many devices



Apps

Table of applications available on the given server



Policies

Restrict device functionality: password rules, camera, Google services



Profiles

Configure email, location, app rules, documents, and backups



Labels

Label groups and users to assign devices to them



Audit logs

Collect and review events occurring on the server



Tasks

Tasks sent to devices by users or the system



Service

Data on devices ever activated on the server



Security

Table of security events recorded on devices



Reports

Configure and generate reports about devices in the system



Settings

Access control, LDAP, SMTP, certificates, roles, and other settings



Integrations

Android Enterprise, Apple Business Manager, Entra ID, and other...



File Manager

Manage files on iOS and Android devices remotely

Login

Updated: Dec 17, 2025

Login page allows you to log in to the Proget console using domain, local or Microsoft Entra ID mode.

Sign in ? EN ▾

Login mode: ☒ Domain ☐ Local ☐ Microsoft Entra ID

Domain\Username

Password

Sign in

1 Domain login

- Enter domain username and password
- Confirm with the 'Sign in' button
- For this option to be work, LDAP needs to be added and correctly configured in the Proget console

2 Local login

- Enter the local username or email and password
- Confirm with the 'Sign in' button
- If you forgot your password, you can use 'Forgot your password?' button and you will receive a link to reset your password via email

3 Microsoft Entra ID login

- After clicking 'Microsoft Entra ID' button you will be transferred Microsoft page where you can log in to Microsoft account
- Subsequently you will be logged in to Proget console automatically

- For this option to be work, Microsoft Entra ID needs to be added and correctly configured in the Proget console

4

Help

4.1 Admin guide

- After clicking the 'See Guide' button, you will be redirected to the Proget documentation, where you will find information about our system (e.g. FAQ, known issues, changelog)

4.2 Knowledge base

- After clicking the 'Go to site' button, you will be redirected to the Proget website, where you will find information about the entire system

4.3 Suggestions

- After clicking the 'Make Your Suggestion' button, you can share feedback on existing features or propose new solutions
- Email address to the Product Development Department

4.4 Support

- After clicking the 'Submit a ticket' button, you will be redirected to the Proget page, where you will be able to send a ticket with the problem to the support department
- Email address to the Proget support department

4.5 Sales

- Email address to Proget sales department

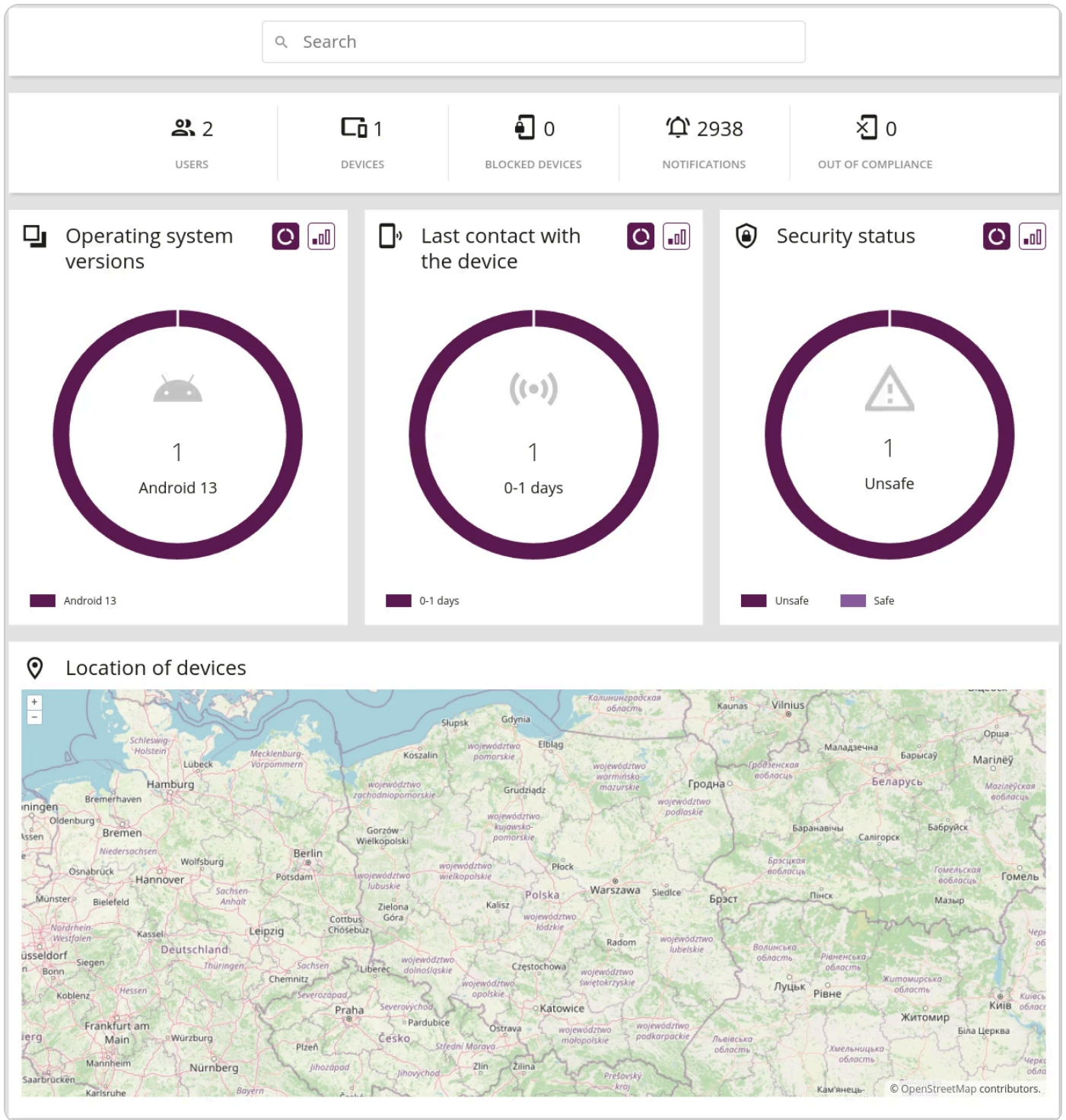
4.6 Professional

- After clicking the 'Check the offer' button, you will be redirected to the Proget store, where you can find and purchase our additional services

Dashboard

Updated: Dec 3, 2024

The dashboard tab shows the number of users, devices and notifications on a given server. Here you can find information about devices such as: operating system versions, last contact with the device and security status. If any device from the console has downloaded location, it will be displayed on the map.



1 Search

- Here you can search for anything that has been created or added to the console, e.g. profiles, policies, users, devices.

2 Users

- Number of Users added to the Proget console
- This button takes you to the Users tab

3 Devices

- Number of Devices activated in the Proget console
- This button takes you to the Devices tab

4 Blocked devices

- Number of Blocked devices in the Proget console
- This button takes you to the Devices tab and shows blocked devices

5 Notifications

- Number of Notifications in the Proget console
- This button takes you to the Notifications

6 Out of compliance

- Number of devices out of compliance in the Proget console
- This button takes you to the Security tab

7 Operating system versions

- Interactive chart containing data on operating system versions
- Convertible to a bar chart

8**Last contact with the device**

- Interactive chart containing data on last contact with the devices in days
- Convertible to a bar chart

9**Security status**

- Interactive chart containing data on security status of the devices
- Convertible to a bar chart

10**Location of devices**

- If the location is read from the devices, they are displayed on this map
- If there are no devices with read location, the map is centered according to the country selected in the settings

My Card

Updated: Jul 16, 2026

The My card tab gives you information about a user and devices that have been assigned to him. Furthermore, it gives you the possibility to perform actions on the user and the active devices.

Example User ...

Generate activation

Show activation

LABELS

userExample Group

EMAIL ADDRESS

exampleuser@domain.com

FIRST NAME AND SURNAME

Example User

USERNAME

exampleuser

FIRST NAME

Example

SURNAME

User

TITLE

None

Devices

Attributes

Certificates

Audit logs

Backups

Settings

Dependency graph

Selected: 0

Deselect all

	MANUFACT...	MODEL	IMEI	SERIAL NUMBER	ALIAS	ACTIVATION TYPE	DEVICE LAST CONT...
☐	APPLE	iPhone 7	202000000000000	202000000000000	-	IOS	2026-05-14 11:38:23
☐	GOOGLE	Pixel XL	UNIDENTIFIED		-	Android	2026-05-14 08:41:24
☐	XIAOMI	24129PN74G	UNIDENTIFIED		-	Android Enterprise Profile Owner	2026-05-14 09:33:30
☐	SAMSUNG	SM-A236B	202100000000000	202100000000000	-	Android Enterprise Device Owner	2026-05-14 11:53:32

1

User Actions

- Available user actions
 - Generate activations
 - Send email
 - Mark as VIP
 - Manage labels
 - Reset two-factor authentication
 - Change password
 - Generate PIN
 - Certificates

2

Generate Activation

2.1 Activation template

- Select an available activation template from the dropdown list
- Available activation templates for the Android platform include:
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - Android MDM
- Required

2.2 Add activation template

- If you do not have an activation template available, you can create one using this action
- Click on the title to learn how to set it up

2.3 Need help?

- Click if you need help with device activation or want to learn what the given activation means

2.4 Generate activation

- This action allows you to generate an activation for selected platform

2.5 iOS

- Generate activation for devices with the iOS system

2.6 macOS

- Generate activation for devices with the macOS system

2.7 Windows

- Generate activation for devices with the Windows system

3 Show Activation

- Here you can view the activation, that has already been generated

4 Devices

5 Attributes

6 Certificates

7 Audit Logs

8 Backups

9 Settings

10 Dependency graph

Devices

Updated: Jun 3, 2026

Here you can view all devices assigned to your user.

Devices

Attributes

Certificates

Audit logs

Backups

Settings

Dependency graph

Selected: 0

Deselect all

	MANUFACT...	MODEL	IMEI	SERIAL NUMBER	ALIAS	ACTIVATION TYPE	DEVICE LAST CONT...
	SAMSUNG	SM-S906B	UNRECOGNIZED	UNRECOGNIZED	-	Android Enterprise Device Owner	2026-05-14 12:22:33
	APPLE	iPhone 7	UNRECOGNIZED	UNRECOGNIZED	-	IOS	2026-05-14 12:12:33
	GOOGLE	Pixel XL	UNRECOGNIZED		-	Android	2026-05-14 12:11:16
	XIAOMI	24129PN74G	UNRECOGNIZED		-	Android Enterprise Profile Owner	2026-05-14 12:15:55

1 Reset device password

- This action allows you to reset the password on the selected device

2 Send message to device

- This action allows you to send a message to the selected device

3 Send alarm message to device

- This action allows you to send an alarm message to the selected device

4 Make a report

- This action allows you to make a data report on the selected device, such as:
 - Storage memory usage report
 - Mobile data usage report
 - Wi-Fi data usage report
 - Application usage report

5 Export data

- This action allows you to export data about the selected device

6 Refresh device

- This action allows you to refresh the selected device

7 Delete device

- This action allows you to remove the device

8 List of devices

- List of devices that have been activated in the console

Attributes

Updated: Jun 3, 2026

Here you can customize the attributes view to your needs.

Devices

Attributes

Certificates

Audit logs

Backups

Settings

Dependency graph

SHOW	ATTRIBUTE	GLOBAL VARIABLE	VALUE
☒	EMAIL ADDRESS	{User:Email}	exampleuser@domain.com
☐	FIRST NAME AND SURNAME	{User:DisplayName}	Example User
☐	USERNAME	{User:Name}	exampleuser
☐	FIRST NAME	{User:FirstName}	Example
☐	SURNAME	{User:LastName}	User
☐	PRINCIPAL NAME	{User:PrincipalName}	-
☐	DISTINGUISHED NAME	{User:DistinguishedName}	-
☐	COMMON NAME	{User:CommonName}	-
☐	DIRECTORY GROUPS	{User:DirectoryGroups}	-
☐	ORGANIZATION	{User:Organization}	-
☐	COUNTRY	{User:Country}	-
☐	ORGANIZATION UNIT	{User:OrganizationUnit}	-
☐	LOCALITY	{User:Locality}	-
☐	STATE	{User:State}	-
☐	ZIP CODE	{User:ZipCode}	-
☐	ADDRESS	{User:Address}	-
☐	PHONE	{User:Phone}	-
☐	FAX	{User:Fax}	-
☐	MOBILE PHONE	{User:Mobile}	+48333000999
☐	TITLE	{User:Title}	-
☐	CUSTOM ATTRIBUTE 1	{User:CustomAttribute1}	Example value
☐	CUSTOM ATTRIBUTE 2	{User:CustomAttribute2}	Example value
☐	CUSTOM ATTRIBUTE 3	{User:CustomAttribute3}	Example value
☐	CUSTOM ATTRIBUTE 4	{User:CustomAttribute4}	Example value

1 Table of Attributes

- Provided attributes are generated based on the account data (local / LDAP / Microsoft Entra ID)
- Create your own attribute using custom attributes

Certificates

Updated: Jun 3, 2026

Here you can see the certificates that have been used by your user in profiles and application configurations.

DevicesAttributesCertificatesAudit logsBackupsSettingsDependency graph

Profile: Start typing...

Issuer: Start typing...

Validity: From SelectTo Select

Revoked: Select

Reset filters

BASICPQL

Selected: 0

Deselect all

	PROFILE	ISSUER	VALIDITY	REVOKED
>	☐ Certifikat(Template)	CA	2027-05-14 12:12:30	-

1 Renew Certificate

- This action allows you to renew the selected certificate

2 Revoke Certificate

- This action allows you to revoke the selected certificate
- The revocation of a certificate will result in the discontinuation of functionality, that uses that certificate
- The selected action is irreversible

3 List of certificates

- List of certificates, containing the main information found in the user certificate

Audit Logs

Updated: Jun 3, 2026

Here you can see all the logs related to your user.

DevicesAttributesCertificatesAudit logsBackupsSettingsDependency graph

Action: SelectStatus: SelectDate of occurrence: From SelectTo Select

Reset filtersBASICPQL

ACTION	STATUS	DATE OF OCCURRENCE	PERFORMED ON	DETAILS
user.backup.qr.generate	Success	2026-05-14 12:18:58	Example User (exampleuse...	Backup QR code generated
user.backup.qr.generate	Success	2026-05-14 12:13:21	Example User (exampleuse...	Backup QR code generated
user.attribute.update	Success	2026-05-14 12:09:11	Example User (exampleuse...	User attribute customAttribute4 updated
user.attribute.update	Success	2026-05-14 12:09:08	Example User (exampleuse...	User attribute customAttribute3 updated
user.attribute.update	Success	2026-05-14 12:09:05	Example User (exampleuse...	User attribute customAttribute2 updated

1

List of audit logs

- History of system events generated by specific user actions, by:
 - System
 - User
 - Mobile device

Backups

Updated: Jun 3, 2026

Here you can create and view your user backups

DevicesAttributesCertificatesAudit logsBackupsSettingsDependency graph

Selected: 0Deselect all

Generate QR code

☐	DEVICE	ID	DATE
☐	SAMSUNG SM-S906B	20bc7219-227f-4629-82e9-eb15c2e67659	2026-05-14 12:22
☐	SM-A236B	-	2026-05-14 12:14

1

Delete backups

- This action allows you to delete backups

2

Generate QR code

- After clicking this button, a window will appear with the option to select the user for whom the QR code should be generated to make a backup copy

3

List of backups

- List of backups that have been created

Settings

Updated: Jun 3, 2026

Here you can view and edit basic information about your user and personalize your console.

DevicesAttributesCertificatesAudit logsBackupsSettingsDependency graph

* First name:

Example

* Surname:

User

* Email:

exampleuser@domain.com

* Username:

exampleuser

Theme:

Light

Submit

1 First name

- User first name
- Required

2 Surname

- User surname
- Required

3 Email

- User email
- Required

4 Username

- Username
- Required

5 Theme

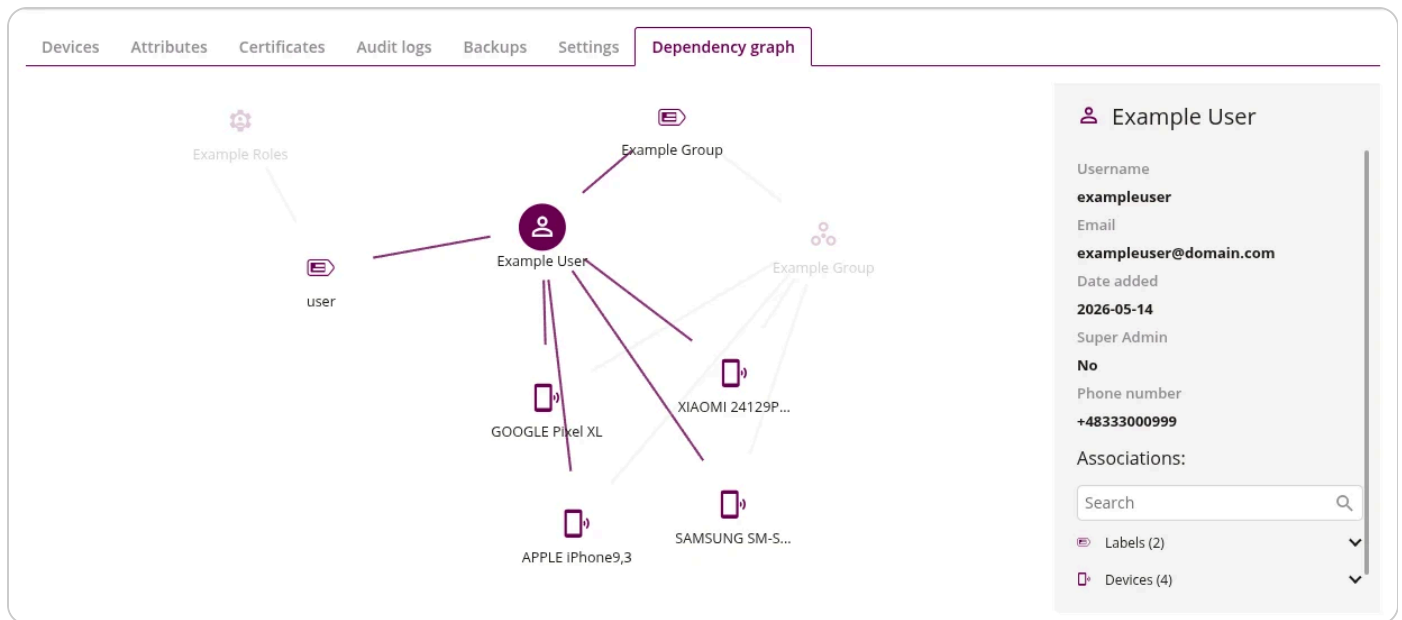
- Type of themes
 - Light
 - Dark
 - Automatic

Dependency graph

Updated: Jun 3, 2026

NEW

The Dependency graph tab displays an interactive visualization of relationships between key system elements such as labels, groups, users, devices, roles and directory integrations (LDAP/Entra). It allows administrators to quickly understand how individual elements are interconnected, without navigating between multiple views. The feature is currently available for super admins only.



1 Graph

- Interactive graph showing the selected entity as the central node with connected elements displayed around it
- Connected elements include devices, groups, roles, labels and directory integrations
- Click on a node to view its details in the side panel
- Nodes with a number represent aggregated elements - click to expand them into individual nodes

2 Details panel

- Side panel showing detailed information about the selected element, such as username, email, date added, super admin status, and phone number
- Associations section lists related elements grouped into accordion categories (e.g. Labels, Devices, Groups, Users, Roles)
- Use the search field to filter associations
- Click on an element to navigate to its detailed view in the system

Users

Updated: Jul 16, 2026

In the users tab you will find a table with information about users on the given server. Here you can perform actions on multiple or single users and also add users to the system from Microsoft Entra ID, LDAP or locally.

7 Assign labels

- This action allows you to associate selected user with a selected label

8 Unassign labels

- This action allows you to remove the association of the selected user with the selected label

9 Reset two factor authentication

- This action allows you to reset two factor authentication for the selected user

10 Lock user

- This action allows you to lock selected user

11 Unlock user

- This action allows you to unlock selected user

12 Assign Super Admin function

- This action allows you to assign Super Admin function to selected user

13 Unassign Super Admin function

- This action allows you to unassign Super Admin function from selected user

14 Certificates

- This action allows you to add external certificates to the user

15 Reset password

- This action allows you to reset the password of selected local user

16 Manage user

- This action allows you to manage selected user, e.g. change name, email, username and reset password

17 Generate PIN

- This action allows you to generate PIN for the selected user and export it

18 Export data

- This action allows you to export data about selected user

19 Delete user

- This action allows you to delete selected user

20 Add user

- Available options for adding a user to the Proget console

20.1 Add user from Microsoft Entra ID

20.2 Add user from LDAP

20.3 Add local user

21 User Backups

- This action will take you to a page where you can send a backup of your private device to the server

22 List of users

- List of all users that were added to the Proget console

Add user from Microsoft Entra ID

Updated: Dec 3, 2024

Add users to the system from Microsoft Entra ID. Microsoft Entra ID is a cloud service that provides administrators with the ability to manage end-user identities and access privileges.

From Microsoft Entra ID

Labels:

Select

Message language:

Do not send

Selected: 0

Deselect all

Add

Select file

☐	EMAIL	USERNAME	FIRST NAME	SURNAME	PHONE NUMBER	MICROSOFT ENTRA ID
No data available						

Results: 0

Page limit: 50

<<

<

1

>

>>

1 Labels

- Select the labels with which you want to associate new users

2 Message language

- Select the language of tin which the message will be sent to the user
- For this feature to work properly, SMTP must first be configured in the Settings tab

3 Delete

- This action allows you to delete selected user

4 Add user

4.1 User in Microsoft Entra ID

- Search for the user in Microsoft Entra ID by email

5 Select file

- Select file with the list of users you want to add to the Proget console
- Allowed file type: csv

6 Download the sample CSV

- This action allows you to download the sample CSV file

Add user from LDAP

Updated: Dec 3, 2024

Add users to the system from LDAP. LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate data about organizations, individuals and other resources such as files and devices in a network.

From LDAP

Labels:
Select

Message language:
Do not send

Selected: 0 | Deselect all

Add | Select file

	EMAIL	USERNAME	FIRST NAME	SURNAME	PHONE NUMBER	LDAP
No data available						

Results: 0 | Page limit: 50

1 Labels

- Select the labels with which you want to associate new users

2 Message language

- Select the language of tin which the message will be sent to the user
- For this feature to work properly, SMTP must first be configured in the Settings tab

3 Delete

- This action allows you to delete selected user

4 Add user

4.1 User in LDAP

- Search for the user in LDAP by email

5 Select file

- Select file with the list of users you want to add to the Proget console
- Allowed file type: csv

6 Download the sample CSV

- This action allows you to download the sample CSV file

Add local user

Updated: Dec 3, 2024

Add local users to the system.

Local

Labels:

Select

Message language:

Do not send

Selected: 0

Deselect all

Remove duplicates

Add

Select file

☐	FIRST NAME	SURNAME	EMAIL	USERNAME	PHONE NUMBER	ACTIONS
No data available						

Results: 0

Page limit: 50

<<

<

1

>

>>

1 Labels

- Select the labels with which you want to associate new users

2 Message language

- Select the language of tin which the message will be sent to the user
- For this feature to work properly, SMTP must first be configured in the Settings tab

3 Delete

- This action allows you to delete selected user

4 Remove duplicate

- This action allows you to remove duplicate users who have the same data when being added

5 Add user

5.1 First name

- Enter first name of the new user

5.2 Surname

- Enter surname of the new user

5.3 Email

- Enter email of the new user

5.4 Username

- Enter username of the new user

5.5 Phone number

- Enter phone number of the new user

6 Select file

- Select file with the list of users you want to add to the Proget console
- Allowed file type: csv

7 Download the sample CSV

- This action allows you to download the sample CSV file

User Backups

Updated: Dec 3, 2024

Here you will be able to send a backup of your private Android device to the server even if it is not activated in the Proget service.

Backups

Created at: From Select To Select

User: Start typing...

Device identifier: Start typing...

Reset filters

Selected: 0

Deselect all

Generate QR code

☐	USER	DEVICE IDENTIFIER	CREATED AT
☐	John Doe	-	2024-08-14 14:16
☐	John Doe	-	2024-08-14 14:16
☐	John Doe	-	2024-08-14 14:15

Results: 3 | Page limit: 50

1

1

Delete

- This action allows you to remove selected backups from the list

2

Generate QR Code

2.1

Enter the user name

- Enter the name of the user for whom the backup will be sent to the server. Then click on the 'Generate' button
- Required

3 List of backups made

- List of backups performed by the user

Generated QR code of backup

1 QR Code

- To send a backup to the server scan the QR code with your private Android device

Activations

Updated: Jul 16, 2026

Click on the selected activation method to view details and adjust settings.



Manual activation

Manually deploy a device with a chosen activation type



Device auto enrollment

Speed up activating multiple devices automatically



Templates

Predefined settings for quickly creating activations



Custom EULA

Custom agreement text shown to users during activation

Manual

Updated: Oct 9, 2025

Manual activation gives you the ability to manually deploy the device with the selected activation type, for the selected user or without user.

Identifier: Start typing...

Created at: From Select To Select

Expiration date: From Select To Select

+

Reset filters

BASICPQL

Selected: 0 | Deselect all

Generate activation

☐	IDENTIFIER	CREATED AT	EXPIRATION DATE	ACTIVATION TYPE	CREATED BY	CREATED FOR
☐	12345-67890	2025-05-21 07:46:59	2025-05-22 07:46:59	Windows	Example Example	Example Example
☐	98765-43210	2025-05-21 07:46:40	2025-05-22 07:46:40	Android Enterprise Device Owner	Example Example	
☐	54321-09876	2025-05-21 07:46:35	2025-05-22 07:46:35	Android Enterprise Profile Owner	Example Example	
☐	21098-76543	2025-05-21 07:46:31	2025-05-22 07:46:31	Android	Example Example	
☐	87654-32109	2025-05-21 07:46:27	2025-05-22 07:46:27	iOS	Example Example	
☐	65432-10987	2025-05-21 07:46:23	2025-05-22 07:46:23	macOS	Example Example	

1 Filter of generated activations

- Use available filters to search for activations, such as:
 - Identifier
 - Created at
 - Expiration date
 - Activation type
 - Created by
 - Created for

2 Show

- This action allows you to preview the available activation selected from the list

3 Delete

- This action allows you to remove one or more activations if selected
- This action is irreversible

4 Generate activations

4.1 Activation template

- Select an available activation template from the dropdown list
- Available activation templates for the Android platform include:
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - Android MDM
- Required

4.2 Add activation template

- If you do not have an activation template available, you can create one using this action

4.3 Without user

- If this option is selected, the activation will be generated without user
- The activated device will not be assigned to any user in the MDM system

4.4 With user

- If this option is selected, you must specify the user to whom the activation will be assigned during generation
- After activation, the device will be assigned to that user in the MDM system

4.5 Activation count

- The slider is available only when the **Without user** option is selected
- Allows you to define the number of activations to be generated, from 1 to 100
- The **Without user** option is required

4.6 Need help?

- Click if you need help with device activation or want to learn what the given activation means

4.7 Generate activation

- This action allows you to generate an activation with the entered settings

4.8 iOS

- Generate activation for devices with the iOS system

4.9 macOS

- Generate activation for devices with the macOS system

4.10 Windows

- Generate activation for devices with the Windows system

5 List of activations

- List of generated activations, containing main information

Automatic

Updated: Oct 13, 2025

The auto enrollment feature significantly increases the speed and streamlines the process of activating multiple devices.

Device auto enrollment

Serial number / IMEI: Start typing...

Activation type: Select

User: Start typing...

Status: Select

+

Reset filters

Selected: 0

Deselect all

Add devices

Import CSV

☐	CREATED AT	SERIAL NUMBER / IMEI	INTEGRATION TYPE	ACTIVATION TYPE	USER	ALIAS	POLICY	STATUS	ENROLLED
☐	2024-08-27 11:37:46	24-08-27 11:37:46	Proget	Android Enterprise Device Owner	John Doe			Added	No
☐	2024-08-27 11:37:28	24-08-27 11:37:28	Proget	iOS	John Doe	Example alias		Added	No

Results: 2

Page limit: 50

<<

<

1

>

>>

1 Filtering in a text window

- You can also filter the results using keywords. Enter the keyword you want to filter by into the according field. The results are filtered dynamically while entering text.

2 Update registration

- Click on the button if you want to make changes for the added activation

3 Delete registration

- Click on the button if you want to delete added activation

4 Add devices

4.1 Integration type

- Select the type of integration:
 - Proget - allows automatic registration of the device after installing the application
 - KME - allows automatic registration of the device along with the installation of the application. Available only on Samsung devices

4.2 Add devices by

- Select the type of device adding:
 - IMEI
 - Serial number

4.3 Assign activation template

- This action allows you to assign an activation template to the selected devices from the list

4.4 Assign policy

- This action allows you to assign a policy to the selected devices from the list

4.5 Assign action after activation

- This action allows you to assign reactions after activating the device in the console, such as:
 - No action
 - Unlink the user from automatic enrollment

4.6 Remove

- This action allows you to remove the added device

4.7 IMEI/Serial Number

- Enter the device identification number

4.8 User

- Enter the user to whom the added device will be assigned

4.9 Activation template

- Assign an activation template for device enrollment

4.10 Policy

- Assign a policy for device enrollment

4.11 Action after activation

- Assign an action to be performed after device activation

4.12 Alias

- Enter an alias for the device

4.13 Add

- Add a new device enrollment

5 Import CSV

5.1 Integration type

- Select the type of integration:
 - Proget - automatic registration of the device after installing the application
 - KME - automatic registration of the device along with the installation of the application.
Available only on Samsung devices

5.2 Add devices by

- Select the type of device adding:
 - IMEI
 - Serial number

5.3 Activation template

- Assign an activation template for device enrollment

5.4 Policy

- Assign a policy that will be imposed on the device during registration

5.5 Assign action after activation

- This action allows you to assign reactions after activating the device in the console, such as:
 - No action
 - Unlink the user from automatic enrollment

5.6 Select file

- This action allows you to add file in order to import devices

- Required

5.7 Download the sample CSV

- This action allows you to download the sample CSV
- This file contains a sample IMEI, user email, registration type and alias

6 Devices list

- List of devices added to auto enrollment
- List of information about the added devices and current status

Templates

Updated: Jun 3, 2026

Activation templates allow you to quickly create activations with predefined settings.

Name: Start typing...

Type: Select

Custom EULA: Select

Reset filters

BASIC

PQL

Selected: 0

Deselect all

Add

☐	NAME	TYPE	CUSTOM EULA	AUTO ENROLLMENT	MICROSOFT ENTRA ID	LDAP
☐	Custom Template - Android	Android	Example Eula	0	0	0
☐	Custom Template - Android Enterprise Device Owner	Android Enterprise Device Owner		0	0	0
☐	Custom Template - Android Enterprise Profile Owner	Android Enterprise Profile Owner		0	0	0
☐	Custom Template - iOS	iOS		0	0	0
☐	Custom Template - macOS	macOS		0	0	0
☐	Custom Template - Windows	Windows		0	0	0

1Filter of created templates

- Use available filters to search for templates, such as:
 - Name
 - Type
 - Custom EULA

2Copy

- This action allows you to duplicate already existing templates in the console
- You cannot copy a template with the same name

3Edit

- This action allow you to edit chosen template from the list

4Delete

- This action allow you to delete chosen template from the list
- Multiple deletions are allowed

5 Add

- This action allows you to add a new template

6 List of templates

- List of all created templates with their parameters

Template configuration

Updated: Jul 16, 2026

Here you can configure the activation template according to your needs by selecting the activation type for Android, Apple iOS, Apple macOS or Windows devices

* Name:

Custom Template - Android Enterprise Device Owner

Activation type:

Android Enterprise Device Owner

SECURITY

☐ Allow multiple device activations ⓘ

☒ Limit the number of days for activation

No of days for activation:

1

No of activation attempts:

3

Generated identifier length:

8

Generated password length:

4

ACTIVATION MESSAGE

* Deliver activation by email: ⓘ

Ask while generating activation

* Topic:

Android Enterprise Device Owner - Activation Message

* Message:

B

I

U

S

≡

≡

≡

2

↔

↶

↷

↻

</>

Default message

The following instruction will help you activate your Android mobile device in Device Owner mode on Proget. Follow the steps described below:
 Server address: **{Server:hostname}**
 User e-mail address: **{User:Email}**
 Activation password: **{Activation:PIN}**
 Activation expiration date: **{Activation:PINExpirationDate}**

SETTINGS ON THE DEVICE

General

Custom EULA:

Example Eula

X

▼

Android Enterprise

☐ Leave all system apps enabled ⓘ

☒ Add a Wi-Fi connection to the QR code

* SSID:

Example

☐ Hidden network

Security type:

Personal WPA

* Preshared key:

👁

Back

Submit

1 Name

- Enter the name of the Template
- Maximum length of the text is 255

2 Activation type

- Chose the type of activation, such as
 - Android Enterprise Device Owner

- Android Enterprise Profile Owner
- Android
- iOS
- macOS
- Windows

3 Security settings

3.1 Allow multiple device activations

- If checked, this function allows multiple devices to be activated on the Proget system. If unchecked, activation is removed when the first device is deployed

3.2 Limit the number of days for activation

- If checked, you can declared the number of days for activation

3.3 No of days for activation

- Select the number of days for activation

3.4 No of activation attempts

- Select how many times the generated activation will be possible to use

3.5 Generated identifier length

- Select the length of the identifier which will be generated during activation

3.6 Generated password length

- Select the length of the password which will be generated during activation

4 Activation message settings

4.1 Deliver activation by email

- Chose the option deliver activation by email, such as:
 - Do not send
 - Ask while generating activation
 - Send
- For this feature to work properly, SMTP must first be configured in the Settings tab

4.2 Topic

- Enter the topic of activation email
- Maximum length of text is 255
- Required if **Do not send** is not chosen

4.3 Message

- Enter the text of activation email
- Required if **Do not send** is not chosen

5 Settings on the device with Android system

5.1 Custom EULA

- If created, you are allowed to set your own custom EULA for this activation
 - To learn how to create a custom EULA, click the title

5.2 Leave all system apps enabled

- If checked, the feature allows to keep the system apps enabled on the device added to the Proget system
- Available on Android Enterprise Profile Owner and Android Enterprise Device Owner when deployed via Enterprise QR codes

5.3 Add a Wi-Fi connection to the QR code

- If checked, the device will be automatically connected to the network
- The QR code will contain an unencrypted Wi-Fi password

5.4 SSID

- Enter the name that identifies the wireless network
- Required

5.5 Hidden network

- Required if the network for which we prepare configuration hides the SSID

5.6 Security type

- One of:
 - None
 - Personal WPA
- If **None** is chosen, the network will be without security
- If **Personal WPA/WPA2** is chosen, user authentication management is via WPA pre-shared key

5.7 Preshared key

- Enter the preshared key to authenticate into Wi-Fi
- Available if **Security type: Personal WPA** is chosen

6 Settings on the device with iOS and macOS system

6.1 Custom EULA

- If created, you are allowed to set your own custom EULA for this activation
 - To learn how to create a custom EULA, click the title

6.2 Enable declarative management

- If selected, the user and administrator gain additional features such as:
 - Benefits for the organization:
 - Easier enforcement of software updates
 - Dynamic and scalable management
 - Increased data security through policy and settings management
 - Benefits for the end user:
 - Smoother operation of the device's operating system
 - Devices maintain independence from the network, keep the required state on their own, and automatically reconfigure once the connection is restored
- Required iOS version 16 or later
- Required macOS version 13 or later

6.3 Show Proget Store icon

- If selected, the Proget Store icon will be displayed on the device

6.4 Allow device wipe

- If selected, you are allowed to wipe your non-supervised device
- Does not apply to devices deployed by ABM

6.5 Allow inspection of installed applications

- If selected, applications from your non-supervised device will be visible to the Proget console administrator

- Does not apply to devices deployed by ABM

Custom EULA

Updated: Jun 3, 2026

The content of the agreement that will be displayed to the user during the device activation process. The user must accept it to complete device enrollment.

Name:

[Reset filters](#)

BASIC [PQL](#)

Selected: 0 | [Deselect all](#)

[Add](#) 

☐	NAME ▾	ACTIVATIONS	ACTIVATION TEMPLATES	DEVICES
☐	Example Eula	1	2	1

1 Filter of created custom EULAs

- Use available filters to search for custom EULA, such as:
 - Name

2 Copy

- This action allows you to duplicate already existing EULA in the console
- You cannot copy a EULA with the same name

3 Edit

- This action allow you to edit chosen EULA from the list

4 Delete

- This action allow you to delete chosen EULA from the list
- Multiple deletions are allowed

5 Add

- This action allows you to add a new custom EULA

6 List of custom EULAs

- List of all created EULAs with their parameters

EULA configuration

Updated: Jun 3, 2026

Here you can define a custom EULA by specifying its name, title, and the content that will be displayed on the device during activation.

* Name:

Example Eula

* Title:

Example Title

* Content:

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

(577 / 200000 chars)

1 Name

- Enter the name of the custom EULA
- Maximum length of the text is 255

2 Title

- Enter the title of EULA
- Maximum length of the text is 64

3 Content

- Enter the EULA content
- Maximum length of the text is 200000

Devices

Updated: Jul 16, 2026

The device tab shows a table with information about devices activated on the given server.

IMEI:

Serial number:

User:

Security status: Select

+

Reset filters

BASIC PQL

Selected: 0

...

Generate activation

▼

☐	MANUFACTURER ▼	MODEL ▼	SYSTEM VERSION ▼	ACTIVATION TYPE ▲
☐	SAMSUNG	SM-A236B	Android 14	Android Enterprise Device Owner
☐	XIAOMI	24129PN74G	Android 16	Android Enterprise Profile Owner
☐	GOOGLE	Pixel XL	Android 10	Android
☐	APPLE	iPhone 7	iOS 15.8.7	iOS
☐	APPLE	Mac14,7	macOS 26.2	macOS
☐	Innotek GmbH	VirtualBox	Windows 10 Enterprise Evaluation	Windows

1 Filtering in a text window

- You can also filter the results, using keywords. Enter the keyword you want to filter by into the according field. The results are filtered dynamically when entering text.

2 Quick actions

2.1 Add to Apple Business Manager profile

- This action allows you to assign the selected device to the Apple Business Manager profile

2.2 Remove association with Apple Business Manager

- This action allows you to delete the selected device from the Apple Business Manager profile

2.3 Send Custom Apple Command

- This action allows you to send a Custom Apple Command to the device

2.4 Enable declarative management

- This action allows you to enable declarative management on an iOS or macOS device

2.5 Add Android Enterprise account

- This action allows you to add an Android Enterprise account to the selected device

2.6 Delete Android Enterprise account

NEW

- This action allows you to remove an Android Enterprise account on the selected device

2.7 Check Android Enterprise status

- This action allows you to check the Android Enterprise account status on the selected device

2.8 Assign user

- This action allows you to assign a user to the selected device

2.9 Unassign user

- This action allows you to unassign a user from the selected device

2.10 Lock device screen

- This action allows you to lock the screen on the selected device

2.11 Enable Activation Lock

- This action allows you to enable Activation Lock on the selected devices

2.12 Disable Activation Lock

- This action allows you to disable Activation Lock on the selected devices

2.13 Reset device password

- This action allows you to reset password on the selected device

2.14 Send message to device

- This action allows you to send a message to the selected device
 - Basic text formatting support (including bold and italic) as well clickable links to: **NEW**
 - websites '(https://...)'
 - phone calls '(tel://...)'
 - specific apps via deep links '(myapp://...)'

2.15 Send alarm message do device

- This action allows you to send an alarm message to the selected device

2.16 Make a report

- This action allows you to make a data report on the selected device, such as:
 - Storage memory usage report
 - Mobile data usage report
 - Wi-Fi data usage report
 - Application usage report

2.17 Export data

- This action allows you to export data about the selected device

2.18 Refresh device

- This action allows you to refresh the selected device

2.19 Update apps

- This action allows you to update all apps on the selected devices

2.20 Set ownership

- This action allows you to set an ownership status of the device, such as:
 - Private
 - Business
 - COPE

2.21 Delete device

- This action allows you to remove the device

3 Generate activation

- After clicking the button, you will be transferred to the manual activation page, where you will be able to generate an activation

4 Device table

4.1 Android Enterprise Device Owner Activation

4.2 Android Enterprise Profile Owner (COPE) Activation

4.3 Android Activation

4.4 iOS (Supervised mode) Activation

4.5 macOS Activation

4.6 Windows Activation

Activations

Updated: Jul 16, 2026

Click on the activation you are interested in for details.



Android Enterprise Device Owner Activation

Requires a factory-reset device to activate



Android Enterprise Profile Owner (COPE) Activation

Extended management for Android 11+ factory-reset devices



Android Activation

Simplest activation type with basic remote management



iOS (Supervised mode) Activation

Extended device control, requires Apple Business Manager setup



macOS Activation

Activate and configure restrictions on macOS devices



Windows Activation

Activate and configure restrictions on Windows devices

1 Generale information

1.1 Enter device alias

- This action allows you to set the device alias. Alias can help with identifying the device

1.2 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

1.3 Generate service password

- This action allows you to generate a service password for the device on which the lost mode has been imposed

2 Quick actions

2.1 Block device

- This action allows you to send an action to block the device. When device is blocked, user can only call the administrator or emergency number which is entered during "Block device" action

2.2 Unlock Device

- This action allows you to send an action to unlock the device

2.3 Remote desktop

- To use this action you need app Proget Remote to be installed on your device. Proget Remote is an application that allows you to remotely access your Android device screen from Proget server

2.4 Reset password

- This action allows you to send an action to the device that will trigger a password reset request

2.5 Change password

- This action allows you to send an action to the device to set a new password on the device

2.6 Wipe device

- This action allows you to restore factory settings

2.7 Wipe company data

- This action allows you to wipe company data. After performing this action device that is registered in the Proget console will be deleted and further management of this device won't

be possible. Proget applications will be still visible and another registration in the Proget console will be possible

2.8 Lock device screen

- This action allows you to send an action to the device that will lock device screen

2.9 Send message

- This action allows you to send a message. While performing this action administrator can choose how the message will be visible on the device

2.10 Send alert

- This action allows you to send an alert message. While performing this action administrator must set message content and can choose additional options. Alert message will be immediately visible on the device with characteristic sound and user will be forced to accept that he read the message

2.11 Forward phone calls

- This action allows you to send an action to forward phone calls to a given phone number

2.12 Delete forward phone calls

- This action allows you to send an action to delete the number to which the calls were forwarded

2.13 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

2.14 Reboot device

- This action allows you to send an action to the device to reboot the device

2.15 Enable kiosk

- This action allows you to send an action to the device to enable the kiosk profile. The action is available when a kiosk profile is added to the device

2.16 Disable kiosk

- This action allows you to send an action to the device to disable the kiosk profile. The action is available when a kiosk profile is added to the device

2.17 Verify the device

- This action allows you to verify device compatibility with Play Integrity policy

2.18 Generate an event log

- This action allows you to generate and send audit logs to Proget server

3 Tables

3.1 Details

3.2 Policy

3.3 Profiles

3.4 Applications

3.5 Location

3.6 Backups

3.7 Audit log

3.8 Tasks

3.9 Dependency graph

3.10 File Manager

3.11 Reports

3.12 Export

3.13 User accounts

3.14 System bug reports

3.15 Photos during device lock

3.16 Users

Service password

Updated: Jun 9, 2026

NEW

The Service password panel allows the administrator to generate an emergency service password for the device. The password is linked to a specific device and has a defined validity period (default 24 hours, minimum 5 minutes, maximum 30 days). It works even when the device is in Lost Mode, Kiosk, has no internet connection, or the local database is damaged. After use, the device enters a 60-minute privileged window, after which it returns to the state required by policies. The password can be entered manually or scanned as a QR code on the device.



Service password

* Select actions: ⓘ

- ☐ Unblock device
- ☐ Disable Kiosk
- ☐ Remove network restrictions ⓘ
- ☐ Allow developer options
- ☐ Allow deactivation
- ☐ Allow factory reset
- ☐ Emergency Database Reset ⓘ
- ☐ Set Password ⓘ

* Service password expiration date (on device):

2026-05-07 10:23



Time to expire: in about 24 hours

- ☒ Generate QR code
- ☒ Send service password via email

* Email:

example@domain.com

Message language:

English



Cancel

Generate

1 Unlock device

- If checked, the service password will unlock the device from Lost Mode

2 Disable Kiosk

- If checked, the service password will exit the device from Kiosk mode

3 Remove network restrictions

- If checked, the service password will temporarily remove network restrictions on the device
 - The action removes restrictions imposed by network-related policies:
 - Allow configuring mobile networks
 - Allow mobile data usage while roaming

- Allow tethering configuration and mobile hotspots
- Allow edit Wi-Fi configuration
- Specify settings for Wi-Fi sleep configuration (Keep Always)
- Allow removing added Wi-Fi networks
- Allow private DNS configuration

4 Allow developer options

- If checked, the service password will temporarily enable developer options on the device

5 Allow deactivation

- If checked, the service password will allow deactivation of the Proget MDM application on the device

6 Allow factory reset

- If checked, the service password will allow the user to perform a factory reset on the device

7 Emergency Database Reset

- If checked, the service password will authorize an emergency reset of the Proget MDM application database on the device
 - Use the service password in the Proget application in case of an application synchronization error
- It cannot be combined with other actions

8 Set Password

- If checked, the service password will allow setting a new device password in the Direct Boot scenario (after device restart)
 - Use the service password if you forget the device PIN. To do this, restart the device, tap the Proget notification, enter the generated service password, and set a new password on the device. The service password depends on the 'Lock screen notifications' policy settings.

- It cannot be combined with other actions

9 Service password expiration date (on device)

- Set the date and time when the service password will expire on the device
- Default validity is 24 hours, minimum 5 minutes, maximum 30 days

10 Generate QR code

- If checked, a QR code will be generated along with the service password for easier scanning on the device

11 Send service password via email

- If checked, the generated service password will be sent to the specified email address

12 Email

- Enter the email address to which the service password will be sent
- Required if 'Send service password via email' is checked

13 Message language

- Select the language in which the email message with the service password will be sent

14 Generate

14.1 Service password generated for device

- Displays the generated service password for the device
- The password can be copied to clipboard using the copy icon

14.2 QR code

- Displays the QR code containing the service password for scanning on the device
- Visible only if 'Generate QR code' was checked

Android Enterprise Profile Owner (COPE)

Updated: Jul 16, 2026

Android Enterprise Profile Owner is a type of activation in which all actions are performed in the area of the device's service space. This activation allows basic management of the devices workspace.

Android Enterprise Profile Owner (COPE) activation allows the use of extended functions limiting and configuring the device. It can only be activated on Android devices with Android 11 or higher which have been reset to the factory settings.

SAMSUNG SM-A225F

User:

Example User

Activation type:

Android Enterprise Profile Owner (COPE)

Alias:

Enter device alias

Last contact:

2026-05-22 11:48:37

Battery level: 69%

Health: Good

Internal storage: 5.2%

Total: 49.59 GiB (53.25 GB) Free: 47.01 GiB (50.48 GB)

RAM: 56.03%

Total: 3.63 GiB (3.89 GB) Free: 1.60 GiB (1.71 GB)

Generate service password

Details

Policy

Profiles

Applications

Location

Backups

Audit logs

Tasks

Dependency graph

File Manager

Reports

User accounts

Technical data

Manufacturer:

SAMSUNG

Model:

SM-A225F

OS:

Android 13 (33)

Serial number:

808F73MPCN6A

IMEI 1:

359467626779677

IMEI 2:

359467626779678

Proget ID:

855 104

Activation date:

2026-05-22 11:44:17

App version:

2.20.1 (1201)

Patch version:

TP1A.220624.014.A225FXXSBDYE1

Bootloader version:

A225FXXSBDYE1

Security patch:

2025-05-01

System update status:

No info

CPU:

Mediatek MT6769V/CT (arm64-v8a)

Connection type:

Wi-Fi

IP:

192.168.3.142

Wi-Fi SSID:

<unknown ssid>

Roaming:

✗

Data encryption:

✓

Access to device usage data:

✓

Android Enterprise status:

Registered

Google Play services:

✓

Remote password change on the device:

✓

Access to background activity:

✓

Access to Wi-Fi management:

✓

Runtime permissions:

✓ Telephone ✗ SMS ✓ Call log ...

Groups

Example Group

Security

✗ 0

⚠ 0

✓ 2

ℹ 0

Root status 2026-05-22 11:44:18

Play Integrity verification status 2026-05-22 11:44:25

1

Generale information

1.1 Enter device alias

- This action allows you to set the device alias. Alias can help with identifying the device

1.2 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

1.3 Generate service password

- This action allows you to generate a service password for the device on which the lost mode has been imposed

2 Quick actions

2.1 Remote desktop

- To use this action you need app Proget Remote to be installed on your device. Proget Remote is an application that allows you to remotely access your Android device screen from Proget server

2.2 Change company password

- This action allows you to send an action to the device to set a new password on the container

2.3 Wipe device

- This action allows you to restore factory settings

2.4 Wipe company data

- This action allows you to wipe company data. After performing this action device that is registered in the Proget console will be deleted and further management of this device won't be possible. Proget applications will be visible and another registration in the Proget console will be possible

2.5 Lock device screen

- This action allows you to send an action to the device that will trigger lock device screen

2.6 Send message

- This action allows you to send a message. While performing this action administrator can choose how the message will be visible on the device

2.7 Send alert

- This action allows you to send an alert message. During performing this action administrator must set message content and can choose additional options. Alert message will be immediately visible at phone with characteristic sound and user will be forced to accept that he read the message

2.8 Forward phone calls

- This action allows you to send an action to forward phone calls to a given phone number

2.9 Delete forward phone calls

- This action allows you to send an action to delete the number to which the calls were forwarded

2.10 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

2.11 Force device password change

- This action allows you to send an action to the device that will trigger a password reset request

2.12 Force company password change

- This action allows you to send an action to the device that will trigger a password change request

2.13 Container lock reset

- This action allows you to reset container lock. After performing this actions user will be forced to re-enter the password in the work space.

2.14 Lock workspace

- This action allows you to send an action to the device that will lock the work space

2.15 Unlock workspace

- This action allows you to send an action to the device that will unlock the work space

2.16 Verify the device

- This action allows you to verify device compatibility with Play Integrity policy

2.17 Generate an event log

- This action allows you to generate and send audit logs to Proget server

3 Tables

3.1 Details

3.2 Policy

3.3 Profiles

3.4 Applications

3.5 Location

3.6 Backups

3.7 Audit log

3.8 Tasks

3.9 Dependency graph

3.10 File Manager

3.11 Reports

Service password

Updated: Jun 9, 2026

NEW

The Service password panel allows the administrator to generate an emergency service password for the device. The password is linked to a specific device and has a defined validity period (default 24 hours, minimum 5 minutes, maximum 30 days). It works even when the device has no internet connection or the local database is damaged. On COPE activation, the 'Unlock device' action unlocks the work space (not the entire device), and the Kiosk profile is not available. The 'Set Password' option works differently than on Device Owner - the code is generated independently (without QR), only the expiration date can be selected (not the time), and the code is valid for the entire selected day (max 1 use per day). After use, the device enters a 60-minute privileged window, after which it returns to the state required by policies. The password can be entered manually or scanned as a QR code on the device.



Service password

* Select actions: ⓘ

- ☐ Unblock device
- ☐ Disable Kiosk
- ☐ Remove network restrictions ⓘ
- ☐ Allow developer options
- ☐ Allow deactivation
- ☐ Allow factory reset
- ☐ Emergency Database Reset ⓘ
- ☐ Set Password (COPE only) ⓘ

* Service password expiration date (on device):

2026-05-07 11:05



Time to expire: in about 24 hours

- ☒ Generate QR code
- ☒ Send service password via email

* Email:

example@domain.com

Message language:

English



Cancel

Generate

1 Unlock device

- If checked, the service password will unlock the device from Lost Mode

2 Disable Kiosk

- If checked, the service password will exit the device from Kiosk mode

3 Remove network restrictions

- If checked, the service password will temporarily remove network restrictions on the device
 - The action removes restrictions imposed by network-related policies:
 - Allow configuring mobile networks
 - Allow mobile data usage while roaming

- Allow tethering configuration and mobile hotspots
- Allow edit Wi-Fi configuration
- Specify settings for Wi-Fi sleep configuration (Keep Always)
- Allow removing added Wi-Fi networks
- Allow private DNS configuration (COPE only)

4 Allow developer options

- If checked, the service password will temporarily enable developer options on the device

5 Allow deactivation

- If checked, the service password will allow deactivation of the Proget MDM application on the device

6 Allow factory reset

- If checked, the service password will allow the user to perform a factory reset on the device

7 Emergency Database Reset

- If checked, the service password will authorize an emergency reset of the Proget MDM application database on the device
 - Use the service password in the Proget application in case of an application synchronization error
- It cannot be combined with other actions

8 Set Password (COPE only)

- If checked, the service password will allow setting a new device password in the Direct Boot scenario (after device restart)
 - Use the service password if you forget the device PIN. To do this, restart the device, tap the Proget notification, and enter the generated service password.
- It cannot be combined with other actions

9 Service password expiration date (on device)

- Set the date and time when the service password will expire on the device
- Default validity is 24 hours, minimum 5 minutes, maximum 30 days

10 Generate QR code

- If checked, a QR code will be generated along with the service password for easier scanning on the device

11 Send service password via email

- If checked, the generated service password will be sent to the specified email address

12 Email

- Enter the email address to which the service password will be sent
- Required if 'Send service password via email' is checked

13 Message language

- Select the language in which the email message with the service password will be sent

14 Generate

14.1 Service password generated for device

- Displays the generated service password for the device
- The password can be copied to clipboard using the copy icon

14.2 QR code

- Displays the QR code containing the service password for scanning on the device
- Visible only if 'Generate QR code' was checked

Android

Updated: Jul 16, 2026

Android is the simplest type of activation that allows you to manage the device space from the Proget console. It has basic functionalities of the system, enabling remote management of mobile devices.

GOOGLE Pixel XL

User:

Example User

Activation type:

Android

Alias:

Enter device alias

Last contact:

2026-05-13 13:17:43

Battery level: 100%

Health: Good

Internal storage: 24.06%

Total: 24.32 GiB (26.11 GB) Free: 18.47 GiB (19.83 GB)

External storage:

No external memory card

RAM: 50.78%

Total: 3.68 GiB (3.95 GB) Free: 1.81 GiB (1.94 GB)

Generate service password

Details

Policy

Profiles

Applications

Location

Backups

Audit logs

Tasks

Dependency graph

Reports

Export

User accounts

Technical data

Manufacturer:

GOOGLE

Model:

Pixel XL

OS:

Android 10 (29)

Serial number:

No info

IMEI :

UNDEFINED

Proget ID:

988 801

Activation date:

2026-05-13 07:30:09

App version:

2.20 (1200)

Patch version:

QP1A.191005.007.A3

Bootloader version:

8996-012001-1908071822

Security patch:

2019-10-06

System update status:

No info

CPU:

null null (arm64-v8a)

Connection type:

Wi-Fi

IP:

192.168.2.217

Wi-Fi MAC:

8c:80:80:82:a3:99

Wi-Fi SSID:

ProgetUnifi

Roaming:

✗

Data encryption:

✓

Access to device usage data:

✓

Android Enterprise status:

Not applicable

Google Play services:

✓

Access to background activity:

✓

Access to Wi-Fi management:

✓

Runtime permissions:

✓ Telephone ✓ SMS ✓ Call log ...

Groups

Example Group

Security

No password on the device

2026-05-13 07:30:14

The lack of a password on the device allows access to the data by unauthorized persons.

1

Generale information

1.1 Enter device alias

- This action allows you to set the device alias. Alias can help with identifying the device

1.2 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

1.3 Generate service password

- This action allows you to generate a service password for the device on which the lost mode has been imposed

2 Quick actions

2.1 Remote desktop

- To use this action you need app Proget Remote to be installed on your device. Proget Remote is an application that allows you to remotely access your Android device screen from Proget server

2.2 Reset password

- This action allows you to send an action to the device that will trigger a password reset request

2.3 Change password

- This action allows you to send an action to the device to set new password on the device

2.4 Wipe device

- This action allows you to restore factory settings

2.5 Wipe company data

- This action allows you to wipe company data. After performing this action device that is registered to the Proget console will be deleted and further management of this device won't be possible. Proget applications will be visible and another registration to Proget console will be possible

2.6 Lock device screen

- This action allows you to send an action to the device that will trigger lock device screen

2.7 Send message

- This action allows you to send a message. While performing this action administrator can choose how the message will be visible on the device

2.8 Send alert

- This action allows you to send an alert message. While performing this action administrator must set message content and can choose additional options. Alert message will be immediately visible at phone with characteristic sound and user will be forced to accept that he read the message

2.9 Forward phone calls

- This action allows you to send an action to forward phone calls to a given phone number

2.10 Delete forward phone calls

- This action allows you to send an action to delete the number to which the calls were forwarded

2.11 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

2.12 Verify the device

- This action allows you to verify device compatibility with Play Integrity policy

2.13 Generate an event log

- This action allows you to generate and send audit logs to Proget server
-

3.1 Details

3.2 Policy

3.3 Profiles

3.4 Applications

3.5 Location

3.6 Backups

3.7 Audit logs

3.8 Tasks

3.9 Dependency graph

3.10 Reports

3.11 Export

Service password

Updated: Jun 9, 2026

NEW

The Service password panel allows the administrator to generate an emergency service password for the device. The password is linked to a specific device and has a defined validity period (default 24 hours, minimum 5 minutes, maximum 30 days). It works even when the device is in Lost Mode, has no internet connection, or the local database is damaged. After use, the device enters a 60-minute privileged window, after which it returns to the state required by policies. The password can be entered manually or scanned as a QR code on the device.



Service password

* Select actions: ⓘ

- ☐ Unblock device
- ☐ Disable Kiosk
- ☐ Remove network restrictions ⓘ
- ☐ Allow developer options
- ☐ Allow deactivation
- ☐ Allow factory reset
- ☐ Emergency Database Reset ⓘ
- ☐ Set Password ⓘ

* Service password expiration date (on device):

2026-05-07 11:19



Time to expire: in 1 day

- ☒ Generate QR code
- ☒ Send service password via email

* Email:

example@domain.com

Message language:

English



Cancel

Generate

1 Unlock device

- If checked, the service password will unlock the device from Lost Mode

2 Disable Kiosk

- If checked, the service password will exit the device from Kiosk mode

3 Remove network restrictions

- If checked, the service password will temporarily remove network restrictions on the device
 - The action removes restrictions imposed by network-related policies:
 - Allow configuring mobile networks
 - Allow mobile data usage while roaming

- Allow tethering configuration and mobile hotspots
- Allow edit Wi-Fi configuration
- Specify settings for Wi-Fi sleep configuration (Keep Always)
- Allow removing added Wi-Fi networks
- Allow private DNS configuration

4 Allow developer options

- If checked, the service password will temporarily enable developer options on the device

5 Allow deactivation

- If checked, the service password will allow deactivation of the Proget MDM application on the device

6 Allow factory reset

- If checked, the service password will allow the user to perform a factory reset on the device

7 Emergency Database Reset

- If checked, the service password will authorize an emergency reset of the Proget MDM application database on the device
 - Use the service password in the Proget application in case of an application synchronization error
- It cannot be combined with other actions

8 Set Password

- If checked, the service password will allow setting a new device password in the Direct Boot scenario (after device restart)
 - Use the service password if you forget the device PIN. To do this, restart the device, tap the Proget notification, enter the generated service password, and set a new password on the device. The service password depends on the 'Lock screen notifications' policy settings.

- It cannot be combined with other actions

9 Service password expiration date (on device)

- Set the date and time when the service password will expire on the device
- Default validity is 24 hours, minimum 5 minutes, maximum 30 days

10 Generate QR code

- If checked, a QR code will be generated along with the service password for easier scanning on the device

11 Send service password via email

- If checked, the generated service password will be sent to the specified email address

12 Email

- Enter the email address to which the service password will be sent
- Required if 'Send service password via email' is checked

13 Message language

- Select the language in which the email message with the service password will be sent

14 Generate

14.1 Service password generated for device

- Displays the generated service password for the device
- The password can be copied to clipboard using the copy icon

14.2 QR code

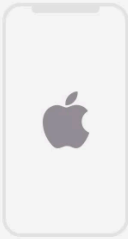
- Displays the QR code containing the service password for scanning on the device
- Visible only if 'Generate QR code' was checked

iOS (Supervised mode)

Updated: Jul 16, 2026

The iOS supervised activation allows the use of extended functions limiting and configuring the device. To use it you need to have the correct Apple Business Manager configuration and the device with iOS operating system.

APPLE iPhone17,3



User:

Example User

Activation type:

iOS (Supervised mode)

Alias:

Enter device alias

Last contact:

2026-05-22 10:24:06

Battery level: 100%

Internal storage: 15.32%

Total: 128.00 GiB (137.44 GB) Free: 108.39 GiB (116.39 GB)

External storage:

No external memory card

Details

Policy

Profiles

Applications

Location

Audit logs

Tasks

Dependency graph

File Manager

Technical data

Manufacturer:

APPLE

Model:

iPhone17,3

OS:

iOS 26.4.2

Serial number:

XXXXXXXXXXXX

IMEI 1:

XXXXXXXXXXXX

IMEI 2:

XXXXXXXXXXXX

Proget ID:

867 367

Activation date:

2026-05-22 10:23:46

System update status:

Update available

Declarative management:

✓

Update Version:

26.5

Wi-Fi MAC:

XXXXXXXXXXXX

Roaming:

✗

Data encryption:

✓

Lost mode enabled:

✗

Groups

Example Group

Security

✗ 0

⚠ 0

✓ 1

ℹ 0

Device secured

1

Generale information

1.1 Enter device alias

- This action allows you to set the device alias. Alias can help with identifying the device

1.2 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

2 Quick actions

2.1 Reset password

- This action allows you to send an action to the device that will trigger a password reset request

2.2 Wipe device

- This action allows you to restore factory settings

2.3 Wipe company data

- This action allows you to wipe company data. After performing this action device that is registered to the Proget console will be deleted and further management of this device won't be possible. Proget applications will be visible and another registration to Proget console will be possible

2.4 Lock device screen

- This action allows you to send an action to the device that will lock device screen

2.5 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

2.6 Enable lost mode

- This action allows you to send an action to block the device. When device is blocked, user can only call to the administrator or emergency number which is entered during "Block device" action

2.7 Disable lost mode

- This action allows you to send an action to unlock the device

2.8 Send Custom Apple Command

- This action allows you to send a Custom Apple Command to the device

3 Tables

3.1 Details

3.2 Policy

3.3 Profiles

3.4 Applications

3.5 Location

3.6 Audit log

3.7 Tasks

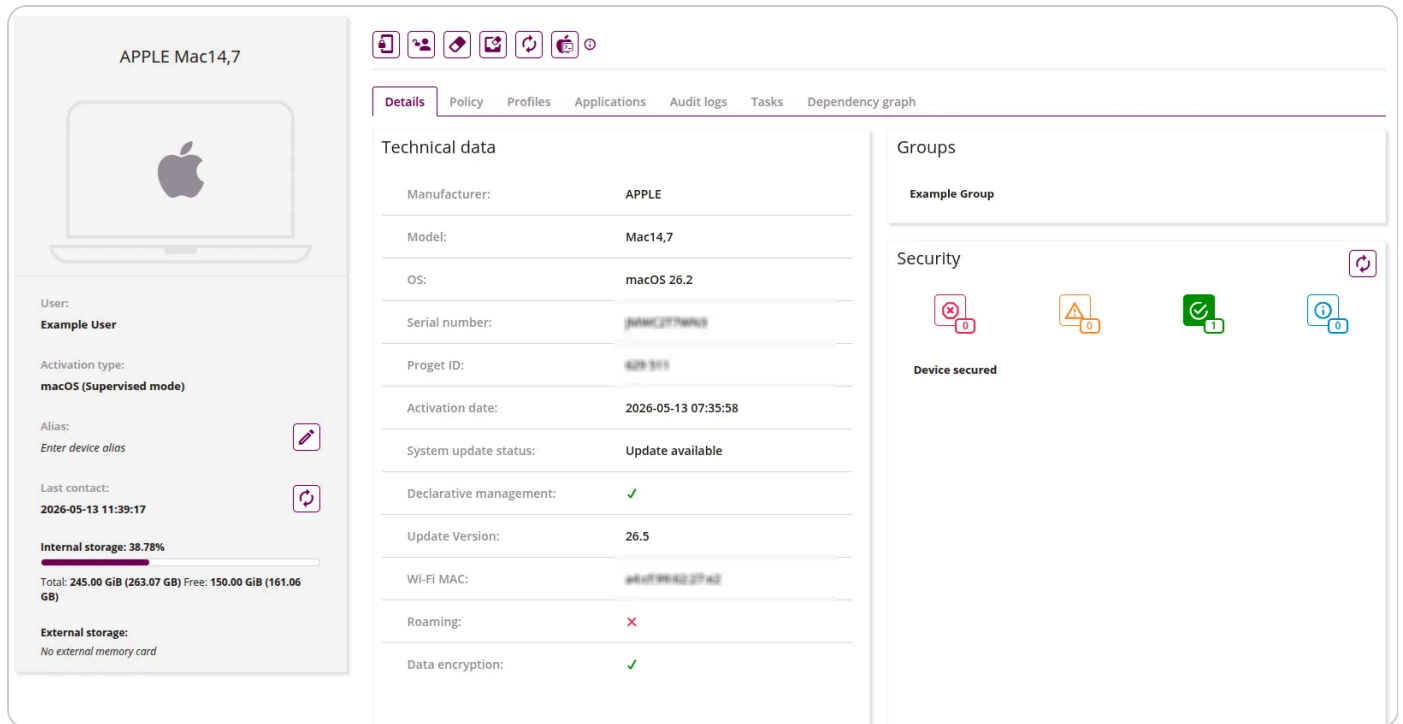
3.8 Dependency graph

3.9 File Manager

macOS

Updated: Jul 16, 2026

The macOS device activation allows the use of functions limiting and configuring the device. You can perform it on the device with the macOS operating system.



1 Generale information

1.1 Enter device alias

- This action allows you to set the device alias. Alias can help with identifying the device

1.2 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

2

Quick actions

2.1 Block device

- This action allows you to send an action to block the device. When device is blocked, user can only call to the administrator or emergency number which is entered during "Block device" action

2.2 Unlock device

- This action allows you to send an action to unlock the device

2.3 Wipe data

- This action allows you to restore factory settings

2.4 Wipe company data

- This action allows you to wipe company data. After performing this action device that is registered to the Proget console will be deleted and further management of this device won't be possible. Proget applications will be visible and another registration to Proget console will be possible

2.5 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

2.6 Send Custom Apple Command

- This action allows you to send a Custom Apple Command to the device
-

3 Tables

3.1 Details

3.2 Policy

3.3 Profiles

3.4 Applications

3.5 Audit log

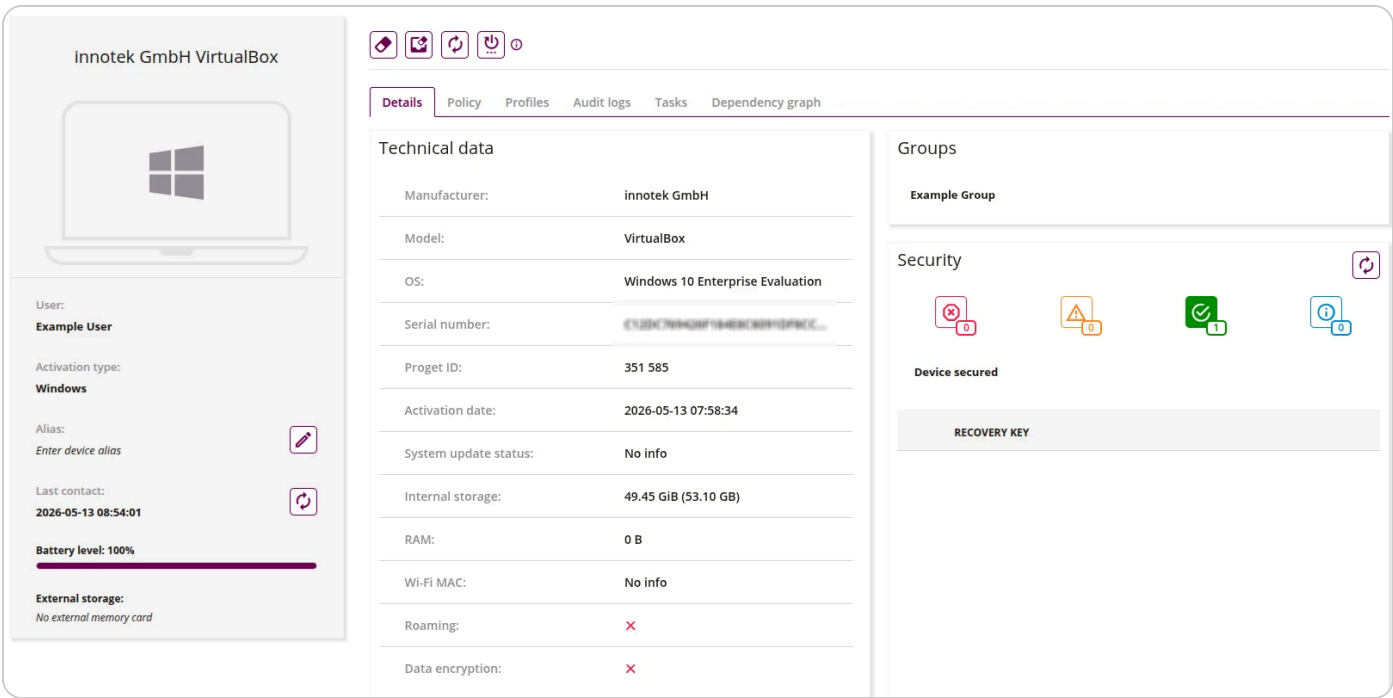
3.6 Tasks

3.7 Dependency graph

Windows

Updated: Jul 16, 2026

The Windows device activation allows the use of functions limiting and configuring the device. You can perform it on the device with the Windows operating system.



1 Generale information

1.1 Enter device alias

- This action allows you to set the device alias. Alias can help with identifying the device

1.2 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

2 Quick actions

2.1 Wipe data

- This action allows you to restore factory settings

2.2 Wipe company data

- This action allows you to wipe company data. After performing this action device that is registered to the Proget console will be deleted and further management of this device won't be possible. Proget applications will be visible and another registration to Proget console will be possible

2.3 Refresh device

- This action allows you to send a refresh action to the device to update information and device status

2.4 Reboot device

- This action allows you to send an action to the device to reboot the device

3 Tables

3.1 Details

3.2 Policy

3.3 Profiles

3.4 Audit log

3.5 Tasks

3.6 Dependency graph

Devices tabs

Updated: Jul 16, 2026

Click on the device tab you are interested in for details.



Details

Device details, applied policy, and security status



Policy

Monitor assigned policy and verify device compliance



Profiles

Profiles assigned to the device from groups or directly



Applications

Installed applications with available management actions



Location

Previously recorded locations and force-locate the device



Backups

Create and browse backups of contacts, SMS/MMS, and calls



Audit logs

Generate and browse audit logs from the device



Tasks

All tasks generated for this device



Dependency graph

Interactive graph of the device's relationships to other elements



File Manager

Remotely browse, upload, and manage files on the device



Reports

Create and browse device usage reports



Export

Export SMS, contacts, and call list from the device



User accounts



System bug reports

List of all user accounts added on the device

Request Android bug reports, auto-deleted after 30 days



Photos during device lock

Photos captured while the device was locked



Users

Users who logged into the kiosk with their parameters

Details

Updated: Jun 24, 2025

Here you can find details about the device, policy applied and security of the device. You can also assign policies directly to the device.

Technical data

Manufacturer:	SAMSUNG
Model:	SM-A225F
OS:	Android 13 (33)
Serial number:	888738PC8GA
IMEI 1:	259476280777073
IMEI 2:	354476280777073
Proget ID:	698 357
Activation date:	2025-10-17 09:26:47
App version:	2.19.0 (1111)
Patch version:	TP1A.220624.014.A225FXXSBDYE1
Bootloader version:	A225FXXSBDYE1
Security patch:	2025-05-01
System update status:	No info
CPU:	Mediatek MT6769V/CT (arm64-v8a)
Connection type:	WiFi
IP:	192.168.0.48
Wi-Fi MAC:	98:96:48:48:98:98
Wi-Fi SSID:	PROGET-1
Roaming:	✗
Data encryption:	✓
Access to device usage data:	✓
Android Enterprise status:	Registered
Google Play services:	✓
Remote password change on the device:	✓
Lost mode enabled:	✗
Access to background activity:	✓
Access to Wi-Fi management:	✓
Runtime permissions:	✓ Telephone ✓ SMS ✓ Call log ✓ ...

Groups

🔗 Example Group

Security



Root status

2025-10-17 09:26:48

Play Integrity verification status

2025-10-17 09:26:57

1

Technical data

- Here you can see the most important technical data about your device, such as:
 - device manufacturer
 - device model
 - device IMEI
 - Wi-Fi SSID
 - The version of the Proget application, e.t.c

2 Groups

- Here you can see the groups that are currently assigned to the device

3 Security

- Here you can see the security status of your device. There are four types of security status in the Proget system, such us:
 - Safe
 - Unsafe
 - Information
 - Critical
- Examples of statuses that can be found here:
 - No password on the device
 - Root status
 - Play integrity verification status

Policy

Updated: Feb 12, 2025

Here, you can monitor the policy assigned by administrator and check its application on the device. You can also compare the expected settings with the actual configuration to verify compliance.

Device policy

Default policy (Allocation: Default)

Matching: 68

Modification date: 2025-07-08 14:31:52

Management

1

Device policy

- Information about the name and assignment of the policy to the device
- Clicking on the policy name will redirect the user to its configuration

2

Matching

2.1 Policy filter

- Search policies by filtering by:
 - Status
 - Matched
 - Mismatched
 - Name
 - Start typing the policy name, and the results will be dynamically filtered
 - Category
 - Applications
 - Functionality
 - Location
 - Password
 - Security

2.2 Policy Matching Table

- Information about policies available in the table:
 - Policy Match
 - Policy Category
 - Current policy status on the device
 - Required policy status on the device
 - Policy details

3 Management

3.1 Edit policy on the device

- This action allows you to editing the policy directly assigned to the device

3.2 Reapply policy

- This action allows you to re-sending the policy to the device

Profiles

Updated: Dec 3, 2024

Here you can find all of the profiles assigned to this device: profiles assigned from group and profiles assigned directly. From here you can assign profiles directly to the device.

Device profiles

Selected: 0

Deselect all



Edit



☐	PROFILE NAME	CATEGORY	ALLOCATION
☐	Example Business Documents profile	Business documents	ExampleGroup
☐	Example Kiosk profile	Kiosk	ExampleGroup
☐	Example location profile	Location	Device

Results: 3

Page limit:

50



1



1

Delete profile

- This action allows you to remove the added profile

2

Edit

- This action allows you to edit profiles on the device. You can manage profiles on your device by adding and removing them

3

Refresh

- This action allows you to refresh the list of profiles

4

Profile list

- List of all profiles added to the device. The list contains information whether the profiles are added directly to the device or from a group

Applications

Updated: Jun 24, 2025

Here you can find a table with information about applications installed on the given device. You can add applications to the device and perform actions on them.

Applications

Matching: 5

Modification date: 2025-06-03 09:25:21

All applications

Management

1

Matching

1.1 Filters

- Application filter allows you to search for applications by data, such as:
 - Status
 - App name
 - App ID

1.2 Synchronize application

- This action allows you to synchronize the application status on the device

1.3 Refresh data

- This action allows you to refresh data of applications on the device managed by Proget console

1.4 App list

- List of all managed applications with their status

2 All applications

2.1 Filters

- Application filter allows you to search for applications by data, such as:
 - App name
 - App ID
 - Installed by
 - Blocked

2.2 Clear app data

- This action allows you to clear the application data on the device by sending an action from the console

2.3 Disable app

- This action allows you to disable the application on the device by sending an action from the console

2.4 Enable app

- This action allows you to enable blocked application on the device by sending an action from the console

2.5 Start app

- This action allows you to start the application on the device by sending an action from the console

2.6 Delete app

- This action allows you do delete application from the device by sending an action from the console

2.7 App list

- List of all applications on the device with its parameters

3 Management

3.1 Clear app data

- This action allows you to clear the application data on the device by sending an action from the console

3.2 Start app

- This action allows you to start the application on the device by sending an action from the console

3.3 Send configuration

- This action allows you to send configuration to the application on the device by sending an action from the console, e.g. for the Gmail app

3.4 Edit

- This action allows you to edit the app list and prime the installation of work apps on the device

3.5 Refresh data

- This action allows you to refresh the list of applications

3.6 App list

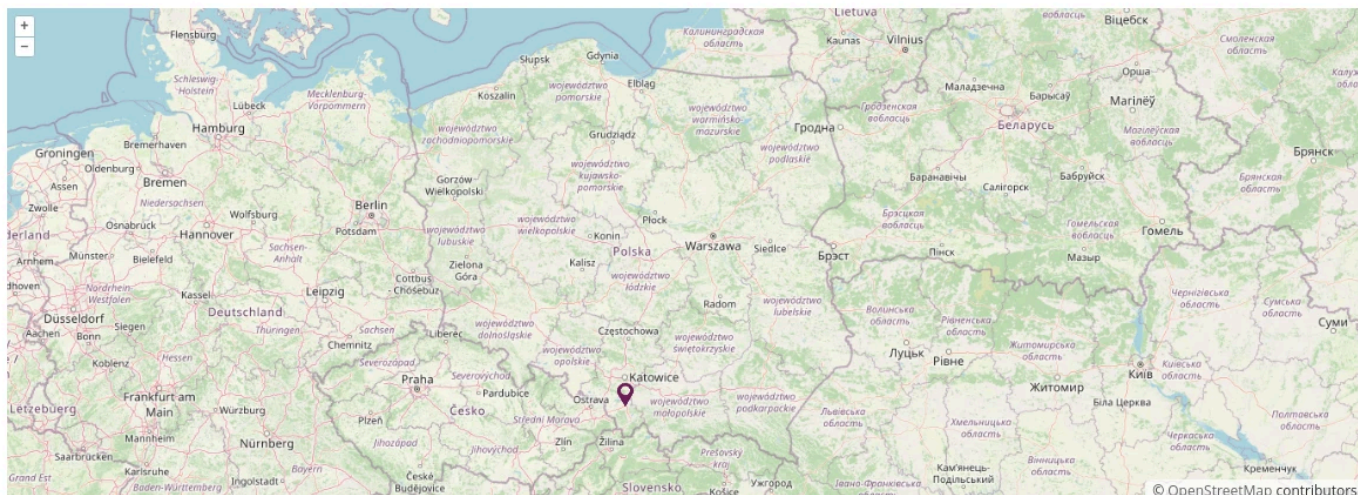
- List of all managed applications on the device

Location

Updated: Dec 3, 2024

Here you can check the list of previously downloaded locations of this device. You can also force the location of the device at this time.

Location



Location History

Date: From Select ... To Select date

Reset filters

☐ Show route on the map

Force location



DATE	LATITUDE	LONGITUDE	ALTITUDE	SPEED	ACCURACY
2020-11-02 08:14:01	49.8227789	19.1406250	248.3	0 km/h	13.44
2020-11-02 08:14:08	49.8227789	19.1406250	248.3	0 km/h	13.44

Results: 2 | Page limit: 50



1 Location map

- On this map you can see the location of device which is indicated by a pins

2 Location date

- This functionality allows you to check the location of the device in selected time periods

3 Show route on the map

- This functionality shows the route from the oldest location to the newest, i.e. the route along which the device moved

4 Force location

- This action allows you to force the current location of the device

5 Refresh

- This action allows you to refresh the list of the location

6 Location list

- List of all device locations and its parameters

Backups

Updated: Dec 3, 2024

Here you can make a backup and find all of the previously made backups from this device. The available backup options are backup of contacts, backup of SMS/MMS and backup of call log.

Backup of this device

Selected: 0

Deselect all



Make a backup

☐	DATE
☐	2024-10-02 12:39

Results: 1

Page limit: 50



1



Other backup

Selected: 0

Deselect all





☐	DEVICE	ID	DATE
☐	Hammer Iron V	2024-10-02 12:47	2024-10-02 12:47

Results: 1

Page limit: 10



1



1 Restore

- This action allows you to restore the available backups on your device

2 Delete

- This action allows you do delete the available backups

3 Make a backup

- This action allows you to create a device backup, such as:
 - Backup of contacts
 - Backup of SMS/MMS
 - Backup of call log

4 Refresh

- This action allows you to refresh the list of backup, if the generated backup is not displayed

5 Backup list

- List of generated backups

6 Restore

- This action allows you to restore the available backups on the other devices

7 Delete

- This action allows you do delete the available backups

8 Refresh

- This action allows you to refresh the list of other backup

9 Other backup list

- List of all other backups with its parameters

Audit log

Updated: Dec 3, 2024

Here you can generate an audit log from the device and find all of the previously generated audit logs.

Audit logs

Action: Select  

Status: Select  

Date of occurrence: From Select To Select  

Reset filters

ACTION	STATUS	DATE OF OCCURRENCE 	PERFORMED BY	PERFORMED ON	DETAILS
device.activate	Success	2024-10-02 12:41:45	SAMSUNG SM-A22...	SAMSUNG SM-A22...	Device activated
device.ownership....	Success	2024-10-02 12:41:44	SAMSUNG SM-A22...	SAMSUNG SM-A22...	Device ownership updated

Results: 2 | Page limit: 50 

  1  

1

Filter

- Use filters to find the right log

2

Search

- Use the search engine to find the right log

3

List of audit log

- List of logs that have been generated as a result of a specific action in the console or on the device

Tasks

Updated: Dec 3, 2024

Here you can find all of the tasks generated on this device.

Tasks

Complete date: Select date

Action: Select

Created by: Start typing...

Status: Select

Reset filters

SENT DATE	COMPLETE DATE	ACTION	CREATED BY	STATUS
2024-10-02 13:23:36	2024-10-02 13:23:53	Export calls	example	Success
2024-10-02 13:23:33	2024-10-02 13:23:53	Export contacts	example	Success
2024-10-02 13:23:31	2024-10-02 13:23:53	Export sms	example	Success
2024-10-02 12:42:03	2024-10-02 12:42:07	Add profile: Kiosk ⓘ	system	Success
2024-10-02 12:42:02	2024-10-02 12:45:44	Policy update ⓘ	system	Success
2024-10-02 12:41:44	2024-10-02 12:41:44	Policy update ⓘ	system	Success
2024-10-02 12:41:44	2024-10-02 12:41:44	Refresh device data	system	Success

Results: 7 | Page limit: 50

<<

<

1

>

>>

1 Filters

- Use filters to search for relevant tasks

2 Clear pending tasks in the application

- This action allows you to clear pending tasks with status created, canceled or failed.

3 Refresh

- This action allows you to refresh the task status in the task list

4 Tasks list

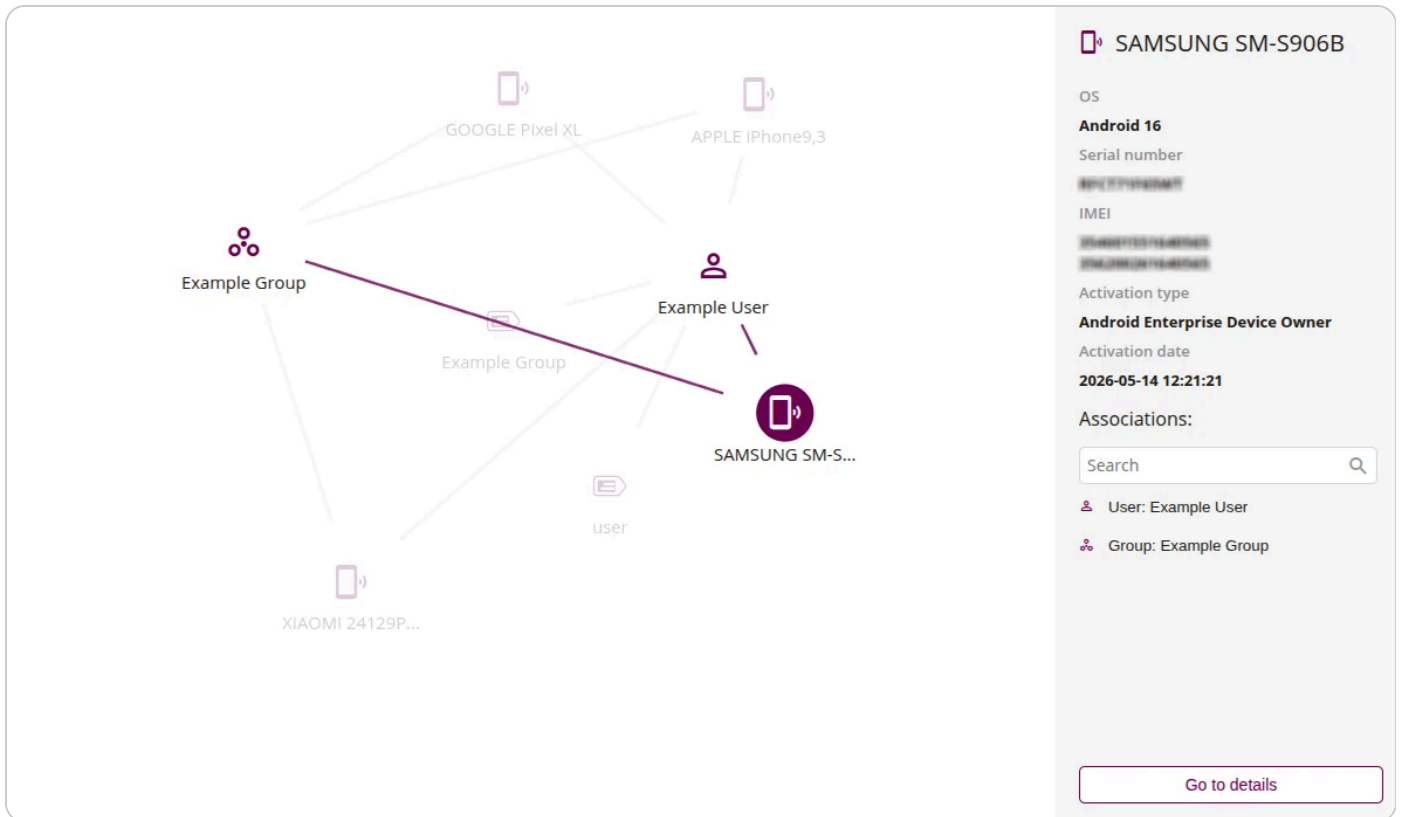
- List of all tasks with its parameters

Dependency graph

Updated: Jun 3, 2026

NEW

The Dependency graph tab on the device card displays an interactive visualization of relationships between the selected device and other system elements such as users, groups, roles, labels, profiles, policies, and directory integrations (LDAP/Entra). It allows administrators to quickly understand what is assigned to or associated with a specific device, without navigating between multiple views.



1 Graph

- Interactive graph showing the device as the central node with connected elements displayed around it
- Connected elements include users, groups, roles, labels, profiles, policies, and directory integrations assigned to or associated with the device
- Click on a node to view its details in the side panel
- Nodes with a number represent aggregated elements - click to expand them into individual nodes

2 Details panel

- Side panel showing detailed information about the selected element
- When the device node is selected, it displays device-specific data such as OS, serial number, IMEI, activation type, and activation date
- Associations section lists related elements grouped into accordion categories (e.g. Users, Groups, Roles, Labels)

- Use the search field to filter associations
- Click on an element to navigate to the detailed view in the system

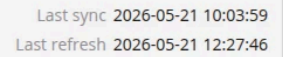
File Manager

Updated: Jun 3, 2026

BETA

The File Manager tab allows the administrator to remotely manage files on the device. From this view, you can browse the file structure, create and delete directories, upload and download files, and track the status of file operation tasks. The feature works on Android (Device Owner, Profile Owner) and iOS (within the File Manager app sandbox). Queued actions are visualized in the tree structure as a shadow structure (green: addition, red: deletion, yellow: folder not synchronized). Tasks are executed asynchronously - even when the device is offline, they will be carried out after the connection is restored.

Auto-refresh: None Refresh



- | Example File | |
|--------------|---------------------|
| Path | /Example File |
| Size | 9.73 MiB (10.20 MB) |
| Items | 2 |
| Modified | 2026-05-20 08:20:35 |

Tasks	▼
Files	▼
Management	▼

1

1.1 Auto-refresh

- Select the auto-refresh interval for the file structure view from the dropdown

1.2 Refresh

- This action allows you to refresh the file structure view

1.3 Expand all

- This action allows you to expand all directories in the file tree

1.4 Collapse all

- This action allows you to collapse all directories in the file tree

1.5 Force files structure synchronization

- This action allows you to force the device to synchronize its file structure with the server

1.6 Request directory creation

- This action allows you to request the creation of a new directory on the device

1.7 Upload file

- This action allows you to upload a file from the console to the selected directory on the device

1.8 Request directory deletion

- This action allows you to request the deletion of the selected directory on the device

1.9 File structure

- Tree view of the device file system with directories and files
- Queued actions are visible in the tree as a shadow structure (green: addition, red: deletion, yellow: folder not synchronized)
- Right-click on a file or directory to access context actions (e.g. request file deletion, download file)

1.10 Details of selected element

- Panel showing details of the selected file or directory, such as:
 - Path
 - Size
 - Items
 - Modified

2 Tasks

2.1 Filters

- Filters allow you to search for tasks by data, such as:
 - Status
 - Type

2.2 Cancel task

- This action allows you to cancel a task that has not yet been delivered to the device
- Available only for tasks with status "Pending"
- If the cancelled task was a file upload, the associated file is also deleted from the server

2.3 List of tasks

- List of all file operation tasks and their parameters

3 Files

3.1 Filters

- Filters allow you to search for files by data, such as:
 - File name
 - Type

3.2 Download file

- This action allows you to download a file stored on the server to your computer

3.3 Delete file

- This action allows you to delete the selected file from the server

3.4 List of files

- List of all files stored on the server associated with this device and their parameters

4 Management

4.1 Regenerate authorization code

- This action allows you to regenerate the authorization code used by the File Manager mobile app to authenticate with the server
- Use when the mobile app cannot establish a connection or requires re-authorization

Reports

Updated: Dec 3, 2024

Here you can create a report of the device usage data and find all of the previously created reports.

Reports

Selected: 0

Deselect all

Create report

	DELIVERY DATE	ELEMENTS	PERIOD	STATUS	ISSUED BY	
✓	☐	2024-11-20 09:45:37	Mobile data usage Wi-Fi data usage Application usage Storage capacity	2024-11-20 - 2024-11-20 2024-11-20 - 2024-11-20 2024-11-20 - 2024-11-20 -	Done Done Done Done	ironman

☒ Storage capacity ☐ Mobile data usage ☐ Wi-Fi data usage ☐ Application usage

Report data:
-
Number of applications: 180
Data used: 1.48 GiB (1.59 GB)

Export report

Google

Google Play services

Android System WebView

Messages

WhatsApp

Gboard

Settings

Speech Services by Google

Phone

Other

ICON	TYPE	NAME	APPLICATION ID / P...	DATA USED	PERCENTAGE SHARE
	Application	Google	com.google.android.googl equicksearchbox	242.99 MiB (254.80 MB)	16.075
	Application	Google Play services	com.google.android.gms	148.40 MiB (155.61 MB)	9.817

1

Delete report

- This action allows you to delete the created report

2

Create report

- This action allows you to create a device report, such as:
 - Storage memory usage report
 - Mobile data usage report
 - Wi-Fi data usage report
 - Application usage report

3

Refresh

- This action allows you to refresh the list of reports, if the generated report is not displayed

4 Reports list

- List of all reports generated from the device with its parameters

Export

Updated: Dec 3, 2024

Here you can export SMS, contacts and call list from the device and find all of the previously made exports.

Export

Date:

Type:

Reset filters

Selected: 0 | Deselect all



Export SMS

Export contacts

Export Call List



☐	DATE 	TYPE 	SIZE 
☐	2024-10-02 12:19:59	Call List	141 B
☐	2024-10-02 12:19:57	Contacts	64 B
☐	2024-10-02 12:19:55	SMS	350 B

Results: 3 | Page limit:

<<

<

1

>

>>

1 Export filter

- Export filter allows you to search for exported files, such as:
 - Date
 - Type

2 Download export

- This action allows you to download exported files from the device

3 Delete export

- This action allows you to remove selected record from the export list

4 Export SMS

- This action allows you to export the SMS file from the device

5 Export contacts

- This action allows you to export the contacts file from the device

6 Export Call list

- This action allows you to export the call list file from the device

7 Refresh

- This action allows you to refresh the export list

8 Export list

- List of all exported files and its parameters

User accounts

Updated: Jun 9, 2026

Here you can find the list of all the user accounts that are added on the device.

User accounts

Selected: 0

Deselect all



☐	NAME	TYPE
☐	Anonymous Account	al.x.grok
☐	work 8623817118814726823818713817188188@android-for-work.googleusercontent.com	com.google.work

1

Delete

NEW

- This action allows you to remove an account that is present on the device
- For some accounts, after using the 'Delete' action, user interaction on the device may be required. In such cases, the task status will depend on the action taken by the user.
- The selected action is irreversible.
- Android Enterprise account deletion is not available

2

User accounts list

- List of all user accounts added on the device with its parameters

System bug reports

Updated: Jun 3, 2026

NEW

The System bug reports tab allows the administrator to request the generation of an Android system bug report (bugreport/dumpstate) on the device. After the user confirms the 'Share' action in the system notification, the report is sent to the MDM server and displayed in the console for diagnostic purposes. Reports older than 30 days are automatically deleted.

System bug reports

ⓘ After generating the report on your phone, **be sure to click "Share"** in the system notification. Without this, the report **will not be sent to the console**. System bug reports older than 30 days will be automatically deleted.

Completion date: From Select To Select

Status: Select

[Reset filters](#)

[BASIC](#) [PQL](#)

Selected: 0

[Deselect all](#)



[Generate report](#)



☐	COMPLETION DATE	REPORT	STATUS
☐	2026-05-15 09:10:38	System errors	Completed
☐	2026-05-15 07:42:02	System errors	Completed

1 Filters

- Filters allow you to search for generated reports by data, such as:
 - Completion date
 - Status

2 Download

- This action allows you to download the generated report file from the device

3 Delete

- This action allows you to remove selected record from the report list

4 Generate report

- This action allows you to request the device to generate a system bug report
 - After clicking, the device receives a task to generate the report
- The user must confirm the 'Share' action in the system notification on the device (required for the report to be sent to the console)

5 Refresh

- This action allows you to refresh the report list

6 List of generated reports

- List of all generated reports and its parameters
- Select reports using checkboxes to perform bulk download or delete actions

Photos during device lock

Updated: Dec 3, 2024

Here you can find all of the photos taken during device lock from this device.

Photos during device lock

Date: From Select To Select

[Reset filters](#)

Selected: 0

[Deselect all](#)



☐	DATE	FILE
> ☐	2024-10-03 07:54:08	1727934848247-front.jpg
> ☐	2024-10-03 07:54:07	1727934847551-back.jpg
> ☐	2024-10-03 07:45:03	1727934303113-back.jpg
> ☐	2024-10-03 07:45:03	1727934303762-front.jpg

Results: 4



1 Filters

- This functionality allows you to filter photos taken while the device was locked by date and file name

2 Delete

- This action allows you to remove photos taken while the device is locked from the list

3 Refresh

- This action allows you to refresh the photo list

4 Photos during device lock list

- List of all photos taken while using the device during device lock

Users

Updated: Dec 3, 2024

Here you can find the list of all the users that logged into the kiosk with its parameters.

Users

Selected: 0

Deselect all



☐	FIRST NAME	SURNAME	USERNAME	LOGIN DATE	STATUS
☐	Example	Example	example	2024-10-03 07:49:31	Positive
☐	-	-	example user	2024-10-03 07:45:40	Positive

Results: 2

Page limit: 50

<<

<

1

>

>>

1

Download

- This action allows you to download user information logs

2

User list

- List of all users that logged into the kiosk with its parameters

Groups

Updated: Dec 3, 2024

The groups tab shows the list of the previously created groups on the server. Groups in the Proget system are used for quick and convenient allocation of policies, profiles and applications for many users and devices at the same time. You can create many groups with different settings. One user can belong to several groups, as long as there are no conflicts between groups (i.e. they do not have policies or profiles of the same type).

Name: Employee X

Policies: Start typing...

Profiles: Start typing...

Filter type: Select v

Reset filters

Selected: 0 | Deselect all



Group priorities Add 

☐	NAME v	POLICIES	PROFILES	APPLICATIONS v	DEVICES v
☐	Employee	- Android Enterprise Profile Owner policy - Android Enterprise Device Owner policy	- ExampleActiveSyncProfile - ExampleBusinessDocumentsProfile - ExampleKioskProfile - ExampleGeofencingProfile	1	0

Results: 1 | Page limit: 50 v



1 Groups filter

- Groups filter allows you to search for groups by data, such as:
 - Name
 - Policies
 - Profiles

2 Update group

- This action allows you to update the group and assign it a new name

3 Copy group

- This action allows you to duplicate already existing groups in the console

4 Add applications

- This action allows you to add an application for single or multiple selected groups from the list

5 Delete group

- This action allows you to delete single or multiple selected groups from the list
- This action is not available for groups that are assigned to a user

6 Group priorities

- This button will take you to a page where you can manage group priorities

7 Add group

7.1 Set name

- Set a name to create a new group
- Required

7.2 Link to label

- Create a label, or link to an existing one

8 Groups list

- List of all groups with their parameters

8.1 Selected Group

Group Priorities

Updated: Feb 12, 2025

Group priorities

	NAME	POLICIES	PROFILES	APPLICATI...	USERS	DEVICES	
1	↕ admin	0	0	0		0	...
2	↕ user	0	0	0		1	...
3	↕ Employee	0	0	2		1	...
4	↕ testGroup	0	0	0		1	...

Back

Submit

1 Priority list of groups

- Priority list of groups, where the order indicates their importance.

Enter position

1 Enter position

- Set the group position by number
- Required

Selected group

Updated: Jun 3, 2026

Here you can find general information about selected group and make changes to an existing group.

Employee

Filters assigned to group

device.user.label = Employee

Group assigned profiles

- ExampleActiveSyncProfile
- ExampleBusinessDocumentsProfile
- ExampleKioskProfile
- ExampleGeofencingProfile

Group assigned policies

- Android Enterprise Device Owner policy
- Android Enterprise Profile Owner policy

Group assigned apps

Device

Container

Gmail - Email by Google

<<

<

1

>

>>

Devices assigned to group

IMEI: Start typing...

Serial number: Start typing...

User: Start typing...

+

Reset filters

MANUFACTURER	MODEL	IMEI	SERIAL NUMBER	USER	ACTIVATION TYPE
SAMSUNG	SM-G970F	XXXXXXXXXXXX	XXXXXXXXXXXX	John Doe	Android Enterprise Device Owner

Results: 1 | Page limit: 50

<<

<

1

>

>>

Back

1 Edit group name

- This action allows you to edit the group name

2 Edit group filter

- This action allows you to edit the group filter

3 Edit the group profiles

- This action allows you to edit the profiles in the group

4 Edit the group policies

- This action allows you to edit the policies in the group

5 Update applications assigned by group

5.1 Applications Filter

- The app filter allows you to search for app which are added to the group by data, such as:
 - App name
 - Package Id
 - Origin
 - Platform

5.2 Delete

- This action allows you to remove selected applications from the group

5.3 Global settings for selected applications

- The application settings window allows you to configure platform-specific parameters:
- Android
 - Automatic installation mode (apps from the store)
 - One-time installation - the app is installed once; if uninstalled by the user, it will not be reinstalled
 - Force installation - the app is installed automatically; if uninstalled, it will be reinstalled
 - Do not install - the app is not installed on the device
 - Automatic installation mode (apps from files or external resources)
 - Force installation - the app is installed automatically; if uninstalled, it will be reinstalled
 - Do not install - the app is not installed on the device
 - Automatic update mode
 - Default update - the app updates according to default settings
 - High priority update - the app updates automatically as soon as a new version appears in Google Play

- Postponed update - the app does not update automatically despite a new version being available
- According to policy - the app updates according to the policy assigned to the device
- Uninstall settings
 - Uninstall not blocked - the user can uninstall the app
 - Uninstall blocked - the user cannot uninstall the app
 - According to policy - behavior consistent with the policy assigned to the device
- Wi-Fi connection requirements
 - Wi-Fi required - the app installs/updates only over a Wi-Fi connection
 - Wi-Fi not required - the app installs/updates over any connection
 - According to policy - behavior consistent with the policy assigned to the device
- Installation priority
 - High - an app with this priority is installed first in the queue
 - Normal - the app is installed in the standard order
 - Low - an app with this priority is installed last in the queue
- Install only when idle - installation occurs only when the device is not in use
 - Yes
 - No
- Install only while charging - installation occurs only when the device is connected to a charger
 - Yes
 - No
- Notify the user after assigning app configuration - displays a notification after a new configuration is assigned
 - Yes
 - No
- Clear app data before assigning configuration - removes existing app data before applying the new configuration

- Yes
- No
- Apple
 - Required
 - Yes - the app is required on the device and is installed automatically
 - No - the app is not required, the user can install it optionally
 - Profile
 - List of available configuration profiles to assign to the app
 - None
 - Management options
 - None - No setting
 - Remove app - If the app was installed as managed, it will be removed when the MDM profile is removed
 - Prevent backup - Prevents backups of the app's data from being created
 - Remove app and prevent backup - Combines both functions: removes the app when the MDM profile is removed and prevents backups
 - Convert from unmanaged to managed - take control of an app previously installed by the user
 - Yes
 - No
 - Lockable - allows the app to be locked on the device screen (Feature available from iOS 18)
 - Yes
 - No
 - Hideable - allows the app icon to be hidden
 - Yes
 - No
 - Feature available only when 'Lockable' is enabled
 - Removable - allows the user to uninstall the app

- Yes
- No
- Screen lock for Tap to Pay - forces a screen lock after a Tap to Pay transaction
 - Yes
 - No
- Enable direct downloads for associated domains
 - Yes
 - No
- Manage associated domains
 - Add
 - Remove
- Associated domains (list of domains in the format applinks:example.com)
 - Available if the 'Add' option is selected in 'Manage associated domains'

5.4 Add applications

- Assign applications to the group

5.5 Configure single application

- The application configuration window allows you to set platform-specific parameters:
- Android
 - Automatic installation mode (apps from the store)
 - Automatic installation mode (apps from files or external resources)
 - Automatic update mode
 - Uninstall settings
 - Wi-Fi connection requirements
 - Installation priority
 - Install only when idle - installation occurs only when the device is not in use

- Install only while charging - installation occurs only when the device is connected to a charger
- Notify the user after assigning app configuration - displays a notification after a new configuration is assigned
- Clear app data before assigning configuration - removes existing app data before applying the new configuration
- Application version - allows you to select a specific version of the app to install on the device
- Application configuration - allows you to assign additional configuration parameters to the app (e.g. managed app configuration)
- Apple
 - Required
 - Application version - allows you to select a specific version of the app to install on the device
 - Profile
 - Application configuration - allows you to assign additional configuration parameters to the app (e.g. managed app configuration)
 - Management options
 - Convert from unmanaged to managed - take control of an app previously installed by the user
 - Lockable - allows the app to be locked on the device screen (Feature available from iOS 18)
 - Hideable - allows the app icon to be hidden
 - Removable - allows the user to uninstall the app
 - Screen lock for Tap to Pay - forces a screen lock after a Tap to Pay transaction
 - Enable direct downloads for associated domains
 - Manage associated domains
 - Associated domains (list of domains in the format applinks:example.com)

6 Device list

- List of all devices added to the group, with their parameters

Manage filter

Updated: Jul 16, 2026

Group filter management allows you to assign groups to selected devices in different ways

Manage filter of the group Employee NEW

 Give feedback

Select:

☐ No devices

☐ All devices

☒ Custom settings

 Specify conditions for adding devices to a group using PQL syntax. Go to the [knowledge base](#) to find out more.

device.user.label = Employee ×

 Saved filters ▼

Results: 1

Back Submit

MANUFACTURER	MODEL	USER
SAMSUNG	SM-G970F	John Doe

Results: 1 | Page limit: 50 ▼

<< < 1 > >>

1 No devices

- The selected filter will not assign the group to any device

2 All devices

- The selected filter will assign the group to all devices in the system and those, that will be enrolled to it

3 Custom settings

- The selected filter allows you to enter your own PQL filter

4 Filter field

- The PQL filter allows you to search for devices, that are already added to the system and those, that will be enrolled according to the data:
 - IMEI
 - Serial number
 - Proget ID
 - Manufacturer
 - Model
- Maximum query length: 4000
- Maximum conditions count: 50
- Required

5 Saved filters

- This action allows you to select a filter from the list, that is already created in the system

6 Number of devices

- List of all devices with their parameters, to which groups will be added

Proget Query Language (PQL)

Updated: Jun 3, 2026

Proget Query Language (PQL) is a simple query language that allows you to filter devices in your system. With PQL, you can dynamically assign devices to groups based on defined criteria, creating so-called dynamic groups. Previously, groups were static - administrators manually assigned devices to groups. Now, with PQL, groups can automatically include devices that meet certain conditions, such as device data or user labels. It is also possible to combine different criteria within a single query. Dynamic grouping allows the configuration to be pre-prepared and automatically assigned to devices, even if they are not yet present in the system. The configuration can be modified based on user attributes taken from external directories such as Active Directory. Changes made to the directory can automatically affect the configuration of devices in the Proget system. With PQL, it is easy to create device groups without having to manually assign them. If you do not use the advanced features of PQL, the default group creation mechanism will automatically create a label for the group. For compatibility with previous versions of the system, simply assign the user a label with the same name as the group.

Manage filter of the group Employee

Select:

☐ No devices

☒ All devices

☐ Custom settings

All devices will be assigned to this group
Results: 2

BackSubmit

1 No devices

- Empty group to which no devices will be assigned

2 All devices

- Automatically included all devices in the system

3 Custom settings

- Allows the creation of PQL filters based on specific criteria
-

Custom settings

In the "Custom Settings" section, the administrator can create PQL filters using the available parameters. The system prompts for available options when typing, making query creation intuitive. When the syntax is correct, the administrator can see a list of devices that meet the filter conditions, facilitating ongoing verification of the results.

To better understand the syntax of the filters, here are some basic concepts:

Key elements of the PQL filter

- **Phrase**
 - A single expression consisting of a *parameter*, *operator* and *value*
 - Each filter must contain at least one phrase
 - Phrases can be combined using logical operators (*AND*, *OR*)
 - **Parameter**
 - Specifies the attribute of the device or its owner that is being filtered
 - **Operator**
 - Combines a *parameter* with a *value* and defines the relationship between them
 - **Value**
 - The right-hand side of an expression, specifying what we are looking for (e.g. text, number, logical value)
 - **Connector**
 - Combines phrases into more complex queries
 - Available connectors: *AND*, *OR*
-

Examples of filters

1

device.os.type = android

- This filter assigns all Android devices to a group

1 **device.user.label != Employee**

- This filter includes all devices whose owner does not have the label "Employee"

1 **device.user.organizationUnit contains Office AND device.user.isBlocked = false AND device.os.type = android**

- This filter combines several criteria:
 - The device belongs to a user whose organisation unit (value synchronised with the directory service) contains the word "Office" in its name
 - The device user is not blocked in the Proget system
 - The device runs on Android

Keys

Keys	Available operators	Value type	Description
device.manufacturer	<i>=, !=, in, not_in</i>	enum	Device manufacturer, e.g. Samsung
device.model	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with, in, not_in</i>	enum	Device model, e.g. <i>iPhone 13</i>
device.serialNumber	<i>=, !=</i>	text	Device serial number
device.progetId	<i>=, !=</i>	text	Device Proget ID, e.g. <i>123 456</i>
device.os.type	<i>=, !=</i>	enum	Device operation system e.g. <i>Android</i>
device.os.versionCode	<i>=, !=, >, >=, <, <=</i>	number	Device operation system version e.g. <i>33</i> (Android 13)
device.activationType	<i>=, !=</i>	enum	Activation type e.g. <i>android_mdm</i>
device.systemUpdateStatus	<i>=, !=</i>	enum	Value from a defined set, e.g. <i>available</i>
device.SIM1.IMEI	<i>=, !=</i>	text	IMEI for SIM1
device.SIM2.IMEI	<i>=, !=</i>	text	IMEI for SIM2
device.SIM1 NEW	<i>=, !=</i>	enum	Indicates whether a SIM card is present in slot 1. Use the value <i><< None >></i> to check if the slot is empty

device.SIM2 NEW	=, !=	enum	Indicates whether a SIM card is present in slot 2. Use the value << <i>None</i> >> to check if the slot is empty
device.SIM1.ICCID	=, !=, in, not_in	text	ICCID for SIM1
device.SIM2.ICCID	=, !=, in, not_in	text	ICCID for SIM2
device.SIM1.carrier	=, !=	text	SIM1 operator
device.SIM2.carrier	=, !=	text	SIM2 operator
device.mdmVersionCode	=, !=, >, >=, <, <=	number	Proget app version code
device.alias	=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with	text	Device alias
device.user	=, !=, in, not_in	text	Device belonging to the user e.g. « <i>None</i> », <i>John Doe - jdoe@example.com</i> (UUID)
device.user.uuid	=, !=	text	User UUID
device.user.isBlocked	=, !=	bool	Device belonging to a blocked user
device.user.email	=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with	text	User email e.g. <i>jdoe@example.com</i>
device.user.type	=, !=	enum	User type e.g. <i>local</i>

device.user.displayName	=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with	text	Name and surname e.g. <i>John Doe</i>
device.user.username	=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with	text	Username e.g. <i>jdoe</i>
device.user.principalName	=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with	text	User principal name e.g. <i>jdoe@example.com</i>
device.user.title	=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with	text	User title
device.user.distinguishedName	=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with	text	User distinguished name (DN)
device.user.commonName	=, !=, contains, not_contains, starts_with, not_starts_with,	text	User common name

	<i>ends_with,</i> <i>not_ends_with</i>		
device.user.country	<i>=, !=</i>	text	User country
device.user.organization	<i>=, !=, contains,</i> <i>not_contains,</i> <i>starts_with,</i> <i>not_starts_with,</i> <i>ends_with,</i> <i>not_ends_with</i>	text	User organization
device.user.organizationUnit	<i>=, !=, contains,</i> <i>not_contains,</i> <i>starts_with,</i> <i>not_starts_with,</i> <i>ends_with,</i> <i>not_ends_with</i>	text	User organization unit
device.user.locacity	<i>=, !=</i>	text	Locacity
device.user.tittle	<i>=, !=, contains,</i> <i>not_contains,</i> <i>starts_with,</i> <i>not_starts_with,</i> <i>ends_with,</i> <i>not_ends_with</i>	text	User tittle
device.user.label	<i>=, !=, in, not_in</i>	text	User label
device.user.directoryGroup	<i>=, !=, in, not_in</i>	text	User directory group
device.user.customAttribute1	<i>=, !=, contains,</i> <i>not_contains,</i> <i>starts_with,</i> <i>not_starts_with,</i> <i>ends_with,</i> <i>not_ends_with</i>	text	Custom attribute 1
device.user.customAttribute2	<i>=, !=, contains,</i> <i>not_contains,</i>	text	Custom attribute 2

	<i>starts_with,</i> <i>not_starts_with,</i> <i>ends_with,</i> <i>not_ends_with</i>		
device.user.customAttribute3	<i>=, !=, contains,</i> <i>not_contains,</i> <i>starts_with,</i> <i>not_starts_with,</i> <i>ends_with,</i> <i>not_ends_with</i>	text	Custom attribute 3
device.user.customAttribute4	<i>=, !=, contains,</i> <i>not_contains,</i> <i>starts_with,</i> <i>not_starts_with,</i> <i>ends_with,</i> <i>not_ends_with</i>	text	Custom attribute 4

References

Reference	Used with keys	Available operators	Description
ALLOWED_SIM_CARDS 	<i>device.SIM1.ICCID,</i> <i>device.SIM2.ICCID</i>	<i>in, not_in</i>	List of allowed SIM cards (ICCID) managed in <i>Settings</i> → <i>Allowed SIM Cards</i>

Operators

- **=** - comparison (equals)
- **!=** - comparison (not equal)

- **<** - comparison (less than)
 - **<=** - comparison (less than or equal)
 - **>** - comparison (greater)
 - **>=** - comparison (greater than or equal)
 - **contains** - contains a specific fragment of text
 - **not_contains** - does not contain a specific fragment of text
 - **starts_with** - starts with a specific fragment of text
 - **not_starts_with** - does not start with a specific fragment of text
 - **ends_with** - ends with a specific fragment of text
 - **not_ends_with** - does not end with a specific fragment of text
 - **in** - contains specific values
 - **not_in** - does not contain specific values
-

Value types

- **text** - e.g. "SAMSUNG". Multi-word values should be enclosed in inverted commas
- **number** - e.g. integer or floating point
- **bool** - bool value (*true* or *false*)
- **enum** - a value from a defined set, e.g. type of operating system
- **reference** - a reference to a predefined list managed elsewhere in the system, e.g. *ALLOWED_SIM_CARDS* referring to the allowed SIM cards list

Apps

Updated: Jul 16, 2026

In the apps tab you can find a table with information about applications on the given server.

App name: Start typing...

Package Id: pl.proget X

Origin: Select

Platform: Select

Reset filters

Selected: 0 | Deselect all

Add

☐	ICON	APP NAME	PACKAGE ID	ORIGIN	PLATFO...
☐		Proget	pl.proget.progetmdm	Store	Android 
☐		Proget Backup	pl.proget.backup	Store	Android 
☐		Proget Backup From File Version: master (33)	pl.proget.backup	File ⓘ	Android 
☐		Proget Filesharing Version: 1.5.0 (14)	pl.proget.filesharing	File ⓘ	Android 
☐		Proget File Sharing	pl.proget.filesharing	Store	Android 
☐		Proget Geofencing	pl.proget.geofencing	Device	Android
☐		Proget OpenVPN	pl.proget.openvpn	Store	Android 
☐		Proget Remote	pl.proget.remote	Store	Android 

Results: 8 | Page limit: 50

<<

<

1

>

>>

1 Filtering in a text window

- You can filter the results, using keywords. Enter the keyword you want to filter by into the according field. The results are filtered dynamically when entering text.

2 Update rules

2.1 Available rules

- Select one of the available rules
- Required

2.2 Android Enterprise - work space

- This action allows you to add selected application to the rules of Android Enterprise - work space, such as:
 - None
 - Unlock apps
 - Blacklist

2.3 Android Enterprise - private space

- This action allows you to add selected application to the rules of Android Enterprise - private space, such as:
 - None
 - Whitelist
 - Blacklist

2.4 iOS (supervisor mode)

- This action allows you to add selected application to the rules of iOS (supervisor mode), such as:
 - None
 - Whitelist
 - Blacklist

3 Sync with the store

- This action allows you to sync selected applications with the store

4 Delete application

- This action allows you to delete selected applications

5 Add application

- After clicking the button, you will be transferred to the tab where adding application to the Proget console is possible

6 List of applications

- List of all applications added to the Proget console from the store or from the file

6.1 Single Android app

6.2 Single Android app from file

6.3 Single iOS app

Add application

Updated: Mar 21, 2025

Here you can add applications to the Proget console from the file, from Google Play or from iTunes.

Add application

☐

From the file

☐

From the external resource ⓘ

☐

Google Play

☐

iTunes

Back

1 Add apps from the file

1.1 Name

- Enter name of the application

1.2 Description

- Enter description of the application

1.3 Select file

- Select an application file
- Allowed file type: .apk, .ipa, .pkg
- The maximum size for uploaded files is 314.52MB (300.00 MiB)

2

Add apps from external resource

2.1 Name

- Enter the name of the application
- Maximum length of the text is 255
- Required

2.2 Package id

- Enter the package id of the application
- Maximum length of the text is 255
- Required

2.3 URL

- Enter the URL link to the external resource where the application is located
- Maximum length of the text is 255
- Required

2.4 Checksum

- Enter the checksum of the application
- The checksum is used to verify that the APK file is intact. It is obtained by converting the APK file to Base64 format and then calculating its SHA-256 hash value. Please refer to the knowledge base for detailed instructions.
- Required

2.5 Version

- Enter the Version of the application
- Maximum length of the text is 255

- Required

2.6 Version code

- Enter the version code of the application
- Maximum value is 2100000000
- Number required

2.7 Authentication required

- Check if authorization for access to an external resource is required
- If checked, entering your login and password is required

2.8 Login

- Enter the login that you use to sing-in to the external resource

2.9 Password

- Enter the password that you use to sing-in to the external resource

2.10 Description

- You can enter a description of the application
- Maximum length of the text is 255

2.11 Select file

- You can set your own icon for an application from an external resource

2.12 Delete

- Delete the selected icon for the application from an external resource

3 Add apps from the Google Play

3.1 Google Play

- Here you can search for the application in Google Play store and add it to the Proget console

4 Add apps from the iTunes

4.1 iTunes

- Here you can search for the application in iTunes store and add it to the Proget console

Single Android app

Updated: Oct 16, 2025

Here you can find information about single application such as: package ID, origin, platform, devices with applied configuration, app config feedback and app versions. You can also perform actions on the application and configure settings such as: app configuration and runtime permissions.

 Gmail



Package Id:
com.google.android.gm

Origin:
Store

Platform:
android

 Description

Connect, create and collaborate with Gmail, part of Google Workspace.

Configuration

Devices

App config feedback

Runtime permissions

Versions

Selected: 0

Deselect all



Add configuration

☐	CONFIGURATION N...	GROUPS	CREATION DATE	MODIFICATION DATE	CREATED BY	MODIFIED BY
☐	Example configuration	-	2025-02-11 12:53:57	2025-02-11 12:54:57	Example user	Example user

1

Go to details in store

- After clicking this button, you will be transferred to the details of the app in the Google Play store site

2

Sync with the store

- After clicking this button, the application will be synchronized with the store

3

Update rules

3.1 Available rules

- Select one of the profile application rules
- Required

3.2 Android Enterprise - work space

- This action allows you to add selected application to the rules of Android Enterprise - work space, such as:
 - None
 - Unlock apps
 - Blacklist

3.3 Android Enterprise - private space

- This action allows you to add selected application to the rules of Android Enterprise - private space, such as:
 - None
 - Whitelist
 - Blacklist

3.4 iOS (supervisor mode)

- This action allows you to add selected application to the rules of iOS (supervisor mode), such as:
 - None
 - Whitelist
 - Blacklist

4 Delete app

- This action allows you to delete application from the Proget console

5 Configuration

5.1 Edit configuration

- This action allows you to edit configuration of the application

5.2 Update configuration

- This action allows you to update configuration of the application

5.3 Copy configuration

- This action allows you to copy configuration of the application

5.4 Remove configuration

- This action allows you to remove configuration of the application

5.5 Add configuration

- This action allows you to add configuration of the application

5.6 List of configurations

- List of configurations of the application

6 Devices

6.1 Clear data

- This action allows you to clear the data of the selected application on all devices on which it is installed

6.2 Disable

- This action allows you to disable selected application on all devices on which it is installed

6.3 Enable

- This action allows you to enable selected application on all devices on which it is installed

6.4 Start

- This action allows you to start selected application on all devices on which it is installed

6.5 Send configuration

- This action allows you to send configuration to selected application on all devices on which it is installed

6.6 Delete

- This action allows you to delete selected application from all devices on which it is installed

6.7 Export

- This action allows you to export the list of devices with the information such as: model, user, device status, version of the installed app etc

6.8 Table settings

- In the table settings, you can choose which columns will be displayed

6.9 List of devices

- List of devices with the information such as: model, user, device status, version of the installed app etc

7 App config feedback

7.1 List of app config feedback

- List of app config feedback with the information about status and devices

8 Runtime permissions

8.1 Runtime permissions

- Runtime permissions where you can change the way they are assigned, such as:
 - Ask the user
 - Grant automatically
 - Deny automatically

9 Versions

9.1 List of versions

- List of versions with its quantity on device and on container

Single Android app from file

Updated: Feb 11, 2025

Here you can find information about single application from file such as: package ID, origin, platform, devices with applied configuration and app versions. You can also perform actions on the application and configure settings such as: app configuration and runtime permissions.

 **Proget File Sharing**



Package Id:
pl.proget.filesharing

Origin:
File

Platform:
android

Version:
1.5.1

Version code:
15

Size:
9.73 MiB (10.20 MB)

Devices

App config feedback

Runtime permissions

Versions

IMEI:

Serial number:

User:

Version:





Selected: 0

Deselect all





☐	MANUFACTURER	MODEL	USER	DEVICE STATUS	VERSION
☐	SAMSUNG	SM-T580	-	Active	master

Results: 1

Page limit:



1

Update application

1.1 Select file

- This button allow you to update the app from a file after by uploading a newer version of the app from your device

1.2 Close

- This button allow you to close the application update dialog

1.3 Update

- This button will allow you to update the application from a file to a newer version

2 Download app

- After clicking this button, the application will downloaded on your device

3 Update rules

3.1 Available rules

- Select one of the profile application rules
- Required

3.2 Android Enterprise - work space

- This action allows you to add selected application to the rules of Android Enterprise - work space, such as:
 - None
 - Unlock apps
 - Blacklist

3.3 Android Enterprise - private space

- This action allows you to add selected application to the rules of Android Enterprise - private space, such as:
 - None
 - Whitelist
 - Blacklist

3.4 iOS (supervisor mode)

- This action allows you to add selected application to the rules of iOS (supervisor mode), such as:
 - None
 - Whitelist
 - Blacklist

4 Configuration schema

4.1 Schema

- Enter the JSON configuration scheme or drag and drop the file here for the selected application from the file that can be configured

4.2 Format JSON

- This button allow you to format the JSON configuration schema

4.3 Cancel

- This button allow you to abort the schema configuration

4.4 Submit

- This button allow you to save the schema configuration you entered

5 Delete app

- This action allows you to delete application from the Proget console

6 Devices

6.1 Clear data

- This action allows you to clear the data of the selected application on all devices on which it is installed

6.2 Start

- This action allows you to start selected application on all devices on which it is installed

6.3 Delete

- This action allows you to delete selected application from all devices on which it is installed

6.4 Export

- This action allows you to export the list of devices with the information such as: model, user, device status, version of the installed app etc

6.5 Table settings

- In the table settings, you can choose which columns will be displayed

6.6 List of devices

- List of devices with the information such as: model, user, device status, version of the installed app etc

7 App config feedback

7.1 List of app config feedback

- List of app config feedback with the information about status and devices

8 Runtime permissions

8.1 List of runtime permissions

- List of runtime permissions where you can change the way they are assigned, such as:
 - Ask the user
 - Grant automatically
 - Deny automatically

9 Versions

9.1 List of versions

- List of versions with its quantity on device and on container

10 Export

- This action allows you to export the list of devices with the information about model, user, device status and version of the app installed

11 Table settings

- In the table settings, you can choose which columns will be displayed

Single iOS app

Updated: Jul 9, 2025

Here you can find information about single application such as: package ID, origin and platform. You can also add app configuration.

 **SinglelosApp**



Package Id:

Origin:

Platform:

Version:

Version code:

Size:

com.petri.calculator.calcul

File

ios

1.0

0

21.18 MiB (22.21 MB)

Configuration

Selected: 0

Deselect all



Add configuration

☐	CONFIGURATION ...	GROUPS	CREATION DATE	MODIFICATION D...	CREATED BY	MODIFIED BY
☐	Example configuration	-	2025-07-08 13:00:21	2025-07-08 13:03:57	Example Example	Example Example

1

Update app

- After clicking this button, you will be able to update the application by selecting the current version from your device

2

Download app

- After clicking this button, the application will be downloaded to your device

3

Add to rule

3.1 Available rules

- Select one of the available rules
- Required

3.2 Android Enterprise - work space

- This action allows you to add selected application to the rules of Android Enterprise - work space, such as:
 - None
 - Unlock apps
 - Blacklist

3.3 Android Enterprise - private space

- This action allows you to add selected application to the rules of Android Enterprise - private space, such as:
 - None
 - Whitelist
 - Blacklist

3.4 iOS (supervisor mode)

- This action allows you to add selected application to the rules of iOS (supervisor mode), such as:
 - None
 - Whitelist
 - Blacklist

4 Delete app

- This action allows you to delete application from the Proget console

5 Add configuration

- This action allows you to add configuration of the application

6 Configuration

- List of configurations of the application

Policies

Updated: Jul 16, 2026

Policies in the Proget system allow you to easily limit user's access of functionalities that are found on mobile devices. Thanks to policies we can, for a selected group of devices, impose the desired complexity of the password, limit the use of the camera, or prohibit the use of Google services. Policies are grouped up by type of activation. You will also find predefined default policies that are compatible with device activations.



Android Enterprise Device Owner

Password, app, security, and location rules for Device Owner mode



Android Enterprise Profile Owner

Password, app, and security rules for the work profile container



Android

Password and security restrictions for Android devices



iOS

Password, apps, education, media, and web filter rules for iOS



macOS

Password, app, education, and functionality restrictions for macOS



Windows

Password, app, BitLocker, and security settings for Windows

Android Enterprise Device Owner

Updated: Jun 8, 2026

Password

Level of password required

- The policy specifies the password level on the device..
 - No level allows the device to have no password
 - The low level allows a pattern and an uncomposed numeric password
 - Medium level allows a numeric password with a minimum of 4 compound characters
 - High level requires a complex numeric password with a minimum of 8 characters or an alphanumeric password with a minimum of 6 characters
 - Custom – numeric, requires a numeric password with a minimum length of 4 characters
 - Custom – complex numeric, requires a complex numeric password with a minimum length of 4 characters
 - Custom – alphanumeric, requires an alphanumeric password with a minimum length of 4 characters, with the option to specify the required number of: numeric, lowercase, uppercase, and special characters

Minimum password length

- The policy defines the minimum length of the password used on the device.

Required number of numerical characters

- Policy defines the number of numerical characters in the device password.

Required number of lower case characters

- Policy defines the number of lower case characters in the device password.

Required number of capital characters

- Policy defines the number of A-Z capital characters in the device password.

Required number of special characters

- Policy defines the number of special `!@#$%^&*()_+<>:"'{}|` characters in the device password.

Number of attempts to unlock

- Policy defines the number of incorrect password attempts followed by a device wipe. The policy does not support Direct Boot if restoring the device to factory settings is forbidden.

Number of passwords saved

- The policy determines what number of passwords are to be kept as impossible to set when it is changed. The policy does not apply if the password type set on the device is a pattern.

Password expiration

- Policy defines how long the password may be used and sets the time for the user to change the password on the device.

Allow unlock device using fingerprint

- The policy determines whether a user can use a fingerprint to unlock the device. The manufacturer may require the imposition of a specific type of password when the setting is enabled.

Allow the iris scanner

- The feature allows the user to configure the iris scanner and use this feature to unlock the device. This policy applies only to devices running Android 9.0 or later. The manufacturer may require the imposition of a specific type of password when the setting is enabled.

Allow face recognition

- The feature allows the user to configure facial recognition and use this feature to unlock the device. This policy applies only to devices running Android 9.0 or later. The manufacturer may require the imposition of a specific type of password when the setting is enabled.

Require lock screen message

- Policy determines whether a defined message is visible on the locked screen of the device.

Lock screen message

- In the window you can define the message that is sent to the device and displayed on the locked screen of the device. The global variables are active in the popup pane. So, if you set {UserDisplayName} to a device with this policy, a value matching the global variable for that user will be sent.

Require device lock with wrong password

- The policy allows you to enter a device lock after a certain number of unsuccessful attempts to enter the password by the user. The policy works simultaneously with the policy "Number of

attempts to unlock".

Number of unlocking attempts

- The policy determines the number of incorrect attempts to enter a password that the user can perform before blocking the device

Message on a blocked device

- Enter the message that you want to display on the blocked device

Phone number

- Enter the phone number to which the user can make a call when the device is locked

Manage business application updates

- The policy allows you to specify the hours for updating business applications on your device. The function is not applicable when the automatic app update mode is set to high priority.

Apps

Allow uninstall apps

- Policy determines whether the user can uninstall the applications installed on the device.

Allow access to public apps in the Google Play Store

- The policy determines whether a user has access to public apps in the Google Play Store.

Specify how to grant permissions for apps

- Policy determines how the permissions for applications are granted. Policy determines whether application permissions are granted automatically, are automatically discarded, or whether the user can decide.

Business apps updates

- The policy allows to define how business apps should be updated.

Allow install apps in metered connections

- The policy determines whether the device can install applications in metered connections. If your network has a data limit, you can define whether the device will install applications.

Force the use of Play Protect

- The policy forces the use of Play Protect to verify the security of unknown apps.

Functionality

Allow use of Bluetooth

- Policy determines whether you can use Bluetooth

Allow sharing via Bluetooth

- The policy specifies whether the user can share data via Bluetooth.

Allow use of NFC

- Policy defines whether you can use NFC. Available from Android 15.

Allow camera

- The policy allows to use of camera. If unchecked, the camera will not work in all apps, including the Proget app.

Allow microphone

- The policy allows to use of microphone. If unchecked, the microphone will not work in all apps, including the Proget app.

Allow configuring mobile networks

- Policy determines whether the user can change the mobile network settings such as network access points, operating mode, network operators.
 - Allow mobile data usage while roaming
 - Policy determines whether the user can use cellular data when the device is in roaming. If the policy is disabled, the user cannot use the Internet while the device is in roaming.

Allow tethering configuration and mobile hotspots

- Policy determines whether the user can set up a tethering and mobile hotspot.

Allow edit Wi-Fi configuration

- Policy determines whether the user can add new Wi-Fi connections. If policy is disabled, the ability to set up new connections is blocked. Wi-Fi connections which was added before policy implementation will continue to be active but will be not editable.

Specify settings for Wi-Fi sleep configuration

- Policy determines the Wi-Fi sleep settings when the device is idle.

Allow removing added Wi-Fi networks

- The policy specifies whether the user can delete Wi-Fi networks added by the administrator using the Wi-Fi profile.

Allow Airplane Mode

- Policy allows to enable airplane mode on your device. Available from Android 9.

Allow user-configured VPN

- Policy determines whether the user can manually configure the VPN profile and change the settings of already added VPN connections. VPN profiles which was added before policy implementation will continue to be active.

Allow outgoing calls

- Policy determines whether the user can make outgoing calls.

Allow SMS messages

- Policy determines whether the user can send and receive SMS.

Allow USB file transfer

- Policy determines whether the user can transfer data from and to the device using a USB connection.

Allow mounting physical media

- Policy determines whether the user can mounting physical media such as SD card and flash drive using USB OTG.

Set time automatically

- Policy determines whether the user can change the time settings. If the policy is enabled, the user cannot manually change the time on the device.

Set timezone automatically

- Policy determines whether the device can automatically change the time zone. If the policy is enabled, the user cannot change the time zone on the device.

Allowed input methods

- Policy determines whether the user can use any input method (for example, a keyboard), only the input methods provided by the device, or only the input methods provided by the device plus additional input methods you specify.
 - Allowed App

- Add an allowed app package ID, e.g. com.android.example

Allowed accessibility services

- Policy determine accessibility services that the user can access. By default, the user can use any accessibility service. System accessibility services may be for example Voice Assistant.
 - Allowed App
 - Add an allowed app package ID, e.g. com.android.example

Default launcher

- Policy determines the package ID of the launcher app that must be used on the device. For this rule to apply to the device, you must push the launcher app to the device.

Limit mobile data usage by apps

- Provide the package ID of apps that will not be able to use the internet via mobile data. Available from Android 9.

Force Always on VPN

- The policy forces indicated VPN app to maintain the connection continuously.
 - Add VPN app
 - Block internet access when VPN is not connected
 - The policy disable internet access if the VPN connection with the selected apps is not established. Available from Android 10.
 - Add exceptions
 - After adding apps to the exceptions, they will be able to connect to the internet despite the blockade being set. Available from Android 10.

Allow to change the screen wallpaper

- Policy determines whether the user can change the screen wallpaper

Allow backup services

- The policy determines whether the user can use backup services.

Hide the Proget icon

- If checked, the Proget application on the device will be hidden

Ask for access to device usage data

- If checked, the user will be asked to assign access to the usage data on the device

Hide Proget notification

- If checked, the Proget notification on the device will be hidden

Default notification for a managed device

- The notification will be displayed on a device managed by the Proget app

Security

Manage accounts on device

- Policy specifies the accounts the user can use. By default, the user can use all accounts except Google..

Allow take screenshots

- Policy defines if user may do screenshots

Allow developer mode

- Policy determines whether the user can enable Developer Mode. If the policy is disabled, the Developer Mode return to the default settings.

Allow safe boot of the device

- Policy determines whether the user can start safe mode on the device. In safe mode, the device starts up without the third party applications.

Allow factory reset

- Policy determines whether the user can restore the device to factory. Restoring device to factory removes the MDM agent and device will be unmanaged.

Use Factory Reset Protection Get Google ID

- The policy force the use of Factory Reset Protection. If the device is restored to factory settings, you will be required to enter the Google ID account details listed below.

Allow the user to deactivate the MDM agent

- The policy determines whether the user can deactivate the device from the MDM agent.

Allow clearing of application data

Deprecated

- Policy allows to clear Proget app data. Clearing the data will disconnect the device from the system.

Allow installation of non Google Play apps

- Policy determine whether a user can install non-Google Play apps using the ACTION_INSTALL_PACKAGE mechanism.

Require device registration in Microsoft Entra ID

- The policy enforces user registration in Microsoft Entra ID. If the policy is enabled, the device will be instructed to sign in to a Microsoft account in purpose of its registration
 - Automatically set the user login
 - Setting this field will automatically insert the specified user login when logging into Microsoft account.

Allow using two SIM cards at the same time

- Policy determines whether you can use two SIM cards at the same time if the device supports two SIM card slots. If the policy is turned off, the device will be blocked until the second SIM card is removed.

Block the SIM card with the PIN code for slot 1 (Samsung only)

- Policy defines whether the device should save a permanent PIN code to unlock the SIM card. Turning on a permanent PIN will block the company's SIM card usage on another device. Each time a company device is turned on, device will automatically unlocks the SIM card using the permanent PIN code. However, if the SIM card is moved to another device, it will remain locked because the PIN code is not known to the user. The policy applies to slot 1.

Block the SIM card with the PIN code for slot 2 (Samsung only, if applicable)

- Policy defines whether the device should save a permanent PIN code to unlock the SIM card. Turning on a permanent PIN will block the company's SIM card usage on another device. Each time a company device is turned on, device will automatically unlocks the SIM card using the permanent PIN code. However, if the SIM card is moved to another device, it will remain locked because the PIN code is not known to the user. The policy applies to slot 2 (if applicable).

Force cyclic downloads from the server

- Policy specifies whether the device should acquire data from the MDM server every specified time interval. Enabling the policy forces the device to contact the server. The date of the last connection will be recorded on the server each time.

Force cyclic data transfer to the server

- Policy determines whether the device should send data to the MDM server every specified time interval. Enabling the policy forces the device to contact the server. The date of the last connection will be stored on the server each time.

Maximum time to lock

- Policy set the maximum time for user activity until the device will lock. This limits the length that the user can set in device settings.

Action after exceeding the inactivity time

- Policy determines whether a defined action should be taken (Clear device data, Clear company data or Block device) after a specified period of inactivity. Action will be taken automatically if the last contact of the device with the server exceeds the defined inactivity time.
 - Inactivity time (in days)
 - Action
 - Message on a blocked device
 - Enter the message that you want to display on the blocked device
 - Phone number
 - Enter the phone number to which the user can make a call when the device is locked

Allow using Smart Lock

- The policy defines the possibility of using Smart Lock on device.
 - Bluetooth
 - The policy allows you to automatically unlock your phone when it is connected via Bluetooth to a trusted device, such as a watch or an in-car speakerphone.
 - NFC
 - The policy allows you to automatically unlock your phone using a trusted NFC tag.
 - Trusted places
 - The policy allows you to configure Trusted places. The device will stay automatically unlocked within a radius of up to 80 meters from the Trusted place.
 - Face

- The device will automatically unlock when it recognizes your face. If you set up a trusted face, the device will search for it each time it starts, and it will unlock when it recognizes it.
- On-body
 - The policy allows you to leave the device unlocked when the device is next to the user (e.g. in his hand, pocket or bag). The device will be locked only after the device has been put down (e.g. on a table); the lock will be activated automatically within a minute.
- Voice
 - The policy allows you to unlock the Google Assistant when saying "Ok Google" on the lock screen, after the device recognized the previously recorded voice. You can give Google commands or open websites without the need to manually unlock the device.

Service password

Deprecated

- The service password allows to define a password to unlock a blocked device, i.e. lost mode. The password defined in the policy works simultaneously with the password on the device card.

Lock screen notifications

- Policy allows you to specify the maximum level of detail of information in notifications on a locked screen (the user can always reduce this level manually).

Store photos from locked device

- Policy defines the maximum time for storing photos on the server taken during the lockdown of the device.

Managing operating system updates

- The policy allows to specify how system updates are managed on your device.

Private DNS Management

- The policy defines how Private DNS is configured on the device. Opportunistic mode allows the device to automatically use Private DNS if available. Specified host requires entering a specific DNS-over-TLS server. This policy applies only to devices running Android 10 or later.

Location

Manage location modes

- The policy allows to define the mode in which the location on the device should be run. Feature available on devices with Android lower than 9.

Manage location state

- The policy allows to set location services on the device. Available from Android 11.

Android Enterprise Profile Owner

Updated: Jun 8, 2026

Password - Device

Level of password required

- The policy specifies the password level on the device..
 - No level allows the device to have no password
 - The low level allows a pattern and an uncomposed numeric password
 - Medium level allows a numeric password with a minimum of 4 compound characters
 - High level requires a complex numeric password with a minimum of 8 characters or an alphanumeric password with a minimum of 6 characters
 - Custom – numeric, requires a numeric password with a minimum length of 4 characters
 - Custom – complex numeric, requires a complex numeric password with a minimum length of 4 characters
 - Custom – alphanumeric, requires an alphanumeric password with a minimum length of 4 characters, with the option to specify the required number of numeric, lowercase, uppercase, and special characters

Minimum password length

- The policy defines the minimum length of the password used on the device.

Required number of numerical characters

- Policy defines the number of numerical characters in the device password.

Required number of lower case characters

- Policy defines the number of lower case characters in the device password.

Required number of capital characters

- Policy defines the number of A-Z capital characters in the device password.

Required number of special characters

- Policy defines the number of special `!@#$%^&*()_+<>:"'{}|` characters in the device password.

Number of attempts to unlock

- Policy defines the number of incorrect password attempts followed by a container wipe. For COPE activation, the device data will be wiped. The policy does not support Direct Boot if restoring the device to factory settings is forbidden.

Number of passwords saved

- Policy defines how many prior passwords the device should remember while changing the password.

Allow unlock device using fingerprint

- Policy determines whether the user can use a fingerprint to unlock the device. If the policy is disabled, the user must enter a password to unlock the device.

Allow the iris scanner

- The function allows the user to configure the iris scanner and use this function to unlock the device. This rule applies only to devices running Android 9.0 and later.

Allow face recognition

- The function allows the user to configure face recognition and use this function to unlock the device. This rule applies only to devices running Android 9.0 and later.

Require lock screen message (COPE only)

- Policy determines whether a defined message is visible on the locked screen of the device.

Lock screen message (COPE only)

- In the window you can define the message that is sent to the device and displayed on the locked screen of the device. The global variables are active in the popup pane. So, if you set {UserDisplayName} to a device with this policy, a value matching the global variable for that user will be sent.

Password - Container

Level of password required

- The policy specifies the password level on the device..
 - No level – allows the device to have no password
 - The low level allows a pattern and an uncomposed numeric password
 - Medium level allows a numeric password with a minimum of 4 compound characters

- High level requires a complex numeric password with a minimum of 8 characters or an alphanumeric password with a minimum of 6 characters
- Custom – numeric, allows a numeric password with a minimum length of 4 characters
- Custom – complex numeric, allows a complex numeric password with a minimum length of 4 characters
- Custom – alphanumeric, requires an alphanumeric password with a minimum length of 4 characters, with the option to specify the required number of numeric, lowercase, uppercase, and special characters

Minimum password length

- The policy defines the minimum length of the password used on the device.

Required number of numerical characters

- Policy defines the number of numerical characters in the device password.

Required number of lower case characters

- Policy defines the number of lower case characters in the device password.

Required number of capital characters

- Policy defines the number of A-Z capital characters in the device password.

Required number of special characters

- Policy defines the number of special !@#\$%^&*()_+<>:"'{}| characters in the device password.

Number of attempts to unlock

- Policy defines the number of incorrect password attempts followed by a container wipe. For COPE activation, the device data will be wiped. The policy does not support Direct Boot if restoring the device to factory settings is forbidden.

Number of passwords saved

- The policy determines what number of passwords are to be kept as impossible to set when it is changed. The policy does not apply if the password type set on the device is a pattern.

Password expiration

- Policy defines how long the password may be used and sets the time for the user to change the password on the device.

Allow unlock device using fingerprint

- The policy determines whether a user can use a fingerprint to unlock the device. The manufacturer may require the imposition of a specific type of password when the setting is enabled.

Allow the iris scanner

- The feature allows the user to configure the iris scanner and use this feature to unlock the device. This policy applies only to devices running Android 9.0 or later. The manufacturer may require the imposition of a specific type of password when the setting is enabled.

Allow face recognition

- The feature allows the user to configure facial recognition and use this feature to unlock the device. This policy applies only to devices running Android 9.0 or later. The manufacturer may require the imposition of a specific type of password when the setting is enabled.

Apps

Allow uninstall apps

- Policy determines whether the user can uninstall the applications installed in the container.

Allow access to public apps in the Google Play Store

- The policy determines whether a user has access to public apps in the Google Play Store.

Specify how to grant permissions for apps

- Policy determines how the permissions for applications are granted. Policy determines whether application permissions are granted automatically, are automatically discarded, or whether the user can decide. For devices with Android 12 and above, automatic permissions related to sensors (e.g. permission.CAMERA) do not work.

Business apps updates

- The policy allows to define how business apps should be updated.

Allow install apps in metered connections

- The policy determines whether the device can install applications in metered connections. If your network has a data limit, you can define whether the device will install applications.

Force the use of Play Protect

- The policy forces the use of Play Protect to verify the security of unknown apps.

Suspend use of private apps (COPE only)

- The policy allows to suspend the use of private apps. When personal apps are suspended the device can only be used for calls.

Allow sharing of data from equivalent applications between spaces

- Policy allows sharing of data from equivalent apps located between private and work spaces. The feature is available from Android 11.
 - Allowed App
 - `policy.field.applications.allowed_cross_profile_apps_list.description`

Functionality

Allowed input methods

- Policy determines whether the user can use any input method (for example, a keyboard), only the input methods provided by the device, or only the input methods provided by the device plus additional input methods you specify.
 - Allowed App
 - Add an allowed app package ID, e.g. `com.android.example`

Allow camera

- The policy allows to use of camera. If unchecked, the camera will not work in all apps, including the Proget app.

Allowed accessibility services

- Policy determine accessibility services that the user can access. By default the user can use any accessibility service. System accessibility services may be for example Voice Assistant.
 - Allowed App
 - Add an allowed app package ID, e.g. `com.android.example`

Limit mobile data usage by apps

- Provide the package ID of apps that will not be able to use the internet via mobile data. Available from Android 9.

Allow Airplane Mode (COPE only)

- Policy allows to enable airplane mode on your device.

Allow use of Bluetooth (COPE only)

- Policy determines whether you can use Bluetooth
 - Allow sharing via Bluetooth (COPE only)
 - The policy specifies whether the user can share data via Bluetooth.

Allow use of NFC (COPE only)

- Policy defines whether you can use NFC. Available from Android 15.

Allow camera (COPE only)

- The policy allows to use of camera. If unchecked, the camera will not work in all apps, including the Proget app.

Allow cell broadcast configuration (COPE only)

- The policy allows for cell broadcast configuration. Cell broadcast consists in sending information to network users within the range of one BTS base station.

Allow date configuration (COPE only)

- The policy allows to configure the date, time and timezone in the settings.

Allow configuring mobile networks (COPE only)

- Policy determines whether the user can change the mobile network settings such as network access points, operating mode, network operators.

Allow private DNS configuration (COPE only)

- The policy allows to change the private DNS configuration.

Allow tethering configuration and mobile hotspots (COPE only)

- Policy determines whether the user can set up a tethering and mobile hotspot.

Allow edit Wi-Fi configuration (COPE only)

- Policy determines whether the user can add new Wi-Fi connections. If policy is disabled, the ability to set up new connections is blocked. Wi-Fi connections which was added before policy implementation will continue to be active but will be not editable.

Allow content capture (COPE only)

- The policy determines whether capturing content for later use by AI is allowed.

Allow content suggestions (COPE only)

- The policy determines whether the user can receive tailored content suggestions based on content capture.

Maximum turn off time of work profile in days (COPE only)

- The policy determines maximum time the work profile is allowed to be turned off. If the profile is turned off for longer, personal apps are suspended on the device.
 - Turn off time (in days)

Allow all input methods (COPE only)

- Policy allows the use of all data input methods (e.g. keyboard), after unchecking, only system methods are allowed. This rule applies only to devices running Android 12 and later.

Force Always on VPN

- The policy forces indicated VPN app to maintain the connection continuously.
 - Add VPN app
 - Block internet access when VPN is not connected
 - The policy disable internet access if the VPN connection with the selected apps is not established. Available from Android 10.
 - Add exceptions
 - After adding apps to the exceptions, they will be able to connect to the internet despite the blockade being set. Available from Android 10.

Ask for access to device usage data

- If checked, the user will be asked to assign access to the usage data on the device

Default notification for a managed device

- The notification will be displayed on a device managed by the Proget app

Security

Manage accounts on device

- The policy specifies the accounts the user can use. By default, the user can use all accounts except Google.

Allow take screenshots

- Policy defines if user can take screenshots. This rule applies only to container.

Allow copying of text between the container and the device

- Policy determines whether the user can copy between spaces, content generated in the container or device.

Allow searching for business contacts in private space

- The Policy determines whether user can search for business contacts in private space.

Allow you to identify your work contact for incoming calls

- The Policy determines whether caller ID information from the managed profile will be shown in the personal space.

Allow the user to deactivate the MDM agent

- The policy determines whether the user can deactivate the device from the MDM agent.

Allow clearing of application data

Deprecated

- Policy allows to clear Proget app data. Clearing the data will disconnect the device from the system.

Require device registration in Microsoft Entra ID

- The policy enforces user registration in Microsoft Entra ID. If the policy is enabled, the device will be instructed to sign in to a Microsoft account in purpose of its registration.
 - Automatically set the user login
 - Setting this field will automatically insert the specified user login when logging into Microsoft account.

Force cyclic downloads from the server

- Policy specifies whether the device should acquire data from the MDM server every specified time interval. Enabling the policy forces the device to contact the server. The date of the last connection will be recorded on the server each time.

Force cyclic data transfer to the server

- Policy determines whether the device should send data to the MDM server every specified time interval. Enabling the policy forces the device to contact the server. The date of the last connection will be stored on the server each time.

Maximum time to lock

- Policy set the maximum time for user activity until the device will lock. This limits the length that the user can set in device settings.
 - Time to lock (in minutes)

Action after exceeding the inactivity time

- Policy determines whether a defined action should be taken (Clear company data or Clear device data for COPE) after a specified period of inactivity. Action will be taken automatically if the last contact of the device with the server exceeds the defined inactivity time.
 - Inactivity time (in days)
 - Action

Allow Bluetooth contacts sharing

- Policy determines whether a user can share contacts from the workspace via Bluetooth.

Allow using Smart Lock

- The policy defines the possibility of using Smart Lock on device.
 - Bluetooth
 - The policy allows you to automatically unlock your phone when it is connected via Bluetooth to a trusted device, such as a watch or an in-car speakerphone.
 - NFC
 - The policy allows you to automatically unlock your phone using a trusted NFC tag.
 - Trusted places
 - The policy allows you to configure Trusted places. The device will stay automatically unlocked within a radius of up to 80 meters from the Trusted place.
 - Face
 - The device will automatically unlock when it recognizes your face. If you set up a trusted face, the device will search for it each time it starts, and it will unlock when it recognizes it.
 - On-body
 - The policy allows you to leave the device unlocked when the device is next to the user (e.g. in his hand, pocket or bag). The device will be locked only after the device has been put down (e.g. on a table); the lock will be activated automatically within a minute.
 - Voice

- The policy allows you to unlock the Google Assistant when saying "Ok Google" on the lock screen, after the device recognized the previously recorded voice. You can give Google commands or open websites without the need to manually unlock the device.

Service password

Deprecated

- The service password allows to define a password to unlock a blocked device, i.e. lost mode. The password defined in the policy works simultaneously with the password on the device card.

Allow installation of non Google Play apps

- The policy determines whether the user can install non-Google Play store apps. 'Do not allow' policy is available on devices with Android 10 or later, for devices with Android older than 10 the policy will work as 'Allow only in private space'.

Allow take screenshots (COPE only)

- Policy defines if user may do screenshots

Use Factory Reset Protection (COPE only) Get Google ID

- The policy force the use of Factory Reset Protection. If the device is restored to factory settings, you will be required to enter the Google ID account details listed below.

Allow developer mode (COPE only)

- Policy determines whether the user can enable Developer Mode. If the policy is disabled, the Developer Mode return to the default settings.

Managing operating system updates (COPE only)

- The policy allows to specify how system updates are managed on your device.

Android

Updated: Jun 8, 2026

Password

Level of password required

- The policy specifies the password level on the device.
 - The low level allows a pattern and an uncomposed numeric password
 - Medium level allows a numeric password with a minimum of 4 compound characters
 - High level requires a complex numeric password with a minimum of 8 characters or an alphanumeric password with a minimum of 6 characters

Minimum password length

- The policy defines the minimum length of the password used on the device.

Required number of numerical characters

- Policy defines the number of numerical characters in the device password.

Required number of lower case characters

- Policy defines the number of lower case characters in the device password.

Required number of capital characters

- Policy defines the number of A-Z capital characters in the device password.

Required number of special characters

- Policy defines the number of special `!@#$%^&*()_+<>:"'{}|` characters in the device password.

Number of attempts to unlock

- Policy defines the number of incorrect password attempts followed by a device wipe.

Number of passwords saved

- The policy determines what number of passwords are to be kept as impossible to set when it is changed. The policy does not apply if the password type set on the device is a pattern.

Password expiration

- Policy defines how long the password may be used and sets the time for the user to change the password on the device.

Allow unlock device using fingerprint

- The policy determines whether a user can use a fingerprint to unlock the device. The manufacturer may require the imposition of a specific type of password when the setting is enabled.

Allow the iris scanner

- The feature allows the user to configure the iris scanner and use this feature to unlock the device. This policy applies only to devices running Android 9.0 or later. The manufacturer may require the imposition of a specific type of password when the setting is enabled.

Allow face recognition

- The feature allows the user to configure facial recognition and use this feature to unlock the device. This policy applies only to devices running Android 9.0 or later. The manufacturer may require the imposition of a specific type of password when the setting is enabled.

Security

Allow the user to deactivate the MDM agent

- The policy determines whether the user can deactivate the device from the MDM agent.

Allow clearing of application data

Deprecated

- Policy allows to clear Proget app data. Clearing the data will disconnect the device from the system.

Action after exceeding the inactivity time

- Policy determines whether a defined action should be taken (Clear device data or Clear company data) after a specified period of inactivity. Action will be taken automatically if the last contact of the device with the server exceeds the defined inactivity time.

Force cyclic downloads from the server

- Policy specifies whether the device should acquire data from the MDM server every specified time interval. Enabling the policy forces the device to contact the server. The date of the last connection will be recorded on the server each time.

Force cyclic data transfer to the server

- Policy determines whether the device should send data to the MDM server every specified time interval. Enabling the policy forces the device to contact the server. The date of the last connection will be stored on the server each time.

Require device encryption

- Policy forces the device to be encrypted if it is supported by the device.

Allow using Smart Lock

- The policy defines the possibility of using Smart Lock on device.
 - Bluetooth
 - The policy allows you to automatically unlock your phone when it is connected via Bluetooth to a trusted device, such as a watch or an in-car speakerphone.
 - NFC
 - The policy allows you to automatically unlock your phone using a trusted NFC tag.
 - Trusted places
 - The policy allows you to configure Trusted places. The device will stay automatically unlocked within a radius of up to 80 meters from the Trusted place.
 - Face
 - The device will automatically unlock when it recognizes your face. If you set up a trusted face, the device will search for it each time it starts, and it will unlock when it recognizes it.
 - On-body
 - The policy allows you to leave the device unlocked when the device is next to the user (e.g., in his hand, pocket, or bag). The device will be locked only after the device has been put down (e.g., on a table); the lock will be activated automatically within a minute.
 - Voice
 - The policy allows you to unlock the Google Assistant when saying "Ok Google" on the lock screen, after the device recognized the previously recorded voice. You can give Google commands or open websites without the need to manually unlock the device.

Service password

Deprecated

- The service password allows to define a password to unlock a blocked device, i.e. lost mode. The password defined in the policy works simultaneously with the password on the device card.

iOS

Updated: Jan 13, 2025

Password

Policy defines requirements for device password. Once done, user must set the device password.

- Policy defines the minimum length of the password used on the device.

Password length

- The policy defines the minimum length of the password used on the device.

Required number of special characters

- Policy defines the number of special `!@#$%^&*()_+<>:"'{}|` characters in the device password.

Number of attempts to unlock

- Policy defines the number of incorrect password attempts followed by a device wipe.

Number of passwords saved

- Policy defines how many prior passwords the device should remember while changing the password.

Password expiration (in days)

- Policy defines how long the password may be used and sets the time for the user to change the password on the device. For value 0, the password does not expire.

Device block grace period

- Policy defines the maximum time for user to unblock the device again without entering the password.

Allow Touch ID or Face ID unlock

- Policy specifies whether user can use Touch ID or Face ID to unlock the device.

Allow device password changes (supervisor mode)

- Policy determines whether a user can add, change, or remove device passwords.

Allow modifying Touch ID or Face ID (supervisor mode)

- Policy specifies whether user can modify Touch ID or Face ID.

Max inactive time (in minutes)

- Policy defines user inactive time duration, then blanks the screen and blocks the device with the current password. On iOS 13 and later, the maximum inactivity time is 5 minutes.

Allow to auto unlock device

- Policy determines whether the automatic device unlock function is available. Available on iOS 14.5 and later.

Apps

Allow using iTunes store

- Policy defines the use of iTunes store.

Allow use News app (supervisor mode)

- Policy determines whether the user can use the News app.

Allow use podcasts (supervisor mode)

- Policy determines whether the user can add new podcasts.

Allow App Clips (supervisor mode)

- If unchecked, prevents a user from adding any App Clips, and removes any existing App Clips on the device. Available in iOS 14.0 and later.

Allow use of Game Center (supervisor mode)

- Policy determines whether the Game Center is available on the device. If the policy is disabled, the Game Center icon is removed from the home screen and the user cannot use the Game Center.
 - Allow multiplayer gaming (supervisor mode)
 - Policy determines whether the user can use multiplayer in games. If the "Allow add friends to Game Center" policy is disabled, the user can only play multiplayer games with existing friends. If the policy is disabled, the user cannot use multiplayer in games and cannot add new friends to the Games Center.
 - Adding Friends from Game Center (supervisor mode)
 - If unselected, prohibits adding friends to Game Center.

Allow use of Safari (supervisor mode)

- If unselected, disables the Safari web browser app, and its icon is removed from the Home screen. This setting also prevents users from opening web clips.
 - Allow autocomplete of fields
 - Policy defines if browser may use autocomplete.
 - Force fraud warning
 - Policy determines whether the Safari warns user if they visit a web site marked as threatened or compromised.
 - Allow use of JavaScript
 - Policy determines whether Safari may use JavaScript. Disabling this feature will block the use of the Proget app store.
 - Allow pop-ups
 - Policy defines if browser should block pop-ups.
 - Accept cookies
 - Policy defines if browser may use cookies.

Default domains

Email domains

- Policy defines email domains that will be considered as default email domains. Email addresses from other domains will be highlighted as external email in Mail app.

Web domains

- Policy defines domains that will be considered as default. This means that if you download a document from the default domain using Safari, it will be considered a managed item. Depending on the open-in policy, the document can be opened by managed or unmanaged applications.

Disallow manually adding passwords to the keychain

- The policy determines whether users can manually add passwords to the keychain. If unchecked, users can add site, user and password in password settings.

Password AutoFill domains

- Policy defines whether users can save passwords in Safari from URLs matching the listed patterns.

Allow to install and update applications (supervisor mode)

- If unselected, disables the App Store, and its icon is removed from the Home screen. Users are unable to install or update their apps.

Allow to install and update applications via the App Store (supervisor mode)

- Policy determines whether an App Store application is available on the device. If the policy is disabled, you will still be able to use iTunes app and update installed applications.

Allow automatic app downloads (supervisor mode)

- Policy determines whether the device can automatically download applications purchased on other device. Policy does not affect updates to existing apps.

Allow QuickPath keyboard (supervisor mode)

- If unselected, disables QuickPath keyboard.

Allow Files to access network drives (supervisor mode)

- If unselected, prevents connecting to network drives in the Files app.

Allow Files to access USB drivers (supervisor mode)

- If unselected, prevents connecting to any connected USB devices in the Files app.

Allow Find My Device (supervisor mode)

- If unselected, disables Find My Device in the Find My app.

Allow Find My Friends (supervisor mode)

- If unselected, disables Find My Friends in the Find My app.

Allow to write contacts to unmanaged accounts

- If selected, managed apps can write contacts to unmanaged contacts accounts. If allow open documents from managed sources in unmanaged destinations is selected, this restriction has no effect.

Allow system apps removal (supervisor mode)

- If unselected, disables the removal of system apps from the device.

Require trusted TLS certificates for AirPrint (supervisor mode)

- If selected, requires trusted certificates for TLS printing communication.

Force automatic update of work apps

- The policy enforces automatic updates of work apps on devices. The apps will be updated when a new version is detected in the App Store.

Education

Allow remote screen observation (supervisor mode)

- If unselected, disables remote screen observation by the Classroom app. If allow screenshot is unselected, the Classroom app doesn't observe remote screens.

Require automatically join to classes (supervisor mode)

- If selected, automatically gives permission to the teacher's requests without prompting the student.

Require request permission to leave classes (supervisor mode)

- If selected, a student enrolled in an unmanaged course through Classroom requests permission from the teacher when attempting to leave the course.

Allow app and device lock (supervisor mode)

- If selected, allows the teacher to lock apps or the device without prompting the student.

Allow screen observation (supervisor mode)

- If selected and Allow remote screen observation is also selected, a student enrolled in a managed course via the Classroom app automatically gives permission to that course teacher's requests to observe the student's screen without prompting the student.

Functionality

Force device periodically connection to the server

- Policy determines whether the device have to connect to the MDM server at a specific time interval. Enabling this policy forces the device to contact the server periodically. The date of the last connection will be saved on the server each time.

Allow camera

- The policy allows to use of camera. If unchecked, the camera will not work in all apps, including the Proget app.
 - Allow using FaceTime (supervisor mode)

- If unselected, hides the FaceTime app.

Allow to take screenshots and record screen

- Policy determines whether the user can take screenshots and record the screen.

Allow use AirDrop (supervisor mode)

- Policy determines whether the user can use the AirDrop sharing feature. If the policy is disabled, the user cannot use the AirDrop feature in any applications and the AirDrop option is removed from the Control Center.

Allow use iMessage (supervisor mode)

- Policy determines whether the user can use iMessage.

Allow use Apple Music service (supervisor mode)

- Policy determines whether the user has access to Apple Music service. If the policy is disabled, the Music application returns to the classic mode.

Allow use radio service (supervisor mode)

- Policy determines whether the user can use iTunes radio.

Allow voice dialing while device is locked

- Policy determines whether the user can make voice calls while the device is locked.

Allow using Siri assistant

- Policy defines using the Personal Assistant and Knowledge Navigator.
 - Allow using Siri assistant with blocked screen
 - Policy defines using the Personal Assistant and Knowledge Navigator when the device is blocked.
 - Enable Siri profanity filter (supervisor mode)
 - Policy determines whether the profanity filter is enabled in Siri.
 - Show user-generated content in Siri (supervisor mode)
 - Policy defines whether a user-generated content is displayed when using Siri.
 - Prohibit connecting to Siri servers when dictating
 - Policy disables connections to Siri Assistant servers for dictation. Available on iOS 14.5 and above.

- Prohibit connecting to Siri servers for translation
 - Policy disables connections to Siri Assistant servers for translation purposes. Available on iOS 15 and above.

Allow iBooks Store (supervisor mode)

- Policy determines whether the iBook Store is available on the device. If the policy is disabled, the user does not have access to the iBooks Store.

Allow removing apps (supervisor mode)

- Specify whether a user can remove apps from an iOS device. Applying this rule to an unsupervised device may have unexpected results.

Allow purchasing with apps

- Policy defines purchasing with apps.

iTunes password required for purchases

- Policy defines if iTunes password is required for purchasing with apps.

Make iCloud backup copy

- Policy defines if user may make a backup copy in iCloud.

Synchronization of documents with iCloud (supervisor mode)

- If unselected, disables document and key-value syncing to iCloud.

Allow keychain sync with iCloud

- If unchecked, disable iCloud keychain syncing.

Allow managed apps to store data in iCloud

- Policy determines whether managed applications can store internal application data in iCloud.

Allow backup of enterprise books

- Policy determines whether the device backup may include an enterprise books.

Allow notes and highlights sync for enterprise books

- Policy determines whether the device can synchronize notes and highlights for enterprise books.

Allow iCloud photo sharing

- Policy determines whether the user can enable photo sharing with iCloud. If the policy is disabled, the user can not share the stream of photos to other people. If policy is disabled, images and videos may be lost.

Allow use iCloud Photo Library (supervisor mode)

- Policy determines whether a user can upload photos to iCloud Photo Library.

Allow iCloud Private Relay (supervisor mode)

- Policy determines whether the iCloud Private Relay internet privacy service is available. Available on iOS 15 and above.

Allow privacy protection in Mail

- If checked, your IP address is hidden from senders and remote content is downloaded privately in the background on receipt of the message (rather than while viewing it). Available on iOS 15.2 and above.

Allow use of NFC (supervisor mode)

- Policy determines whether you can use NFC. Available on iOS 14.2 and above.

Allow use My Photo Stream

- Policy determines whether the user can enable My Photo Stream. If the policy is disabled, photos in My Photo Stream will be deleted from the device and the Camera Roll will no longer be added to My Photo Stream.

Allow data synchronization in roaming

- Policy defines if the device may automatically synchronize data in roaming.

Force encrypted backup copies

- Policy defines if encrypted backup copies must be forced.

Allow unpaired devices to start recovery mode (supervisor mode)

- Policy allows recovery devices to run on an unpaired device. Requires a supervised device. Available on iOS 14.5 and above.

Force limited ad tracking

- Policy determines whether applications on the device can use the Advertising Identifier to provide targeted ads to users.

Allow Apple personalized advertising

- If unchecked, limits Apple personalized advertising. Available in iOS 14 and later.

Allow Erase All Content and Settings (supervisor mode)

- Policy determines whether the user can use the Erase All Content and Settings option to wipe the device.

Accept untrusted TLS certificates

- Policy defines if untrusted TLS certificates may be accepted.

Allow automatic updates to certificate trust settings

- Policy determines whether the device allows automatic updates for trusted certificates over a wireless connection.

Allow installing additional configuration profiles (supervisor mode)

- Policy determines whether the user can install additional configuration profiles on the device.

Allow modifying account settings (supervisor mode)

- Policy determines whether the user can change the account settings which is added to the device. If the policy is disabled, the user cannot add new accounts and modify the settings of the accounts currently in use.

Allow Bluetooth changes (supervisor mode)

- Policy determines whether the user can change the Bluetooth settings on the device.

Allow modifying cellular data app settings (supervisor mode)

- Policy determines whether the user can change the mobile data usage settings for the applications installed on the device.

Allow device name changes (supervisor mode)

- Policy determines whether the user can change the device name.

Allow modifying Find My Friends settings (supervisor mode)

- Policy determines whether the user can change the "Find my friends" settings. The policy works if Find My Friend application is installed on the device.

Allow notification changes (supervisor mode)

- Policy determines whether the user can change the notification settings on the device.

Allow configuring restrictions (supervisor mode)

- Policy determines whether the user can configure their own restrictions on the device to prevent access to applications or device functionality.

Allow wallpaper changes (supervisor mode)

- Policy determines whether the user can change the wallpaper of the device screen.

Allow join only Wi-Fi networks installed by profiles (supervisor mode)

- Policy determines whether the device can join only to Wi-Fi networks installed by the management profile. Available on iOS 14.5 and above.

Allow pairing with a computer that is not an Apple Configurator (supervisor mode)

- Policy determines whether the device can be paired with a computer that is not an Apple Configurator.

Enable Activation Lock for devices with Apple Business Manager (supervisor mode)

- The policy enforces the use of Activation Lock for devices in supervisor mode with Apple Business Manager.

Allow Activation Lock (supervisor mode)

- The policy allows Activation Lock for devices in supervisor mode.

Allow open documents from managed sources in unmanaged destinations

- Policy determines whether the user can open documents and attachments from managed applications and accounts in personal applications. Safari and AirDrop will continue to display all applications as a possible source where the user can open documents regardless of the setting for this rule, or the rule "Allow documents from unmanaged sources in managed destinations".

Allow documents from unmanaged sources in managed destinations

- Policy determines whether the user can open documents and attachments from personal applications and accounts in managed applications. Safari and AirDrop will continue to display all applications as a possible source where the user can open documents regardless of the setting for this rule, or the rule "Allow open documents from managed sources in unmanaged destinations".

Force AirDrop to be unmanaged

- Policy determines whether AirDrop is to be seen as a source for opening in managed applications.

Allow use Handoff

- Policy determines whether the user can use the feature to transfer user activities among multiple devices associated with the user.

Allow Internet results in Spotlight (supervisor mode)

- Policy determines whether the user can use Spotlight search returns to Internet search when searching for content on a device.

Send diagnostic data to Apple

- Policy defines if diagnostic data should be sent to Apple.
 - Allow modifying diagnostics settings (supervisor mode)
 - Policy determines whether the user can change the diagnostic settings.

Enable Apple Watch wrist detection

- Policy determines whether the Apple Watch must use the wrist detection function.

Allow pairing with Apple Watch (supervisor mode)

- Policy determines whether the user can pair the device with an Apple Watch.

Require device passcode on first AirPlay pairing

- Policy determines whether a password is required during the first pairing with AirPlay devices. If policy is enabled, all devices receiving an AirPlay request, must use a pairing password.

Allow use predictive keyboard (supervisor mode)

- Policy determines whether the user can use predictive keyboards.

Allow use keyboard shortcuts (supervisor mode)

- Policy determines whether the user can use keyboard shortcuts on the device keyboard.

Allow use auto-correction (supervisor mode)

- Policy determines whether the user can use keyboard auto-correction.

Allow use spell check (supervisor mode)

- Policy determines whether the user can use spell checking when writing text.

Allow use Define (supervisor mode)

- The policy determines whether the user can use the Define function to search for definitions with a double click.

Show Wallet notifications in Lock screen

- Policy determines whether Wallet notifications are displayed on a locked device screen.

Show Control Center in lock screen

- Policy determines whether the user can access Control Center on the lock screen.

Show Notification Center in lock screen

- Policy determines whether the user access the Notifications view in Notification Center on the lock screen.

Show Today view in lock screen

- Policy determines whether the user can access the Today view in Notification Center on the lock screen.

Allow AirPrint (supervisor mode)

- If unselected, disables AirPrint.

Allow AirPrint credentials storage (supervisor mode)

- If unselected, disables keychain storage of user name and password for AirPrint.

Allow AirPrint iBeacon discovery (supervisor mode)

- If unselected, disables iBeacon discovery of AirPrint printers, which prevents spurious AirPrint Bluetooth beacons from phishing for network traffic.

Allow cellular plan modification (supervisor mode)

- If unselected, users can't change any settings related to their cellular plan.

Allow dictation (supervisor mode)

- If unselected, disallows dictation input.

Allow eSIM modification (supervisor mode)

- If unselected, disables modifications to the eSIM setting.

Allow password autofill (supervisor mode)

- If unselected, disables the AutoFill Passwords feature in iOS (with Keychain and third-party password managers) and the user isn't prompted to use a saved password in Safari or in apps.

Allow password request from nearby devices (supervisor mode)

- If unselected, disables requesting passwords from nearby devices. Feature limited to requesting Wi-Fi access password.

Allow password sharing via AirDrop (supervisor mode)

- If unselected, disables sharing passwords with the Airdrop Passwords feature.

Allow personal hotspot modification (supervisor mode)

- If unselected, disables modifications of the personal hotspot setting.

Allow setup to new device (supervisor mode)

- If unselected, disables the prompt to set up new devices that are nearby.

Allow unmanaged apps to read contacts from managed accounts

- If unselected, unmanaged apps can read from managed contacts accounts. If Allow open documents from managed sources in unmanaged destinations is selected, this restriction has no effect. Also available for user enrollment.

Allow connect devices via USB (supervisor mode)

- If unselected, allows the device to always connect to USB accessories while locked.

Allow create VPN (supervisor mode)

- If unselected, disables the creation of VPN configurations.

Delayed OS updates (supervisor mode)

- If selected, delays user visibility of OS updates.

Delay software updates (supervisor mode)

- Sets how many days to delay a software update on the device. With this restriction in place, the user doesn't see a software update until the specified number of days after the software update release date.

Require authentication before password autofill (supervisor mode)

- If selected, the user must authenticate before passwords or credit card information can be autofilled in Safari and Apps. If this restriction isn't enforced, the user can toggle this feature in

Settings. Only supported on devices with Face ID or Touch ID.

Require automatic date and time (supervisor mode)

- If selected, enables the Set Automatically feature in Date & Time and can't be disabled by the user. The device's time zone is updated only when the device can determine its location using a cellular connection or Wi-Fi with location services enabled.

Require turned on Wi-Fi (supervisor mode)

- If selected, prevents Wi-Fi from being turned off in Settings or Control Center, even by entering or leaving Airplane Mode. It does not prevent selecting which Wi-Fi network to use.

Require Managed Pasteboard

- Helps control the pasting of content from an app that's using Open In management by following the Managed Open In restrictions in force. Apple apps that work with the managed pasteboard include Calendar, Files, Mail, and Notes. Third-party apps are controlled based on whether or not they are managed. When a user attempts to paste content where it isn't permitted, a Paste Not Allowed notice appears along with the organization's name (which can be changed using the Settings command).

Allow Rapid Security Response installation (supervisor mode)

- The policy determines whether a user can install Rapid Security Response. Available for iOS 16 and later.

Allow Rapid Security Response removal (supervisor mode)

- The policy determines whether the user can remove Rapid Security Response. Available for iOS 16 and later.

Media

Ratings region

- Policy determines which region will be used for content ratings.

Allowed content ratings

Movies

- Policy determines the maximum allowed rating for movies that users can download from the iTunes Store. Use this rule to block access to new and existing movies that exceed a maximum rating. If set to "Do not allow movies," all movies purchased from iTunes Store are hidden and users can not preview, purchase, or download movies.

TV Shows

- Policy determines the maximum allowed rating for TV shows that users can download from the iTunes Store. Use this rule to block access to new and existing TV shows that exceed a maximum rating. If set to "Do not allow TV shows," all TV shows purchased from the iTunes Store are hidden and users cannot preview, purchase, or download TV shows.

Apps

- Policy determines the maximum allowed rating for apps that users can download from the App Store. Use this rule to block access to new and existing apps that exceed a maximum rating. This rule does not apply to built-in iOS apps. If set to "Do not allow apps," all apps purchased from the App Store are hidden and users cannot install or update apps.

Allow playback of explicit music, podcasts, and iTunes U media

- Policy determines that explicit music or video content purchased from the iTunes Store or listed in iTunes U is available on an iOS device. Explicit content is flagged by content providers, such as record labels, when sold through the iTunes Store or distributed through iTunes U. If this rule is not selected, explicit music or video content on the device is hidden and users cannot preview, purchase, or download explicit music or video content.

Allow explicit sexual content in iBooks Store

- Policy determines that explicit sexual content purchased from the iBooks Store is available on an iOS device. Explicit content is flagged by content providers when sold through the iBooks Store. If this rule is not selected, explicit books on the device are hidden and users cannot preview, purchase, or download books with explicit sexual content.

Web content filter

Content filtering

- Policy defines whether you can use web content filter to limit the websites that a user can view in Safari or other browser apps on an iOS device.

Turn on automatic filtering (supervisor mode)

- This option enables automatic filtering to identify and block inappropriate content. You can also include specific websites using the following settings "Permitted URLs" and "Blacklisted URLs"

Permitted URLs (supervisor mode)

- Policy defines whether you can add one or more URLs to allow access to specific websites. Users can view websites in this list regardless of whether automatic filtering blocks access.

Blacklisted URLs (supervisor mode)

- Policy defines whether you can add one or more URLs to deny access to specific websites. Users cannot view websites in this list regardless of whether automatic filtering allows access.

Specified Internet addresses (supervisor mode)

- Policy defines whether user has access only to the websites that you specify. Additionally, a bookmark is created in Safari for each allowed website.

macOS

Updated: Jan 13, 2025

Password

Password required

- Policy defines requirements for device password. Once done, user must set the device password.

Password length

- The policy defines the minimum length of the password used on the device.

Number of attempts to unlock

- Policy defines the number of failed attempts to enter the password the user may make prior to blocking the device.

Number of passwords saved

- Policy defines how many prior passwords the device should remember while changing the password.

Password expiration (in days)

- Policy defines how long the password may be used and sets the time for the user to change the password on the device. For value 0, the password does not expire.

Device block grace period

- Policy defines the maximum time for user to unblock the device again without entering the password.

Allow unlock device using fingerprint

- Policy determines whether the user can use a fingerprint to unlock the device. If the policy is disabled, the user must enter a password to unlock the device.

Allow device password changes (supervisor mode)

- Policy determines whether a user can add, change, or remove device passwords.

Max inactive time (in minutes)

- Policy defines user inactive time duration, then blanks the screen and blocks the device with the current password.

Allow to auto unlock device

- Policy determines whether the automatic device unlock function is available.

Apps

Allow using App Store

- Policy defines the use of App Store.

Allow use of Game Center (supervisor mode)

- Policy determines whether the Game Center is available on the device. If the policy is disabled, the Game Center icon is removed from the home screen and the user cannot use the Game Center.

Allow multiplayer gaming (supervisor mode)

- Policy determines whether the user can use multiplayer in games. If the 'Allow add friends to Game Center' policy is disabled, the user can only play multiplayer games with existing friends. If the policy is disabled, the user cannot use multiplayer in games and cannot add new friends to the Games Center.

Adding Friends from Game Center (supervisor mode)

- If unselected, prohibits adding friends to Game Center.

Allow iTunes Filesharing

- If unselected, disables iTunes file sharing services.

Allow autocomplete of fields

- Policy defines if browser may use autocomplete.

Default domains

Email domains

- Policy defines email domains that will be considered as default email domains. Email addresses from other domains will be highlighted as external email in Mail app.

Education

Allow remote screen observation (supervisor mode)

- If unselected, disables remote screen observation by the Classroom app. If allow screenshot is unselected, the Classroom app doesn't observe remote screens.

Require automatically join to ides (supervisor mode)

- If selected, automatically gives permission to the teacher's requests without prompting the student.

Require request permission to leave ides (supervisor mode)

- If selected, a student enrolled in an unmanaged course through Classroom requests permission from the teacher when attempting to leave the course.

Allow app and device lock (supervisor mode)

- If selected, allows the teacher to lock apps or the device without prompting the student.

Allow screen observation (supervisor mode)

- If selected and Allow remote screen observation is also selected, a student enrolled in a managed course via the Classroom app automatically gives permission to that course teacher's requests to observe the student's screen without prompting the student.

Functionality

Allow camera

- The policy allows the use of the camera. If unchecked, the camera will not work in all apps.

Allow to take screenshots and record screen

- Policy determines whether the user can take screenshots and record the screen.

Allow use AirDrop (supervisor mode)

- Policy determines whether the user can use the AirDrop sharing feature. If the policy is disabled, the user cannot use AirDrop in any applications, and the AirDrop option is removed from the Control Center.

Allow use Apple Music service (supervisor mode)

- Policy determines whether the user has access to Apple Music service. If the policy is disabled, the Music application returns to the idic mode.

Synchronization of documents with iCloud (supervisor mode)

- If unselected, disables document and key-value syncing to iCloud.

Allow iCloud Desktop and Documents

- If false, disables cloud desktop and document services.

Allow keychain sync with iCloud

- If unchecked, disables iCloud keychain syncing.

Allow use iCloud Photo Library (supervisor mode)

- Policy determines whether a user can upload photos to iCloud Photo Library.

Allow iCloud Address Book

- If false, disables iCloud Address Book services.

Allow iCloud Bookmarks

- If false, disables iCloud Bookmark sync.

Allow iCloud Calendar

- If false, disables iCloud Calendar services.

Allow iCloud Mail

- If false, disables iCloud Mail services.

Allow iCloud Notes

- If false, disables iCloud Notes services.

Allow iCloud Reminders

- If false, disables iCloud Reminder services.

Allow iCloud Private Relay (supervisor mode)

- Policy determines whether the iCloud Private Relay internet privacy service is available.

Allow wallpaper changes (supervisor mode)

- Policy determines whether the user can change the wallpaper of the device screen.

Allow use Handoff

- Policy determines whether the user can use the feature to transfer user activities among multiple devices associated with the user.

Allow Internet results in Spotlight (supervisor mode)

- Policy determines whether the user can use Spotlight search returns to Internet search when searching for content on a device.

Send diagnostic data to Apple

- Policy defines if diagnostic data should be sent to Apple.

Allow dictation (supervisor mode)

- If unselected, disallows dictation input.

Allow password autofill (supervisor mode)

- If unselected, disables the AutoFill Passwords feature in macOS (with Keychain and third-party password managers) and the user isn't prompted to use a saved password in Safari or in apps.

Allow password request from nearby devices (supervisor mode)

- If unselected, disables requesting passwords from nearby devices. Feature limited to requesting Wi-Fi access password.

Allow password sharing via AirDrop (supervisor mode)

- If unselected, disables sharing passwords with the Airdrop Passwords feature.

Enable Activation Lock for devices with Apple Business Manager (supervisor mode)

- The policy enforces the use of Activation Lock for devices in supervisor mode with Apple Business Manager.

Allow Activation Lock (supervisor mode)

- The policy allows Activation Lock for devices in supervisor mode.

Force delayed app software updates (supervised mode)

- If selected, delays user visibility of non-OS Software Updates.

Delayed OS updates (supervisor mode)

- If selected, delays user visibility of OS updates.

Delay software updates (supervisor mode)

- Sets how many days to delay a software update on the device. With this restriction in place, the user doesn't see a software update until the specified number of days after the software update release date.

Windows

Updated: Jan 13, 2025

Password

Password required

- Policy defines requirements for device password. Once done, the user must set the device password.

Password length

- The policy defines the minimum length of the password used on the device.

Password expiration (in days)

- Policy defines how long the password may be used and sets the time for the user to change the password on the device.

Max inactive time (in minutes)

- Policy defines user inactive time duration, then blanks the screen and blocks the device with the current password.

Number of attempts to unlock

- Policy defines the number of incorrect password attempts. After exceeding the allowable attempts, the device will reboot.

Apps

Allow using Cortana

- Policy defines the use of Cortana voice assistant with the device.

BitLocker

Turn on device encryption

- Enable BitLocker - a solution that enables cryptographic data protection on disks, built into Microsoft operating systems.

Configure encryption methods for disk drives

- This setting allows you to configure the algorithm and cipher strength used by BitLocker Drive Encryption. This setting is applied when you turn on BitLocker. Changing the encryption method has no effect if the drive is already encrypted, or if encryption is in progress.

Prompt for device encryption

- Enable the option "Prompt for device encryption" to prompt users to encrypt the OS drive.

Allow standard user encryption

- The policy allows enforcing device encryption policies in scenarios where the settings are pushed when the current logged in user is an Azure AD administrator account other than the administrator / standard user. This policy is only supported on Azure AD accounts.

Configure recovery options for fixed drives

- This setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This setting is applied when you turn on BitLocker.
 - Fixed drives require encryption
 - If you enable this setting, all fixed data drives that are not BitLocker-protected will be mounted as read-only. If the drive is protected by BitLocker, it will be mounted with read and write access.
 - Configure encryption methods for fixed drives
 - For fixed and operating system drives, we recommend XTS-AES algorithm.
 - Save BitLocker info on fixed data drives to Azure AD DS.
 - Use data recovery agents with BitLocker - fixed data drives
 - Data recovery agents are granted rights to decrypt data encrypted by other users as their PKI certificates have been used to create a BitLocker key protector. They can thus use their credentials to unlock BitLocker-protected drives.
 - Hide recovery options from BitLocker setup wizard
 - Prevent user from specifying recovery options when he turn on BitLocker on a drive.
 - Disable BitLocker until fixed data drive recovery information is stored on Azure AD DS
 - Prevent user from enabling BitLocker unless the computer is connected to the domain and the backup of Bitlocker recovery information to Azure AD DS succeeds.
 - Select recovery information to be stored on Azure AD DS

- Generate recovery key
 - The 256-bit recovery key is system-generated and is stored on an external USB drive.
- Generate recovery password
 - The 48 digit recovery password is system generated and it has to be either printed or stored on an external USB drive.
- Removable drives require encryption
 - If you enable this setting, all removable data drives that are not BitLocker-protected will be mounted as read-only. If the drive is protected by BitLocker, it will be mounted with read and write access.
- Configure encryption methods for removable drives
 - For removable drives, you should use AES-CBC 128-bit or AES-CBC 256-bit if the drive will be used in other devices that are not running Windows 10, version 1511.
- Configure encryption methods for operating system drives
 - For operating system drives, we recommend XTS-AES algorithm.
- Minimum length for BitLocker startup PIN
 - This setting allows you to configure a minimum length for a Trusted Platform Module (TPM) startup PIN. The startup PIN must have a minimum length of 6 to 20 digits.
- Configure the pre-boot recovery message
- Custom recovery message and URL
- Configure recovery options for system drives
 - Choose how BitLocker-protected operating system drives can be recovered.
- Save BitLocker info on OS drives to Azure AD DS.
- Use data recovery agents with BitLocker - OS drives
 - Bitlocker data recovery agents are individuals whose public key infrastructure (PKI) certificates have been used to create a BitLocker key protector, so those individuals can use their credentials to unlock BitLocker-protected drives. Bitlocker Data recovery agents can be used to recover BitLocker-protected operating system drives, fixed data drives, and removable data drives.
- Hide recovery options from BitLocker setup wizard

- Prevent user from specifying recovery options when BitLocker is turned on on a drive.
- Disable BitLocker until OS drive recovery information is stored on Azure AD DS
 - Prevent user from enabling BitLocker unless the computer is connected to the domain and the backup of Bitlocker recovery information to Azure AD DS succeeds.
- Select recovery information to be stored on Azure AD DS
- Generate recovery key
 - The 256-bit recovery key is system-generated and is stored on an external USB drive.
- Generate recovery password
 - The 48 digit recovery password is system generated and it has to be either printed or stored on an external USB drive.
- Authenticate with TPM startup pin
 - Requires the entry of a 6 to 20 digit personal identification number (PIN), configured by the user during BitLocker setup.
- Enable BitLocker without a Trusted Platform Module (TPM)
 - In this mode either a password or a USB key drive is required to unlock Bitlocker-Encrypted PC
- Authentication with TPM
 - "Required" enables a TPM only mode, wherein encryption keys are stored in the TPM chip. User will have a SSO experience without requiring a PIN or startup key during boot.
- Authentication with TPM and startup key
 - When using a startup key, the key information used to encrypt the drive is stored on the USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible.
- Authentication with TPM and PIN
 - Requires the entry of a 6 to 20 digit personal identification number (PIN), configured by the user during BitLocker setup.
- Authentication with TPM, startup key and PIN
 - Required by default if the system has no TPM.

Functionality

Allow camera

- The policy allows the use of the camera. If unchecked, the camera will not work in all apps, including the Proget app.

Location services

- Policy specifies whether the device can use location services.

Cellular data

- Policy specifies whether the device can use Cellular data.

Allow VPN via Cellular data

- Policy determines whether VPN on the device can use Cellular data.

Cellular data roaming

- Policy specifies whether the device can use Cellular data while roaming.

Allow VPN via Cellular data roaming

- Policy specifies whether VPN on the device can use Cellular data while roaming.

Allow SD cards

- Policy defines the use of the SD memory card with the device.

Allow display of notifications with the screen blocked.

- Policy defines if the device may display notifications in Notification Panel with the device screen blocked.

Allow using Wi-Fi network

- Policy defines the use of the Wi-Fi network module on the device.

Allow Wi-Fi sharing

- Policy allows sharing of Wi-Fi networks.

Allow manual Wi-Fi network configuration

- Policy defines whether users can enable their own wireless Wi-Fi networks on the device.

Allows the user to change date and time settings

- Policy allows users to change date and time settings on the device.

Allow screen capture

- Policy specifies whether users can capture screenshots or screen recordings on the device.

Allow USB debugging

- Policy defines whether USB debugging is allowed on the device.

Allow external storage

- Policy allows the use of external storage devices such as USB drives or external hard drives.

Allow app installation from unknown sources

- Policy determines whether users can install apps from sources other than the official app store.

Allow app removal

- Policy specifies whether users can uninstall apps from the device.

Allow app updates

- Policy allows apps to be updated automatically or manually by users.

Security

Allow device detection by other equipment using Bluetooth

- Policy defines whether the device may be detected by other devices using Bluetooth.

Allow deletion of "Work" account

- Policy defines if the work account may be deleted on the device (disconnecting the device from the MDM system).

Allow factory reset

- Policy defines if the user may restore factory settings to the device.

Proget app password

- The password should be entered when uninstalling the Proget application from the user's device.

Profiles

Updated: Jul 16, 2026

In order to use our system with the full functionality, you must configure the basic profiles. This knowledge is necessary to configure e-mail accounts, locate the device, manage applications through the white and black list, provide the device with the necessary company documents such as: contacts or files. It is also important to protect yourself in case of data loss by backing up.



ActiveSync

Auto-configure email sync with Microsoft Exchange servers



APN

Configure internet, MMS, or WAP access via APN



Apple Business Manager

Automatically activate Apple devices via Apple Business Manager



Apple Update

Configure update schedules and delays for iOS and macOS



Application rules

Manage app installation permission rules on devices



Backup

Back up contacts, SMS/MMS, and call logs



Business Contact

Upload a shared contacts file to user devices



Business Documents

Share company documents for download on devices



Certificate

Send a certificate to the device to authenticate a host



Certificate mapping

Link a certificate or SCEP profile to a specific URL



Connectivity

Configure calls, SMS, and mobile data connectivity



Custom Apple Configuration

Apply custom configuration payloads for Apple devices



Geofencing

Trigger actions based on device location and business zones



IMAP/POP

Connect to email servers via IMAP or POP



Kiosk

Restrict the device to one or a few specific apps



Location

Monitor, refresh, and display device location on a map



Shared Device

Switch users on a shared device without admin action



MTP

Detect device threats and configure security responses



SCEP

Auto-request a user certificate without domain credentials



VPN

Connect the device to the local corporate network



Wallpaper

Personalize the home and lock screen image



Wi-Fi

Define trusted Wi-Fi networks and secure authorization

ActiveSync

Updated: Jun 3, 2026

ActiveSync profile allows you to configure automatically an email profile on device to connect to the email server like Microsoft Exchange and data synchronization, etc. email, calendar, contacts.

Compatibility:

- iOS
- Windows **Deprecated**

* Name:

Example

Domain:

Example

Gateway:

None

Port:

443

* Email server:

mail.example.com

Synchronization time frame:

1 day

Synchronization interval:

Automatic - Push

Authentication:

Password

Certificate:

Select

SCEP profile:

Select

* Email:

{User:Email}

* Username:

{User:Name}

Account name:

{User:DisplayName}

☐ Use OAuth for Authentication

OAuth Sign in URL:

OAuth Token Request URL:

☒ Use SSL

☐ Accept all SSL certificates

☐ Sync Calendar

☐ Synchronize contacts

☐ Automatic sync in roaming

☐ Allow edit account settings

S/MIME

☐ Use S/MIME

☐ Always sign emails with a S/MIME certificate

☐ Default encrypt emails with a S/MIME certificate

☐ Ask the user whether to encrypt message

1 Name

- Enter the name of the ActiveSync profile
- Maximum length of the text is 255
- Required

2 Server Config

2.1 Domain

- Enter the domain name of the Exchange server
- Maximum length of the text is 32

2.2 Gateway

- Choose the gateway profile from the list, which will secure traffic between the mobile device and internal e-mail systems

2.3 Port

- Enter the protocol port by means of which the connection is made to the service (port 443 is used by default for connection using TLS / SSL)
- Maximum value is 65535
- Required

2.4 E-mail server

- Enter the name of the server on which the account was created
- Maximum length of the text is 32
- Required

2.5 Synchronization time frame

- Specifies from which period of time the data will be synchronized
- One of:
 - 1 day
 - Week
 - 2 weeks
 - Month
 - All

2.6 Synchronization interval

- Specifies the frequency of data synchronization (Automatically or time period)
- One of:
 - Automatic - Push
 - Never
 - 5 min
 - 10 min
 - 30 min
 - 1 hour

2.7 Authentication

- Choose the password for authentication
- One of:
 - Password
 - Certificate
 - SCEP profile

2.8 Certificate

- Choose the Certificate profile which will be used for authentication

2.9 SCEP profile

- Choose the SCEP profile which will be used for authentication

3 User Config

3.1 e-mail

- Enter an e-mail address for which the profile will be configured
- Global variables available
- Maximum length of the text is 255
- Required

3.2 Username

- Username that matches the name for the Exchange account
- Global variables available
- Maximum length of the text is 32
- Required

3.3 Account name

- Global variables available
- Maximum length of the text is 32

3.4 Use OAuth for Authentication

- If checked, allows user to authorize automatically
- Available only on devices with iOS 12.0 or higher

3.5 OAuth Sign in URL

- URL to the endpoint that authenticates user credentials
- Available only on devices with iOS 12.0 or higher
- Available if "Use OAuth for Authentication" is checked
- Maximum length of the text is 512

3.6 OAuth Token Request URL

- Authorization tokens to prove an identity between consumers and service providers
- Available only on devices with iOS 12.0 or higher
- Available if "Use OAuth for Authentication" is checked
- Maximum length of the text is 512

4 Security Config

4.1 Use SSL

- If checked, using SSL when connecting is allowed. It ensure that connection is secure by SSL certificate.

4.2 Accept all SSL certificates

- If checked, all the certificates for the connection will be accepted

4.3 Sync Calendar

- If checked, calendar data will be downloaded during account synchronization

4.4 Synchronize contacts

- If checked, contacts will be downloaded during account synchronization

4.5 Automatic sync in roaming

- If checked, the Exchange account data will be automatically synchronized (with a specified interval) also using roaming data, this may result in additional costs being charged

4.6 Allow edit account settings

- If checked, changing the account settings from the application will be allowed

4.7 Use S/MIME

- If checked, mail will be encrypted with S/MIME standard

4.8 Always sign e-mails with a S/MIME certificate

- If checked, mails always will be signed with S/MIME certificate. It ensure that the message in receiver inbox is the exact message that started with the sender.
- Available if "Use S/Mime" is checked

4.9 Default encrypt e-mails with a S/MIME certificate

- If checked, mails will be encrypted with S/MIME certificate. It ensure that the message content will be only shown for persons with right key.
- Available if "Use S/Mime" is checked

4.10 Ask the user whether to encrypt message

- If checked, user has the option of choose whether the message should be encrypted
- Available if,"Use S/Mime" is checked

APN

Updated: Jun 3, 2026

APN configuration provides access to the Internet or optionally provides access to MMS or WAP.

Compatibility:

- Android Enterprise Device Owner
 - Android Enterprise Profile Owner (COPE)
 - iOS
-

* Name:

Example



Android Enterprise configuration ⓘ



Samsung configuration



iOS configuration

1 Name

- Enter the name of the APN profile
- Maximum length of the text is 255
- Required

2 Android Enterprise Configuration

3 Samsung Configuration

4 iOS Configuration

Android Enterprise configuration

Updated: Dec 3, 2024

APN configuration provides access to the Internet or optionally provides access to MMS or WAP.

* APN:

internet

Type of credentials:

PAP



* MCC:

260

* MNC:

06

* Name:

Example APN configuration

Carrier ID:

User:

Password:



* APN type: ⓘ

Default



MVNO type:

Select



Network type:

Select



Protocol:

Select



Roaming protocol:

Select



Proxy settings:

Proxy server address:

Proxy server port:

MMS:

MMSC:

MMS proxy server address:

MMS proxy server port:

1 APN

- Enter the Access Point Name
- Maximum length of the text is 255
- Required

2 Type of credentials

- One of:
 - PAP
 - CHAP
 - PAP or CHAP

3 MCC

- Enter the Mobile Country Code
- Three-digit number
- Required

4 MNC

- Enter the Mobile Network Code
- Two or three-digit number
- Required

5 Name

- Enter the name of the APN
- Maximum length of the text is 255
- Required

6 Carrier ID

- Enter the android platform-wide identifier for a carrier

7 User

- Enter the username
- Maximum length of the text is 255

8 Password

- Enter the user password
- Maximum length of the text is 255

9 APN type

- Available options:

- Default
- Emergency
- CBS
- FOTA
- DUN
- MMS
- MCX
- IA
- IMS
- SUPL
- HIPRI
- XCAP

- Required

10 MVNO type

- One of:

- SPM
- IMSI
- GID
- ICCID

11 Network Type

- Available options:

- Unknown
- GPRS
- EDGE
- CDMA
- EVDO_0

- EVDO_A
- 1xRTT
- HSDPA
- HSUPA
- HSPA
- EVDO_B
- IDEN
- LTE
- EHRDP
- HSPAP
- GSM
- TD_SCDMA
- IWLAN
- NR

12 Protocol

- One of:
 - IP
 - IPv6
 - IPv4v6
 - PPP
 - Non IP
 - Unstructured

13 Roaming protocol

- One of:
 - IP
 - IPv6
 - IPv4v6

- PPP
- Non IP
- Unstructured

14 Proxy server address

- Enter the proxy server address
- Maximum length of the text is 255

15 Proxy server port

- Enter the proxy server port
- Maximum value is 65535

16 MMSC

- Enter the Multimedia Messaging Service Center
- Maximum length of the text is 255

17 MMS proxy server address

- Enter the Multimedia Messaging Service server address
- Maximum length of the text is 255

18 MMS proxy server port

- Enter the Multimedia Messaging Service server port
- Maximum value is 65535

Samsung configuration

Updated: Dec 3, 2024

APN configuration provides access to the Internet or optionally provides access to MMS or WAP.

* APN:

internet

* Name:

Example APN configuration

Type of credentials:

PAP



* MCC:

260

* MNC:

06

User:

Password:



Server address:



Set as preferred ⓘ

Proxy settings:

Proxy server address:

Proxy server port:

MMS:

MMSC:

MMS proxy server address: _____

MMS proxy server port: _____

1 APN

- Enter the Access Point Name
- Maximum length of the text is 255
- Required

2 Name

- Enter the name of the APN
- Maximum length of the text is 255
- Required

3 Type of credentials

- One of:
 - PAP
 - CHAP
 - PAP or CHAP

4 MCC

- Enter the Mobile Country Code
- Three-digit number
- Required

5 MNC

- Enter the Mobile Network Code
- Two or three-digit number
- Required

6 User

- Enter the username
- Maximum length of the text is 255

7 Password

- Enter the user password
- Maximum length of the text is 255

8 Server address

- Enter the server address
- Maximum length of the text is 255

9 Set as preferred

- If checked, new preferred APN set on device will overwrite previous given preferred APN

10 Proxy server address

- Enter the proxy server address
- Maximum length of the text is 255

11 Proxy server port

- Enter the proxy server port
- Maximum value is 65535

12 MMSC

- Enter the Multimedia Messaging Service Center
- Maximum length of the text is 255

13 MMS proxy server address

- Enter the Multimedia Messaging Service server address
- Maximum length of the text is 255

14 MMS proxy server port

- Enter the Multimedia Messaging Service server port
- Maximum value is 65535

15 SUPL

- If checked, APN sets up a secure connection with the location server in the operator's network

iOS configuration

Updated: Dec 3, 2024

APN configuration provides access to the Internet or optionally provides access to MMS or WAP.

Type of APN configuration:

Default APN



Default APN

* APN:

internet

Type of credentials:

PAP



User:

Password:



Data APN

APN:

Type of credentials:

PAP



User:

Password:



Proxy server address:

Proxy server port:

1 Type of APN configuration

- Choose a type of APN configuration
- One of:
 - Default APN
 - Data APN
 - Default APN and Data APN

2 Default APN - APN

- Enter the Default APN Access Point Name
- Maximum length of the text is 255
- Required if "Default APN" or "Default APN and Data APN" is chosen

3 Default APN - Type of credentials

- One of:
 - PAP
 - CHAP

4 Default APN - User

- Enter the Default APN username
- Maximum length of the text is 255

5 Default APN - Password

- Enter the Default APN user password
- Maximum length of the text is 255

6 Data APN - APN

- Enter the Data APN Access Point Name

- Maximum length of the text is 255
- Required if type of APN configuration is "Data APN" or "Default APN and Data APN"

7 Data APN - Type of credentials

- One of:
 - PAP
 - CHAP
- Available if "Default APN" or "Default APN and Data APN" is chosen

8 Data APN - User

- Enter the Data APN username
- Maximum length of the text is 255
- Available if "Default APN" or "Default APN and Data APN" is chosen

9 Data APN - Password

- Enter the Data APN user password
- Maximum length of the text is 255
- Available if "Default APN" or "Default APN and Data APN" is chosen

10 Proxy server address

- Enter the proxy server address
- Maximum length of the text is 255
- Available if "Default APN" or "Default APN and Data APN" is chosen

11 Proxy server port

- Enter the proxy server port
- Maximum value is 65535
- Available if "Default APN" or "Default APN and Data APN" is chosen

1 Name

- Name of the Apple Business Manager profile
- Maximum length of the text is 255
- Required

2 Basic informations

2.1 Department

- Name of the department which will be displayed on the managed profile settings
- Maximum length of the text is 125
- Required

2.2 Support phone number

- Support phone number
- Maximum length of the text is 32
- Required

2.3 Mark as default

- If checked, the profile will automatically be added to all devices newly provided by Apple Business Manager
- There may be only one default profile

3 MDM Profile Settings

3.1 Allow removal of MDM profile

- If checked, user will be able to manually delete the MDM profile
- Supervisor mode required

3.2 Allow pairing

- If checked, user will be able to pair Apple device with a host such as iTunes

3.3 Host certificate

- If chosen, the device will continue to pair with a host that possesses one of these certificates

Settings of the first run

4 MacOS and iOS

4.1 Skip the Choose Your Lock screen

- If checked, choose your Lock screen will be skipped
- Available on iOS 13 or higher
- Available on macOS 10.14 or higher

4.2 Skip the App Store panel

- If checked, App Store panel will be skipped
- Available on iOS 14.3 or higher
- Available on macOS 11.1 or higher

4.3 Skip location services settings

- If checked, location services settings will be skipped
- Available on iOS 7 or higher
- Available on macOS 10.11 or higher

4.4 Skip restore and backup settings

- If checked, restore and backup settings will be skipped
- Available on iOS 7 or higher
- Available on macOS 10.9 or higher

4.5 Skip Apple ID and iCloud settings

- If checked:
 - Apple ID and iCloud settings will be skipped
 - Apple Pay settings will be automatically turned off
- Available on iOS 7 or higher
- Available on macOS 10.9 or higher

4.6 Skip Terms and Conditions

- If checked, Terms and Conditions will be skipped
- Available on iOS 7 or higher
- Available on macOS 10.9 or higher

4.7 Skip Siri settings

- If checked, Siri settings will be skipped
- Available on iOS 7 or higher
- Available on macOS 10.12 or higher

4.8 Skip Diagnostics settings

- If checked, Diagnostics settings will be skipped
- Available on iOS 7 or higher
- Available on macOS 10.9 or higher

4.9 Skip Touch ID settings

- If checked:
 - Touch ID settings will be skipped
 - Apple Pay settings will be automatically turned off
- Available on iOS 8.1 or higher
- Available on macOS 10.12.4 or higher

4.10 Skip Apple Pay settings

- If checked, Apple Pay setup will be skipped
- Available on iOS 8.1 or higher
- Available on macOS 10.12.4 or higher

4.11 Skip Privacy screen

- If checked, privacy panel will be skipped
- Available on iOS 11.13 or higher
- Available on macOS 10.13.4 or higher

4.12 Skip Screen Time screen

- If checked, Screen Time panel will be skipped
- Available on iOS 12 or higher
- Available on macOS 10.15 or higher

5 Only iOS

5.1 Skip Device to Device Migration panel

- If checked, Device to Device Migration panel will be skipped
- Available on iOS 13+
- Available on iOS 13 or higher

5.2 Skip iMessage panel

- If checked, iMessage panel will be skipped
- Available on iOS 10 or higher

5.3 Skip Restore Completed panel

- If checked, Restore Completed panel will be skipped
- Available on iOS 14 or higher

5.4 Skip Software Update Complete panel

- If checked, Software Update Complete panel will be skipped
- Available on iOS 14 or higher

5.5 Skip Get Started panel

- If checked, Get Started panel will be skipped
- Available on iOS 13 or higher

5.6 Skip the Move from Android settings

- If checked, Move from Android settings will be skipped
- Available on iOS 9 or higher

5.7 Skip Passcode creation

- If checked:

- Passcode creation will be skipped
- Apple Pay settings and Touch ID settings will be automatically turned off
- Available on iOS 7 or higher

5.8 Skip Zoom settings

- If checked, Zoom settings will be skipped
- Available on iOS 8.3 or higher

5.9 Skip Apple Watch Migration screen

- If checked, Apple Watch Migration screen will be skipped
- Available on iOS 11 or higher

5.10 Skip iMessage and FaceTime screen

- If checked, iMessage and FaceTime screen will be skipped
- Available on iOS 12 or higher

5.11 Skip Mandatory Software Update screen

- If checked, Mandatory Software Update screen will be skipped
- Available on iOS 12 or higher

5.12 Skip Add cellular Plan screen

- If checked, Skip Add cellular Plan screen will be skipped
- Available on iOS 12 or higher

6 Only MacOS

6.1 Skip accessibility panel

- If checked, accessibility panel will be skipped
- Available on macOS 11 or higher

6.2 Skip iCloud Analytics screen

- If checked, iCloud Analytics screen will be skipped
- Available on macOS 10.12.4 or higher

6.3 Skip Unlock Your Mac with your Apple Watch panel

- If checked, Unlock Your Mac with your Apple Watch panel will be skipped
- Available on macOS 12 or higher

6.4 Skip the FileVault screen for OS X devices

- If checked, FileVault screen for OS X devices will be skipped
- Available on macOS 10.10 or higher

6.5 Skip iCloud Storage settings

- If checked, iCloud Storage settings will be skipped
- Available on macOS 10.13.4 or higher

Apple Update

Updated: Jun 3, 2026

The Apple Update profile allows you to configure update settings for iOS and macOS. It enables you to define, among other things, the installation schedule, update delays, and rules for downloading them. For the profile to function properly, declarative management must be enabled on the device.

Compatibility:

- iOS (from iOS 17)
 - macOS (from macOS 14)
-

Add new Apple Update profile

* Name:

Example Apple Update profile

* Type:

Force latest version



URL address:

https://support.apple.com/guide/iphone/update-ios-iph3e504502/ios

* Days from release:

10

* Force install time:

23:00



Force installation date:

Version: ⓘ

Build version:

Back

Submit

1 Name

- Name of the Apple Business Manager profile
- Maximum length of the text is 255
- Required

2 Type

- Select the device update type, such as:
 - Force latest version
 - The device will be updated to the latest available software version, regardless of the currently installed one
 - Specific version
 - Allows specifying the exact software version to which the device should be updated

3 URL address

- Provide a URL to a web page with additional information for users about the forced software update

4 Days from release

- Specify the number of days after the update is released that the installation will be automatically enforced on the device
- Available if selected **Force latest version**
- Required

5 Force install time

- Set the local time at which the software update installation will be enforced
- Available if selected **Force latest version**
- Required

6 Force installation date

- Set the local date when the software update installation should be enforced (RFC3339 format, without time zone offset)
- Available if selected **Specific version**
- Required

7 Version

- Select the target operating system version to which the device should be updated
- Available if selected **Specific version**
- Required

8

Build version

- Enter the target system build version that should be installed on the device
- Available if selected **Specific version**

Application rules

Updated: Jun 3, 2026

Profile Application rules can add rules that will manage permissions on the installation of the application on user devices. Blocking system applications may result in wrong operation or damage to the device.

Compatibility:

- Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - iOS (Supervised mode)
-

* Name:

Example

① Adding apps to the profile will not force their installation on the device. The view below is for illustrative purposes only. Only the package name is taken into account and the icon and name of the application may differ on the device.

Android Enterprise - work space

Android Enterprise - private space

iOS (supervisor mode)

1 Name

- Enter the name of the Application Rules profile
- Maximum length of the text is 255
- Required

2 Android Enterprise - work space

3 Android Enterprise - private space

4 iOS (Supervised mode)

Android Enterprise - work space

Updated: Dec 3, 2024

Profile Application rules can add rules that will manage permissions on the installation of the application on user devices. Blocking system applications may result in wrong operation or damage to the device.

The screenshot displays two side-by-side panels in the Android Enterprise console. The left panel is titled 'UNLOCK APPS' and the right panel is titled 'BLACKLIST'. Both panels feature a search bar labeled 'Package id: Start typing...', a 'Reset filters' link, and a table with columns 'ICON', 'APP NAME', and 'PACKAGE ID'. The tables are currently empty, showing 'No data available'. Below the tables are pagination controls and buttons for 'Clear list', 'Add application manually', and 'Add applications from system'.

1 Unlock apps

1.1 Clear list

- Removes all applications added to list

1.2 Add application manually

- Add application to the application rules profile by providing its package ID

1.3 Add applications from system

- Add applications from list of available applications in the system

2 Blacklist

2.1 Block all apps

- If checked, blocks all applications on device except Proget app, Settings and Google Play

2.2 Clear list

- Removes all applications added to list

2.3 Add application manually

- Add application to the application rules profile by providing its package ID

2.4 Add applications from system

- Add applications from list of available applications in the system

Android Enterprise - private space

Updated: Dec 3, 2024

Profile Application rules can add rules that will manage permissions on the installation of the application on user devices. Blocking system applications may result in wrong operation or damage to the device.

Available for COPE activation

WHITELIST

Package Id: Start typing...

Reset filters

Selected: 0

Deselect all

ICON

APP NAME

PACKAGE ID

No data available

Results: 0

Clear list

Add application manually

Add applications from system

BLACKLIST

Package Id: Start typing...

Reset filters

Selected: 0

Deselect all

ICON

APP NAME

PACKAGE ID

No data available

Results: 0

Clear list

Add application manually

Add applications from system

1 Whitelist

1.1 Clear list

- Removes all applications added to list

1.2 Add application manually

- Add application to the application rules profile by providing its package ID

1.3 Add applications from system

- Add applications from list of available applications in the system

2 Blacklist

2.1 Clear list

- Removes all applications added to list

2.2 Add application manually

- Add application to the application rules profile by providing its package ID

2.3 Add applications from system

- Add applications from list of available applications in the system

iOS (Supervised mode)

Updated: Dec 3, 2024

Profile Application rules can add rules that will manage permissions on the installation of the application on user devices. Blocking system applications may result in wrong operation or damage to the device.

WHITELIST

Package id: Start typing...

Reset filters

Selected: 0

Deselect all

ICON

APP NAME

PACKAGE ID

No data available

Results: 0

<<

<

1

>

>>

Clear list

Add application manually

Add applications from system

Add default applications

BLACKLIST

Package id: Start typing...

Reset filters

Selected: 0

Deselect all

ICON

APP NAME

PACKAGE ID

No data available

Results: 0

<<

<

1

>

>>

Clear list

Add application manually

Add applications from system

1

Whitelist

1.1 Clear list

- Removes all applications added to list

1.2 Add application manually

- Add application to the application rules profile by providing its package ID

1.3 Add applications from system

- Add applications from list of available applications in the system

1.4 Add default applications

- Add default applications to the application rules profile

2 Blacklist

2.1 Clear list

- Removes all applications added to list

2.2 Add application manually

- Add application to the application rules profile by providing its package ID

2.3 Add applications from system

- Add applications from list of available applications in the system

Backup

Updated: Jun 3, 2026

Backup profile allows you to create backup of contacts, SMS, MMS and call log. When configuring a profile, you can specify items, storage space, and backup frequency.

Compatibility:

- Android
- Android Enterprise Profile Owner
- Android Enterprise Device Owner

* Name:

Example

BACKUP ITEMS

☒ Make a backup of contacts

☒ Make a copy of SMS / MMS ⓘ

☒ Make a backup of call log

☒ Allow the use of mobile data

FREQUENCY

Frequency of sending (in days, 1-30):

1

* What time?:

12:00

DELETING COPIES

☒ Delete backup

Older than (in days, 1-365):

30

1 Name

- Enter the name of the Backup profile
- Maximum length of the text is 255
- Required

2 Backup Items

2.1 Make backup of contacts

- If checked, allows to make a backup of contacts from the device

2.2 Make copy of SMS / MMS

- If checked, allows to make a copy of SMS / MMS from the device

2.3 Make backup of call log

- If checked, allows to make a backup of call log from the device

2.4 Allow the use of mobile data

- If checked, allows to use mobile data for making Backup

3 Frequency

3.1 Frequency of sending (in days, 1-30)

- Allows to set the backup frequency every specified number of days

3.2 What time?

- Enter the hour at which backup will be sent
- Required

4 Deleting Copies

4.1 Delete backup

- If checked, delete old backups after specific time

4.2 Older than (in days, 1-365)

- Choose the time in days after which previous backups will be deleted

Business contacts

Updated: Jun 3, 2026

Business contacts profile allows you to upload contacts file to the user profiled device.

Compatibility:

- Android
- Android Enterprise Profile Owner
- Android Enterprise Device Owner

* Name:

Example

☐ From a file

☐ Managed from a file

1 Name

- Enter the name of the new Business contacts profile
- Max length of the text is 255
- Required

2 From a file

2.1 VCF file

- Uploaded file name

2.2 Select file

- Allowed file type: VCF
- Max file size is 10MB
- Required

3 Managed from a file

3.1 Select file

- Allowed file type: VCF, CSV
- Maximum file size is 10MB

3.2 Filter

- Enter a character to find contact

3.3 Remove

- Removes selected contact from list

3.4 Add contact

- Add new contact

4

Add contact

4.1 First name

- Enter the first name of new contact
- Maximum length of the text is 64
- Required if 'Surname' is empty

4.2 Surname

- Enter the surname of new contact
- Maximum length of the text is 64
- Required if 'Name' is empty

4.3 Company

- Enter company name of new contact
- Maximum length of the text is 64

4.4 Department

- Enter department name of new contact
- Maximum length of the text is 64

4.5 Position

- Enter the position of new contact
- Maximum length of the text is 64

4.6 Phone number 1

- Enter the first phone number of new contact
- Maximum length of the text is 32
- Required

4.7 Phone number 2

- Enter the second number of new contact
- Maximum length of the text is 32

4.8 Email

- Enter the E-mail of new contact
- Maximum length of the text is 255

5 Edit

5.1 Filter

- Enter a character to find contact

5.2 Remove

- Removes selected contacts
- Removed contact will be moved to the modified contact list with status 'Removed'

5.3 Add contact

- Add new contact

5.4 Edit

- Edit selected contacts
- Edited contact will be moved to the modified contact list with status 'Edited'

5.5 Remove

- Remove chosen contacts
- Removed contact will be moved to the modified contact list with status 'Removed'

6 On contact removed

6.1 Remove

- Remove selected contacts from the modified contacts list

6.2 Edit

- Edit chosen contact from the modified contacts list

6.3 Remove

- Remove chosen contact from the modified contacts list

Business documents

Updated: Jun 3, 2026

Business documents profile allows upload documents to server. This can be downloaded on user device with his profile.

Compatibility:

- Android
- Android Enterprise Profile Owner
- Android Enterprise Device Owner

Name: ⓘ

Example

☒ Allow downloading files via Wi-Fi wireless network

☒ Allow downloading files via data transmission

☐ Notify changes

☐ Add files to the Downloads folder ⓘ

☐ Download files automatically

BUSINESS DOCUMENTS

Example directory

Selected: 0 | Deselect all

Create directory

Upload files

	NAME	SIZE	CREATION DATE
☐	Example directory	Elements: 0	-
☐	example.vcf	708 B	2024-09-05 02:08:24

1

Name

- Enter the name of the Business documents profile
- Maximum length of the text is 255
- Required

2

Configuration

2.1 Allow downloading files via Wi-Fi wireless network

- If checked, downloading files via Wi-Fi is allowed

2.2 Allow downloading files via data transmission

- If checked, downloading files via data transmission is allowed

2.3 Notify changes

- If checked, user will be informed about changes in Business documents profile

2.4 Add files to the Downloads folder

- If checked, files will be add to Download folder on device

2.5 Download files automatically

- If checked, files will be automatically downloaded on your device

3 Directory

3.1 Directory

- Click to view the directory

3.2 Download

- Download selected file

3.3 Rename

- Rename selected file or directory

3.4 Remove

- Remove selected file or directory

3.5 Create directory

- Create new directory

3.6 Upload files

- Upload file from your computer

Certificate

Updated: Jun 8, 2026

Certificate profile allows you to send any certificate to the mobile device to authenticate the host.

Compatibility:

- Android
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - iOS
 - macOS
 - Windows
-

* Name:

☐ File

☐ Template

☐ SCEP

1 Name

- Enter the name of the Certificate profile
- Maximum length of the text is 255
- Required

2 File

- If chosen, profile Certificate is creating via uploading certificate file

3 Template

- If chosen, profile Certificate is creating via template

4 SCEP

NEW

- If chosen, profile Certificate is creating via SCEP server configuration

File

Updated: Jun 8, 2026

The File option allows you to upload a ready-made certificate file from your system to the profile. Use this option when you already have a generated certificate (e.g. issued by an external Certificate Authority) that you want to distribute to devices. Supported file formats: .crt, .cer, .der, .pfx, .p12. If the certificate is password-protected, the password must be provided during upload.

File

Certificate: ⓘ

example.cer - 1.04 KiB (1.06 KB)

Select file

Password:

☒ Certificate for Windows activation ⓘ

* Certificate type:

CA X

1 Certificate

- Chosen file name
- Required

2 Select file

- Select file from the system which will be used in profile
- Allowed file type: .crt, .cer, .der, .pfx, .p12

3 Password

- Enter the certificate password
- Required if certificate is protected by password

4 Certificate for Windows activation

NEW

- When enabled, the certificate uploaded to the profile will be installed on device configured with the Windows activation type.
- Applicable only for Windows devices
- The allowed file extensions for a certificate in the Windows system are: .pem, .crt, .cer, .der

5 Certificate type

NEW

- Select the type of certificate that determines how it will be used on the device
- Available options: CA, Intermediate
- This field is only available when 'Certificate for Windows activation' is enabled

Template

Updated: Jun 9, 2026

The Template is a configuration that automatically generates certificates when a device needs them. It requires a CA certificate created in Certificate Manager. You can also add custom attributes that are embedded in the CSR and configure automatic renewal before certificate expiry.

Template

* CA:

CA

* Key length:

2048

* Encryption signature:

SHA-256

* Scope:

User

* Validity (in days):

365

* Common Name:

{User:Email}

☒ Auto renew

Specify the time before the occurrence of the event in which the certificate should be renewed (in days, 1-14):

3

TYPE	* VALUE	ACTIONS
NT_principal_Name	Value	

Clear

Add

1 CA certificate

- Choose CA certificate that is created in Certificate Manager. It's used to verify certificate identity.
- Required

2 Key length

- Choose length of the key. Defines how strong security will be.
- Required

3 Encryption signature

- Choose a type of hashing algorithm. Defines how strong security will be.
- Required

4 Scope

- Select the scope of the certificate, such as:

- User
- Device
- Required

5 Validity (in days)

- Specify how long certificate will be valid
- Minimum value is 30
- Maximum value is 730
- Required

6 Common Name

- Enter the certificate CN. It's characteristic value of certificate.
- Global variables available
- Required

7 Auto renew

- If checked, certificate will be renewed x days before expiry of his validity

8 Time before certificate should be renewed

- Specify how many days before expiry of certificate validity should it renew

9 Type

- Choose the type of custom attributes, which are pieces of data that are embedded only in the CSR.

10 Value

- Enter the value of type
- Global variables available

11 Remove

- Remove chosen custom attribute

12 Clear

- Remove all custom attributes

13 Add

- Add custom attribute

SCEP

Updated: Jun 9, 2026

NEW

Certificate with SCEP type automatically configure request the user certificate to authenticate the client without specifying domain credentials.

SCEP

* Access address:

Example access address

CA ID:

* Subject:

{User:Email}

* Fingerprint:

Example fingerprint

* Scope:

User

☒ Auto renew

Specify the time before the occurrence of the event in which the certificate should be renewed (in days, 1-14):

3

* Encryption Algorithm:

AES-256

* Encryption signature:

SHA-256

* Key length:

2048

* Password:

.....

☐ Key encipherment

☐ Digital signature

☐ Microsoft User Security

TYPE	* VALUE	ACTIONS
NT_principal_Name	Example value	

Clear

Add

1 SCEP configuration

1.1 Access address

- Enter the name of the URL for the SCEP server (eg. Network Device Enrollment Service)
- Only 80 (HTTP) port is supported by default
- Exemplary URL: `http:///certsrv/mscep/mscep.dll`
- Maximum length of the text is 255
- Required

1.2 CA ID

- Enter the name of the profile for SCEP servers (eg. Network Device Enrollment Service) that support named-profiles.
- Maximum length of the text is 255

1.3 Subject

- Global variables available
- Required

1.4 Fingerprint

- Enter the fingerprint of the CA issuing the root certificate on SCEP server (eg. Network Device Enrollment Service)
- Maximum length of the text is 500
- Required

1.5 Scope

- User
- Device

1.6 Auto renew

- If selected, the certificate will be automatically renewed before expiration

1.7 Renew before

- Specify the time before the occurrence of the event in which the certificate should be renewed (in days, 1-14)
- Default value: 3
- Available when 'Auto renew' is selected

1.8 Encryption Algorithm

- Type of encryption algorithm. Defines how strong security will be.
- One of:
 - AES128
 - AES192
 - AES256
- Required

1.9 Encryption signature

- Type of encryption signature. Defines how strong security will be.
- One of:
 - SHA256
 - SHA384
 - SHA512
- Required

1.10 Key length

- Length of the key. Defines how strong security will be
- One of:
 - 2048

- 3072
- 4096
- Required

1.11 Password

- Enter the enrollment challenge password generated during a SCEP server deployment
- The value should be a 32-digit string of alphanumeric characters
- Maximum length of the text is 255
- Required

1.12 Key encipherment

- If checked, use as key encipherment
- Use when the sender and receiver of the public key need to derive the key without using encryption

1.13 Digital signature

- If checked, use as digital signature
- Specific type of signature that is backed by a digital certificate. It's providing proof of your identity

1.14 Microsoft User Security

- If checked, use the Microsoft User Security certificate template

2 Alternative names

2.1 Type

- One of:
 - Distinguished_Name
 - NT_principal_Name
 - RFC822_Name
 - DNS_Name
- Required

2.2 Value

- Global variables available
- Required

2.3 Remove

- Removes added alternative name

2.4 Clear

- Removes all alternative names added to list

2.5 Add

- Adds alternative name to list

Certificate mapping

Updated: Jun 3, 2026

Certificate mapping allows linking a Certificate or SCEP profile with a specific URL. By adding the profile to a device, the supplied certificate will be automatically selected when attempting to connect to the defined URL, whether by a browser or other applications.

Compatibility:

- Android Enterprise Profile Owner
 - Android Enterprise Device Owner
-

Add new certificate mapping profile

ⓘ Assigning a certificate to a URL takes priority over assigning a certificate to an application.

* Name:

Example

Assign Certificate to URL

Example.URL

Certificate



Add

Assign Certificate to App

Example.App

Certificate



Add

Back

Submit

1 Name

- Enter the name of the Certificate mapping profile
- Max length of the text is 255
- Required

2 URL

- Enter the defined URL
- Max length of the text is 255
- Required

3 Certificate

- Choose authorization certificate for the selected URL page
- Required

4 Remove

- Removes URL and Certificate

5 Add URL

- Add new URL

6 Application

- Enter the specified application ID
- Maximum text length is 255
- Required

7 Certificate

- Select an authorization certificate for the selected application
- Required

8 Remove

- Removes the application ID and certificate

9 Add application

- Add new application ID

Connectivity

Updated: Jun 3, 2026

Connectivity profile allows you to enter the configuration related to outgoing and incoming communication from the device (calls, SMS) and the use of mobile data.

Compatibility:

- Android (Samsung)
- Android Enterprise Device Owner (Samsung)

Name:

Example

CONFIGURATION

MOBILE INTERNET

Allow trusted conditions only

CONNECTIONS

Incoming:

Allow trusted conditions only

Outgoing:

Allow trusted conditions only

SMS

Incoming:

Allow trusted conditions only

Outgoing:

Allow trusted conditions only

MMS

Incoming:

Allow trusted conditions only

Outgoing:

Allow trusted conditions only

TRUSTED CONDITIONS

COUNTRIES

Trust all

Trust only

Select

CONTACTS

Trust all

Trust only

Select

CONNECTIVITY RULES

Trust all operators

Trust only

MCC	MNC	ACTIONS
Add	Import from file	

1

Name

- Enter the name of the Connectivity profile
- Maximum length of the text is 255
- Required

2

Configurations

2.1 Mobile Internet

- Specify the principle of using Mobile Internet such as:
 - Block all
 - Allow all
 - Allow trusted conditions only

2.2 Connections Incoming

- Specify the principle of using incoming Connections such as:
 - Block all
 - Allow all
 - Allow trusted conditions only

2.3 Connections Outgoing

- Specify the principle of using outgoing Connections such as:
 - Block all
 - Allow all
 - Allow trusted conditions only

2.4 SMS Incoming

- Specify the principle of using incoming SMS such as:
 - Block all
 - Allow all
 - Allow trusted conditions only

2.5 SMS Outgoing

- Specify the principle of using outgoing SMS such as:
 - Block all

- Allow all
- Allow trusted conditions only

2.6 MMS Incoming

- Specify the principle of using incoming MMS such as:
 - Block all
 - Allow all
 - Allow trusted conditions only

2.7 MMS Incoming

- Specify the principle of using outgoing MMS such as:
 - Block all
 - Allow all
 - Allow trusted conditions only

3 Trusted Conditions

3.1 Countries

- Select a countries where trusted conditions will apply, if selected Trust only

3.2 Contacts

- Select a contacts where trusted conditions will apply, if selected Trust only

3.3 Add Connectivity roles

- Add manually connectivity rules with MCC and MNC codes where trusted conditions will apply, if selected Trust only

3.4 Import for file Connectivity rules

- Import from file connectivity rules with MCC and MNC codes where trusted conditions will apply, if selected Trust only

3.5 Sample CSV file

- Download the sample CSV file with MCC and MNC codes on your device

Custom Apple Configuration

Updated: Jun 3, 2026

A Custom Apple Configuration contains a payload with settings, accounts, credentials, etc., for Apple devices. Custom Apple Configuration allows you to apply custom-specific configuration for Apple devices not yet present in the current version of the Proget server. To create a Custom Apple Configuration, refer to Apple or Proget documentation.

Compatibility:

- iOS
 - macOS
-

* Name:

Example

* Channel:

User

* Configuration: ⓘ

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4   <dict>
5     <key>PayloadVersion</key>
6     <integer>1</integer>
7     <key>PayloadUUID</key>
8     <string>Ignored</string>
9     <key>PayloadType</key>
10    <string>Configuration</string>
11    <key>PayloadIdentifier</key>
12    <string>Ignored</string>
13    <key>PayloadContent</key>
14    <array>
15      <dict>
16        <key>PayloadContent</key>
17        <dict>
18          <key>URL</key>
19          <string>https://scep.example.com/scep</string>
20          <key>Name</key>
21          <string>EnrollmentCAInstance</string>
22          <key>Subject</key>
```

1 Name

- Enter the configuration name
- Maximum length of the text is 125
- Required

2 Channel

- Select a channel for configuration:
 - Device
 - User
- Required

3 Configuration

- Enter the XML configuration or drag and drop the file from your device
- Required

Geofencing

Updated: Jun 3, 2026

Geofencing allows you to customize configuration and restrictions for devices based on its location. The profile allows you to configure specific actions in and outside business zones.

Compatibility:

- Android Enterprise Profile Owner
- Android Enterprise Device Owner

1. Geofencing map

Name:

Example

GEOFENCING ZONES

Selected: 0

At least one zone is required

Add new zone



EVENTS OUTSIDE THE ZONE

EVENTS OUTSIDE THE ZONE

Assign profiles

Lock Device

Wipe company data

Wipe device

Send event notification

- Enter the name of the new Geofencing profile
 - Maximum length of the text is 255
 - Required
-

2. Geofencing zones

1 Edit

- Edit selected zone

2 Remove

- Remove selected zone

3 Created zones

- List of created zones

4 New zone configuration

4.1 Name

- Enter the zone name
- Required

4.2 Latitude

- Enter the zone latitude
- Required

4.3 Longitude

- Enter the zone longitude
- Required

4.4 Range

- Enter the zone range
- Required

4.5 Find place

- Find a place on the map

3. Events

1 Assign policies

1.1 Choose policies

- Choose policies which will be assigned during event

2 Assign profiles

2.1 Choose profiles

- Choose policies which will be assigned during event

3 Lock device

3.1 Tolerance

- Choose the time after which device will lock

3.2 Message

- Enter the message which will be displayed on the locked screen

3.3 Phone number

- Enter the phone number which will be displayed on the locked screen

4 Wipe company data

4.1 Tolerance

- Choose the time after which device will erase company data

5 Wipe device

5.1 Tolerance

- Choose the time after which all device data will be erased

6 Send event notification

6.1 Text field

- Enter the text which will be displayed in notifications on devices outside the zone

IMAP/POP

Updated: Jun 3, 2026

IMAP / POP profile specifies how to connect to e-mail servers via POP or IMAP to synchronize the data, ie. e-mail.

Compatibility:

- iOS
- macOS

* Name:	Example		
* Email:	{User:Email}		
* Account name:	{User:DisplayName}		
* Message sender:	{User:Name}		
Account type:	IMAP		
☐ Set as default			
☐ Enable notifications			

INBOUND SERVER DATA

* Server address:

* User name:

Password:

Type of security:
None

* Port:

OUTGOING SERVER DATA

* Server address:

* User name:

Password:

Type of security:
None

* Port:

1 Name

- Name of the new IMAP/POP profile
- Maximum length of the text is 255
- Required

2 E-mail data

2.1 Email

- Enter the e-mail address for which the profile will be configured
- Global variables available
- Maximum length of the text is 255
- Required

2.2 Account name

- Enter the account name which will be visible in the e-mail client application on the mobile device
- Global variables available
- Maximum length of the text is 128
- Required

2.3 Message sender

- Global variables available
- Maximum length of the text is 128
- Required

2.4 Account type

- One of:
 - POP
 - IMAP

2.5 Set as default

- If checked account will be set as default mail account on the device

2.6 Enable notifications

- If checked notifications regarding mail will be shown on the device

3 Inbound server data

3.1 Server address

- Enter the server address of the e-mail which will be used to send mails
- Maximum length of the text is 255
- Required

3.2 User name

- Enter the user name of the e-mail which will be used to send mails
- Maximum length of the text is 128
- Required

3.3 Password

- Enter the password for the e-mail that will be used to send mails
- Required

3.4 Type of security

- One of:
 - Empty
 - SSL/TLS
 - SSL/TLS (Accept all certificates)
 - STARTTLS
 - STARTTLS (Accept all certificates)

3.5 Port

- Enter the number of the port
- Required

4

Outgoing server data

4.1 Server address

- Enter the server address of the e-mail which will be used to send mails
- Maximum length of the text is 255
- Required

4.2 User name

- Enter the user name of the e-mail which will be used to send mails
- Maximum length of the text is 128
- Required

4.3 Password

- Enter the password for the e-mail that will be used to send mails
- Required

4.4 Type of security

- One of:
 - Empty
 - SSL/TLS
 - SSL/TLS (Accept all certificates)
 - STARTTLS
 - STARTTLS (Accept all certificates)

4.5 Port

- Enter the number of the port
- Required

Kiosk

Updated: Jun 3, 2026

Kiosk profile allows you to limit the functionality of the device to specific applications. You can use the Kiosk profile to configure the device to use only one or a few specific applications.

Compatibility:

- Android Enterprise Device Owner
- iOS (Supervised mode)

Add new Kiosk profile

* Name:

Compatibility Android

Compatibility iOS

1 Name

- Enter the name of the Kiosk profile
- Maximum length of the text is 255
- Required

2 Compatibility Android

3 Compatibility iOS

Android

Updated: Jun 3, 2026

Kiosk profile allows you to limit the functionality of the device to specific applications. You can use the Kiosk profile to configure the device to use only one or a few specific applications.

Compatibility Android

Compatibility iOS

☒ Disable volume adjustment ⓘ

☒ Disable navigation buttons ⓘ

☒ Do not turn off the screen while charging ⓘ

☒ Disable notifications ⓘ

☒ Disable status bar ⓘ

ⓘ Available only on devices where a password requirement policy is not set.

☒ Display Kiosk above the lock screen

Force a kiosk:

Do not force ▼

* PIN: ⓘ

1234

☒ Allow access to settings on the Kiosk exit screen

Manage settings

Kiosk Mode

☒ Single app

☐ Multi app

1

Configuration

1.1 Disable volume adjustment

- If checked, the volume adjustment will be disabled while Kiosk is turned on

1.2 Disable navigation buttons

- If checked, blocks the use of the “Recent Apps”, “Home”, and “Back” buttons while Kiosk is turned on
- Available only on Android Enterprise Device Owner

1.3 Do not turn off the screen while charging

- If checked, the screen will not turn off while charging when Kiosk is turned on

1.4 Disable notifications

- If checked, disallows to use the Home button while Kiosk is turned on
- Available only on devices with Android 9.0 or higher
- Available only on Android Enterprise Device Owner

1.5 Disable status bar

- If checked, disable access to device status bar, after unchecking the device will display information such as battery status, connection to Wi-Fi network, clock
- Available only on devices with Android 9.0 or higher
- Available only on Android Enterprise Device Owner

1.6 Display Kiosk above the lock screen

NEW

- If checked, the Kiosk will be displayed above the lock screen
- By default, the Kiosk is displayed below the lock screen
- Only works when the password policy does not require a password

- Available only on Android Enterprise Device Owner

1.7 Force a kiosk

- Specifies whether or after what time the Kiosk profile will appear on the device (e.g. if the user has exited it)
- One of:
 - Do not force
 - 5
 - 10
 - 15
 - 30
 - 60

1.8 PIN

- Enter the PIN which will be used to exit the kiosk
- Minimum length of the PIN is 4
- Maximum length of the PIN is 16
- Required

1.9 Allow access to settings on the Kiosk exit screen

NEW

- If checked, the user will have access to the Proget settings panel (e.g. Wi-Fi, volume, brightness) on the Kiosk exit screen
- The exit screen is reached by pressing the "Back" button multiple times
- Available in 'Multi app' and 'Single app' Kiosk mode
- Available only on Android Enterprise Device Owner

1.10 Manage settings

NEW

- Configure which settings categories are available on the Kiosk exit screen
 - Wi-Fi
 - Show available networks
 - Wi-Fi Calling
 - Bluetooth
 - Mobile Networks
 - Screen brightness
 - Volume
- If set, requires at least one category
- Available when "Allow access to settings on the Kiosk exit screen" is checked

2 Single app

3 Multi app

Single App

Updated: May 7, 2026

Kiosk profile allows you to limit the functionality of the device to specific applications. You can use the Kiosk profile to configure the device to use only one or a few specific applications.

① Adding apps to the profile will not force their installation on the device. The view below is for illustrative purposes only. Only the package name is taken into account and the icon and name of the application may differ on the device.

APP

Reset filtersBASICPQL

Selected: 0 | Deselect all 

☐	ICON	APP NAME	PACKAGE ID
☐		Gmail	com.google.android.gm

HIDDEN APPS: ①

Reset filtersBASICPQL

Selected: 0 | Deselect all 

☐	ICON	APP NAME	PACKAGE ID
 No data available Data has not been entered yet.			

1 Remove

- Removes an applications added to list

2 Application row

- Details of application added to kiosk

3 Clear list

- Removes all applications added to list

4 Add application manually

- Add application to the kiosk by providing its package ID

5 Add applications from system

- Add applications from list of available applications in the system

6 Hidden apps

- Add applications manually or from the system that you want to hide

Multi App

Updated: Jun 8, 2026

Kiosk profile allows you to limit the functionality of the device to specific applications. You can use the Kiosk profile to configure the device to use only one or a few specific applications.

☒ Require login

* Service user:

Example

* Service PIN:

123456

* Remembering the login:

Forbid

☐ Auto logout ⓘ

Auto logout time:

Instant

☒ Display header

Logo: ⓘ

Select file

Delete

Header Color:

#808182

Header text color:

#FFFFFF

Header text:

Custom Kiosk

(12 / 64 chars)

App text color:

#FFFFFF

Background color / wallpaper:

Color

Wallpaper

Color:

#000000

Wallpaper:

Select file

Set default

Orientation:

Auto

Adding apps to the profile will not force their installation on the device. The view below is for illustrative purposes only. Only the package name is taken into account and the icon and name of the application may differ on the device.

Apps:

Grid: 4x4

Custom Kiosk

+ + + +

+ + + +

PROGET

+ + + +

+ + + +

+

Screen 1

Hidden apps: ⓘ

Package id: Start typing...

Reset filters

BASIC PQL

Selected: 1 | Deselect all

☒	ICON	APP NAME	PACKAGE ID
☒		---	example.package.id

Clear list

Add application manually

Add applications from system

1.1 Require login

- If checked, requires log in to kiosk via service credentials
- Available only on Android Enterprise Device Owner

1.2 Service user

- Enter the kiosk service username
- Required if "Require login" is checked

1.3 Service PIN

- Enter the kiosk service password
- Required if "Require login" is checked

1.4 Remembering the login

- Chose from dropdown:
 - Force
 - Allow
 - Forbid

1.5 Auto logout

NEW

- If enabled, the user will be automatically logged out from the kiosk after the screen goes off
- If disabled, a dedicated logout action becomes available directly on the kiosk screen
- Available only on Android Enterprise Device Owner
- Available when 'Require login' is checked

1.6 Auto logout time

NEW

- Specify the time after the screen goes off, after which the user should be automatically logged out
- The default value is set to 'Instant'
- Available when 'Auto logout' is enabled

2 Header customization

2.1 Display header

- If checked, displays the header in kiosk
- Available only on Android Enterprise Device Owner

2.2 Logo

- Choose the file of the logo in kiosk
- Allowed file type: png
- Required square graphics with maximum dimensions of 192 x 192 px

2.3 Header color

- Choose the color of the screen header background

2.4 Header text color

- Choose the color of the screen header text

2.5 Header text

- Enter the text of the screen header
- Maximum length is 24

3 Launcher configuration

3.1 App text color

- Choose the color of the app text in kiosk
- Available only on Android Enterprise Device Owner

3.2 Background color / wallpaper

- Available only on Android Enterprise Device Owner

3.3 Color

- Choose the color of the screen launcher background
- Available only on Android Enterprise Device Owner

3.4 Wallpaper

- Choose the file of the wallpaper in kiosk
- Allowed file type: png

3.5 Orientation

- One of:
 - Auto
 - Portrait
 - Horizontal

4 Apps

4.1 Grid

- Choose app grid at the Kiosk
- Available sizes depends on chosen orientation

4.2 Application holder

- Add applications to the screen

4.3 Add applications manually

- Add application to the kiosk by providing its package ID

4.4 Add applications from system

- Add applications from list of available applications in the system

4.5 Add custom settings icon

- Restricted access to system settings
 - Wi-Fi
 - Show available networks
 - Wi-Fi Calling
 - Bluetooth
 - Mobile Networks
 - Screen brightness
 - Volume
- If set, requires at least one category
- Can be placed in multiple places on screen

4.6 Add action

- Name

- Set name of the action
- Required
- Choose the type of action, such as: **NEW**
 - Intent
 - This functionality allows you to trigger the specified action, using an intent
 - Intent
 - Enter the intent action to be triggered
 - Required
 - Action type
 - One of:
 - Start activity
 - Start service
 - Send broadcast
 - Default: Start activity
 - Application ID
 - Enter the package name of the application to which the intent should be directed
 - Optional
 - Additional parameters
 - Optional list of extras passed with the intent
 - Each parameter requires:
 - Key
 - Type - one of: String, Integer, Boolean, Float, Double
 - Value
 - Adding an action may allow the user to switch between application views to which they should not have access. To trigger an intent, the application that handles it must be unlocked in the kiosk
 - Logout **NEW**
 - Logs the user out of the kiosk

- Available only when 'Require login' is enabled
- Exit kiosk **NEW**
 - Allows the user to exit the kiosk
 - Requires the service PIN to confirm the exit

4.7 Add screen

- Up to 8 screens

4.8 Remove

- Removes screen

5 Hidden apps

5.1 Remove

- Removes an applications added to list

5.2 Added application

- Added application to the list

5.3 Clear list

- Removes all applications added to list

5.4 Add application manually

- Add application to the kiosk by providing its package ID

5.5 Add applications from system

- Add applications from list of available applications in the system

ios

Updated: Dec 3, 2024

Kiosk profile allows you to limit the functionality of the device to specific applications. You can use the Kiosk profile to configure the device to use only one or a few specific applications.

Compatibility Android

Compatibility iOS

☐

Disable volume adjustment

☒ Disable touch

☐ Disable Screen rotation

☒ Disable Ringer switch

☐ Disable Sleep/Wake button

☐ Disable Auto Lock

☐ Enable VoiceOver

☐ Enable Zoom

☐ Enable Invert Colors

☐ Enable AssistiveTouch

☐ Enable Speak Selection

☐ Enable Mono Audio

i

Adding apps to the profile will not force their installation on the device. The view below is for illustrative purposes only. Only the package name is taken into account and the icon and name of the application may differ on the device.

APP

Package Id:

Start typing...

Reset filters

Selected: 0 | Deselect all



☐	ICON	APP NAME	PACKAGE ID
☐		Gmail - Email by Google	com.google.gmail

Results: 1

<<

<

1

>

>>

Clear list

Add application manually

Add applications from system

1 Configuration

1.1 Disable volume adjustment

- If checked, disable volume buttons in Kiosk

1.2 Disable touch

- If checked, disable touch in Kiosk

1.3 Disable Screen rotation

- If checked, disable Screen rotation in Kiosk

1.4 Disable Ringer switch

- If checked, disable Ringer switch in Kiosk

1.5 Disable Sleep/Wake button

- If checked, disable Sleep/Wake button in Kiosk

1.6 Disable Auto Lock

- If checked, disable Auto Lock in Kiosk

1.7 Enable VoiceOver

- If checked, enable VoiceOver in Kiosk

1.8 Enable Zoom

- If checked, enable Zoom feature in Kiosk

1.9 Enable Invert Colors

- If checked, enable Invert Colors in Kiosk

1.10 Enable AssistiveTouch

- If checked, enable AssistiveTouch in Kiosk

1.11 Enable Speak Selection

- If checked, enable Speak Selection in Kiosk

1.12 Enable Mono Audio

- If checked, enable Mono Audio in Kiosk

2 Apps

2.1 Remove

- Removes an applications added to list

2.2 Application row

- Details of application added to kiosk

2.3 Clear list

- Remove all applications added to list

2.4 Add application manually

- Add application to the kiosk by providing its package ID

2.5 Add applications from system

- Add applications from list of available applications in the system

Location

Updated: Jun 3, 2026

Location profile determines the manner of monitoring the device, refreshing its location and displaying on the map.

Compatibility:

- Android
- Android Enterprise Device Owner
- Android Enterprise Profile Owner

Name:

Example

LOCATION HISTORY

☒ Save History

Time period (in days, 1-90):

1

☐ Require high accuracy ⓘ

☐ Send location when initiating phone call ⓘ

☐ Require location services enabled when initiating a phone call ⓘ

LOCATION

Localization type:

Interval

Time period (in minutes, 5-1440):

5

TIME LIMITS

☐ Time limits for profile ⓘ

Monday:

☒ Off

☐ Whole day

☐ Advanced

Tuesday:

☒ Off

☐ Whole day

☐ Advanced

Wednesday:

☒ Off

☐ Whole day

☐ Advanced

Thursday:

☒ Off

☐ Whole day

☐ Advanced

Friday:

☒ Off

☐ Whole day

☐ Advanced

Saturday:

☒ Off

☐ Whole day

☐ Advanced

Sunday:

☒ Off

☐ Whole day

☐ Advanced

1

Name

- Name of the Location profile
- Maximum length of the text is 255
- Required

2

Location history

2.1 Save history

- Allows to save location history

2.2 Time period (in days, 1-90)

- Set the time period for saving your location history
- Available if "Save History" is checked

2.3 Require high accuracy

- Requires high location accuracy on device
- Option is not supported on devices with Android 9.0 and higher

2.4 Send location when initiating phone call

- Option is not supported on devices with Android Enterprise Profile Owner activation

2.5 Require location services enabled when initiating a phone call

- Option is not supported on devices with Android Enterprise Profile Owner activation
- Available if "Send location when initiating phone call" is checked

3 Location Category

3.1 Interval

3.1.1 Localization Mode

- One of:
 - Interval
 - Tracking

3.1.2 Time Period (in minutes, 5-1440)

- Set location download interval
- Available if "Localization Mode: Interval" is chosen

3.2 Tracking

3.2.1 Localization Mode

- One of:
 - Interval
 - Tracking

3.2.2 Walking (in meters, 100-500)

- Set the distance to download location while walking

3.2.3 Running (in meters, 500-2000)

- Set the distance to download location while running

3.2.4 Driving (in minutes, 1-30)

- Set the distance to download location while driving

3.2.5 Restrictions while moving

- One of:
 - None
 - Lock apps

3.2.6 Specify time of tolerance to disable apps (in seconds, 0-600)

- Specify time of tolerance after which applications will be disabled
- Available if "Restrictions while moving: Lock apps" or "Restrictions while moving: Hide apps" is chosen

3.2.7 Specify time of tolerance to enable apps (in seconds, 0-600)

- Specify time of tolerance after which applications will be enabled

- Available if "Restrictions while moving: Lock apps" or "Restrictions while moving: Hide apps" is chosen

3.2.8 Specify the speed of movement to apply the rule (km/h, 1-60)

- Specify the speed of movement
- Available if "Restrictions while moving: Lock apps" or "Restrictions while moving: Hide apps" is chosen

3.2.9 Clear list

- Removes all applications added to list
- Available if "Restrictions while moving: Lock apps" or "Restrictions while moving: Hide apps" is chosen

3.2.10 Add application manually

- Add app which you want to be excluded from restrictions while moving by providing its package ID
- Available if "Restrictions while moving: Lock apps" or "Restrictions while moving: Hide apps" is chosen

3.2.11 Add applications from system

- Add apps which you want to be excluded from restrictions while moving from list of available applications in the system
- Available if "Restrictions while moving: Lock apps" or "Restrictions while moving: Hide apps" is chosen

4 Time limits

4.1 The limits for the profile

- The limits for the location profile allow you to adjust the location download to the users work time. Time is applied to the users device

4.2 Off

- Location will not be downloaded on selected days

4.3 Whole day

- Location will be downloaded during whole day

4.4 Advanced

- Set the specific time of location download during the day

4.5 From

- Select the time from which you want the location to be downloaded

4.6 To

- Select the time to which you want the location to be downloaded

MTP

Updated: Jun 9, 2026

MTP profile monitors the device and detects potential threats to which it may be exposed. In addition, the profile allows you to configure specific responses to the security incident detected.

Compatibility:

- Android
- Android Enterprise Device Owner
- Android Enterprise Profile Owner

* Name:

Example

ACTION	REACTION
Device protection	
☐ Root: Dangerous ⓘ	Only notify user
☐ Root: Critical ⓘ	Only notify user
☐ Knox Warranty Bit ⓘ	Only notify user
☐ Fake device location ⓘ	Only notify user
☐ USB debugging enabled ⓘ	Only notify user
☐ Developer options enabled ⓘ	Only notify user
☐ No password on the device ⓘ	Only notify user
Application security	
☐ Unsafe admins ⓘ	Only notify user
☐ Installation of prohibited applications ⓘ	Only notify user
Network traffic analysis	
☐ Device has connected to an unsecured Wi-Fi ⓘ	Only notify user
☐ Device has connected to rogue Wi-Fi ⓘ	Only notify user
☐ DNS change on device ⓘ	Only notify user
☐ Proxy change on device ⓘ	Only notify user
☐ Gateway change on device ⓘ	Only notify user
☐ No internet on the device ⓘ	Only notify user

1 Name

- Enter the name of the MTP profile
- Maximum length of the text is 255
- Required

2

Device protection

2.1 Root: Dangerous

- Files used to root have been detected on device. However, this does not mean that device has been rooted. There are known cases when device was pre-loaded with such files in memory.

2.2 Root: Critical

- Rooting is process of obtaining unauthorized access or elevated permissions on the system. It can potentially create security loopholes that may not be easy to find or bypass device security measures.

2.3 Knox Warranty Bit

- The Samsung Knox warranty bit is a security feature that detects if unofficial software has been installed on device. This helps prevent malicious attempts from accessing data. The Knox Warranty Bit detects if a non-Knox kernel has been loaded on the device. It is a one-time programmable bit e-fuse. If a non-Knox boot loader or kernel has been installed on the device, Knox can no longer guarantee the security.

2.4 Fake device location

- The device presents a fake location. The use of a false location can be used to confuse device monitoring systems, including systems granting access to corporate resources based on the location of the device (e.g. geofencing). Feature unavailable on Android Enterprise Profile Owner. The feature requires the use of a location profile to work properly.

2.5 USB debugging enabled

- USB debugging is a configuration option for development purposes only. By enabling USB debugging, device can accept commands from a computer via a USB cable. Does not work for Android Enterprise Profile Owner.

2.6 Developer options enabled

- Developer options are configuration options intended for development purposes only. Once enabled, user can change advanced settings which threatens the integrity of the settings and the security of the device. Does not work for Android Enterprise Profile Owner.

2.7 No password on the device

- The device is not password protected. A strong password protects user data as well as company data from leakage or theft. It is recommended to set a numeric password or PIN code to use the device securely.

3 Application security

3.1 Unsafe admins

- Applications with admin permissions may partially control the device. Most often, such permissions have applications for email, calendar or other business applications that were given such permissions when adding business applications. This particularly applies to applications that require the application of security policies on devices. If the application is not a business application, it is recommended to uninstall the application.

3.2 Add default applications

- Adds applications with admin permissions to control the device

3.3 Remove

- Removes current application from whitelist

3.4 Installation of prohibited applications

- Application marked as unsafe or unwanted by administrator was installed.

3.5 Remove

- Removes current applications from blacklist

4 Network traffic analysis

4.1 Device has connected to an unsecured Wi-Fi

- An unsecured Wi-Fi network is vulnerable to a network attack. An enabled location service is required for Android 8 and above.

4.2 Device has connected to rogue Wi-Fi

- Rogue Wi-Fi can exploit a device vulnerability to connect to unknown Wi-Fi network by impersonating a trusted network. An enabled location service is required for Android 8 and above.

4.3 Safe network configuration 1

- Enter the SSID to connect to with safe network

4.4 Remove

- Removes an already added network

4.5 MAC address

- Enter the correct MAC address to join the safe network
- Required

4.6 Add safe network configuration

- Adds field with new safe network configuration
- Required if 'Safe network configuration 1' checked

4.7 DNS change on device

- Changing the DNS configuration on a device may indicate that data is being sent to an unknown destination (it could be an attempt at an MITM - Man in the middle attack). An enabled location service is required for Android 8 and above.

4.8 Proxy change on device

- Changing the proxy configuration on a device may indicate that data is being sent to an unknown destination (it could be an attempt at an MITM - Man in the middle attack). An enabled location service is required for Android 8 and above.

4.9 Gateway change on device

- Changing the gateway on a device may indicate that data is being sent to an unknown destination (it could be an attempt at an MITM - Man in the middle attack). An enabled location service is required for Android 8 and above.

4.10 No internet on the device

NEW

- The device does not have an active internet connection. Lack of network access may prevent proper communication with the MDM system, receiving security policies, and installing system and application updates.

Reactions

1 Switch

- Enable the switch to select a reaction

2 Reaction

- One of:
 - Only notify user
 - Wipe device
 - Wipe company data
 - Lock workspace
 - Turn off Wi-Fi
 - Turn off Bluetooth

3 Phone number

- Enter the phone number to send the message
- Leaving this field empty will cause the 'Contact Administrator' button not to appear on the device
- Available when 'Reaction' is selected as 'Lock workspace'

4 Header

NEW

- Define the header text. If the field is left empty, the default value will be displayed on the device.
- Available when 'Reaction' is selected as 'Lock workspace'

5 Tolerance

- Set the time period before the reaction is triggered (from 15 minutes to 72 hours)
- Required if 'Reaction' is selected as 'Lock workspace'

6 Message

- Enter the content to send it to the indicated number
- Required if 'Reaction' is selected as 'Lock workspace'

SCEP

Updated: Jul 16, 2026

Deprecated

[Click here to hang out how to create a new certificate type](#)

SCEP profile automatically configure request the user certificate to authenticate the client without specifying domain credentials.

Compatibility:

- Android Enterprise Device Owner
- Android Enterprise Profile Owner

* Name:

Example

* Access address:

Example access address

CA ID:

* Subject:

{User:Email}

* Encryption Algorithm:

AES256

* Encryption signature:

SHA256

* Key length:

2048

* Fingerprint:

Example fingerprint

* Password:

☐ Key encipherment

☐ Digital signature

ALTERNATIVE NAMES

TYPE	* VALUE	ACTIONS
NT_principal_Name	Example value	

Clear

Add

1 Name

- Enter the name of the SCEP profile

- Maximum length of the text is 255
- Required

2

Basic configuration

2.1 Access address

- Enter the name of the URL for the SCEP server (eg. Network Device Enrollment Service)
- Only 80 (HTTP) port is supported by default
- Exemplary URL: `http:///certsrv/mscep/mscep.dll`
- Maximum length of the text is 255
- Required

2.2 CA ID

- Enter the name of the profile for SCEP servers (eg. Network Device Enrollment Service) that support named-profiles.
- Maximum length of the text is 255

2.3 Subject

- Global variables available
- Required

2.4 Encryption Algorithm

- Type of encryption algorithm. Defines how strong security will be.
- One of:
 - DES
 - DES3
 - AES128
 - AES192
 - AES256
- Required

2.5 Encryption signature

- Type of encryption signature. Defines how strong security will be.
- One of:
 - SHA1
 - SHA256
 - SHA384
 - SHA512
- Required

2.6 Key length

- Length of the key. Defines how strong security will be
- One of:
 - 1024
 - 2048
 - 3072
 - 4096
- Required

2.7 Fingerprint

- Enter the fingerprint of the CA issuing the root certificate on SCEP server (eg. Network Device Enrollment Service)
- Maximum length of the text is 500
- Required

2.8 Password

- Enter the enrollment challenge password generated during a SCEP server deployment
- The value should be a 32-digit string of alphanumeric characters
- Maximum length of the text is 255
- Required

2.9 Key encipherment

- If checked, use as key encipherment
- Use when the sender and receiver of the public key need to derive the key without using encryption

2.10 Digital signature

- If checked, use as digital signature
- Specific type of signature that is backed by a digital certificate. It's providing proof of your identity

3 Alternative names

3.1 Type

- One of:
 - Distinguished_Name
 - NT_principal_Name
 - RFC822_Name
 - DNS_Name
- Required

3.2 Value

- Global variables available
- Required

3.3 Remove

- Removes added alternative name

3.4 Clear

- Removes all alternative names added to list

3.5 Add

- Adds alternative name to list

Shared device

Updated: Jun 3, 2026

BETA

The Shared device profile allows user switching on devices without administrator intervention. Device users can use local or domain credentials for authorization and verification.

Compatibility:

- Android Enterprise Device Owner
-

*** Name:**

Example

☐ Login on device ⓘ

☒ Force login

*** Login type:**

Local ▼

System message:

Example message

(15 / 255 chars)



Sign in

Example message

Username

Password ⓘ

Login

☐ Logout from device ⓘ [Coming soon](#)

1 Name

- Enter the name of the Shared device profile
- Max length of the text is 255
- Required

2 Login on device

- Configure the way of login on the device

3 Force login

- If checked, the user must log in to use the device

4 Login type

- Available options:
 - Local
 - Domain
- Required

5 System message

- Enter the text of the message that will be displayed on the login view
- Maximum length is 255

6 Preview

- Preview of the configured profile on the device

7 Logout from the device

Coming soon

VPN

Updated: Jun 3, 2026

VPN profile determines the manner of connecting with the local corporate network.

Compatibility:

- iOS
- macOS

* Name:

Example

TYPE

☐ Proget IPsec

☐ IPsec

☐ IKEv2

☐ L2TP

☐ Custom SSL

1

Name

- Name of the VPN profile
- Maximum length of the text is 255
- Required

2

Proget IPsec

3

IPsec

4

IKEv2

5

L2tp

6

Custom SSL

Proget IPsec

Updated: Dec 3, 2024

Proget IPsec VPN is a custom protocol, consists of set of standards used to establish a VPN connection.

GENERAL

Automatic disconnect: ⓘ

0

Wi-Fi exclusions: ⓘ

Add

VPN Requests (Never Connect):

Add

VPN Requests (Connect if needed):

Add

PROXY

Proxy configuration:

None

URL of the proxy auto configuration:

Name or IP address of the proxy server:

Proxy server port:

User: ⓘ

Password: ⓘ

1.1 Automatic disconnect

- The VPN connection will automatically disconnect after a fixed period of inactivity
- Minimum value is 0
- Maximum value is 1800
- If chosen value is 0 then 'Automatic disconnect' will be off

1.2 Wi-Fi exclusions

- Automatically disconnect when connected to specified Wi-Fi

1.3 VPN Request (Never Connect)

- The field specifies the domain name or URL address. The specified domains will not trigger a VPN connection nor be accessible through an existing VPN connection.

1.4 VPN Request (Connect if needed)

- The field specifies the domain name or URL address. Calling the address with the domain specified in this field will trigger a VPN connection attempt if domain name resolution succeeds. A fully-qualified domain name is supported. A wildcard '*' prefix is supported.

2 Proget IPsec Proxy

2.1 Proxy configuration

- One of:
 - Automatic
 - Manual
- Proxy servers act as relays between the website you're visiting and your device

2.2 URL of the proxy auto configuration

- Enter the URL through which all network traffic will be rerouted
- Required if 'Proxy configuration: Automatic' is chosen

2.3 Name or IP address of the proxy auto configuration

- Enter the IP address or host name of the VPN server
- Required if 'Proxy configuration: Manual' is chosen

2.4 Proxy server port

- Enter the port number which is a part of the addressing information used to identify the receivers and senders of network messages
- Minimum value is 0
- Maximum value is 65535
- Available if 'Proxy configuration: Manual' is chosen

2.5 User

- Enter the name of user account for proxy authentication
- Available if 'Proxy configuration: Manual' is chosen

2.6 Password

- Enter the password of user Proxy authorization
- Available if 'Proxy configuration: Manual' is chosen

IPsec

Updated: Dec 3, 2024

IPsec VPN is a protocol, consists of set of standards used to establish a VPN connection.

GENERAL

* Server: ⓘ

Example server

User: ⓘ

Password: ⓘ

* Authorization method:

Shared Secret / Group Name

* Shared Secret: ⓘ

Group Name: ⓘ

☐ Ask for password ⓘ

☐ Mixed authentication ⓘ

PROXY

Proxy configuration:

None

URL of the proxy auto configuration:

Name or IP address of the proxy server:

Proxy server port:

User: ⓘ

Password: ⓘ

1.1 Server

- Enter name or IP address of the VPN server
- Required

1.2 User

- Enter user account to authorize the connection

1.3 Password

- Enter the user password to authorize the connection

1.4 Authorization method

- Authorization method
- Can't be changed

1.5 Shared Secret

- Enter the common password for VPN connection
- Required

1.6 Group Name

- Enter the Group Identifier for the connection authentication

1.7 Ask for password

- If checked, user will be asked for password on the device

1.8 Mixed authentication

- Authorize a connection with a password, name and server certificate

2 IPsec Proxy

2.1 Proxy configuration

- One of:
 - Automatic
 - Manual
- Proxy servers act as relays between the website you're visiting and your device

2.2 URL of the proxy auto configuration

- Enter the URL through which all browser traffic will be rerouted
- Required if 'Proxy configuration: Automatic' is chosen

2.3 Name or IP address of the proxy auto configuration

- Enter the IP address or host name of the VPN server
- Required if 'Proxy configuration: Manual' is chosen

2.4 Proxy server port

- Enter the port number which is a part of the addressing information used to identify the receivers and senders of network messages
- Minimum value is 0
- Maximum value is 65535
- Available if 'Proxy configuration: Manual' is chosen

2.5 User

- Enter the name of user account for proxy authentication
- Available if 'Proxy configuration: Manual' is chosen

2.6 Password

- Enter the password of user Proxy authorization
- Available if 'Proxy configuration: Manual' is chosen

IKEv2

Updated: Dec 3, 2024

Internet Key Exchange version 2 (IKEv2) is a tunneling protocol, based on IPsec, that establishes a secure VPN communication between VPN devices and defines negotiation and authentication processes for IPsec security associations (SAs).

GENERAL * Address: Example address ☐ Disable MOBIKE Dead Peer Detection Rate: None ☐ Disable redirect ☐ Enable certificate revocation check ☐ Enable fallback ☐ Enable PFS TLS minimum version: 1.0 TLS maximum version: 1.0 * Identifier: Example identifier * NAT Keepalive interval: 20 ☐ Enable NAT Keepalive offload * Remote identifier: Example remote identifier ☐ Use configuration attribute internal IP subnet ☐ Per App VPN	CHILD SA PARAMS Diffie-Hellman group: 1 Encryption algorithm: DES Integrity algorithm: SHA2-256 Life time in minutes: 10 IKE SA PARAMS Diffie-Hellman group: 1 Encryption algorithm: DES Integrity algorithm: SHA2-256 Life time in minutes: 10
AUTHORIZATION TYPE ☒ Certificate Certificate type: ECDSA512 * Certificate: Certificate * Certificate profile: certificateVpn SCEP profile: Select Server certificate common name: Server certificate issuer common name: ☐ Extended auth enabled Extended auth type: Select User: Password: ☐ Shared secret Shared Secret: ☐ Extended auth enabled Extended auth type: Select User: Password: Certificate: Select Certificate profile: Select SCEP profile: Select ☐ None ☐ Extended auth enabled Extended auth type: Select User: Password: Certificate: Select Certificate profile: Select SCEP profile: Select	
PROXY Proxy configuration: None URL of the proxy auto configuration: Name or IP address of the proxy server: Proxy server port: User: Password:	

1

IKEV2 General

1.1 Address

- Enter the address URL
- Required

1.2 Disable MOBIKE

- If checked, MOBIKE is disabled
- MOBIKE allows to remain connected to the VPN even if user move to a different network

1.3 Dead Peer Detection Rate

- The frequency at which the IKEv2 client will run the dead peer detection algorithm
- One of:
 - None
 - Low (every 30 minutes)
 - Medium (every 10 minutes)
 - High (every 1 minute)

1.4 Disable redirect

- If checked, IKEv2 server redirects are disabled

1.5 Enable certificate revocation check

- If checked, evocation checking of the IKEv2 server certificate is enabled
- If checked, during IKEv2 negotiation the certificate identifying the server is checked to see if it has been revoked

1.6 Enable fallback

- If checked, enable the use of cellular data when Wi-Fi connectivity is poor

1.7 Enable PFS

- If checked, Perfect Forward Secrecy is enabled

1.8 TLS minimum version

- One of:
 - 1.0
 - 1.1
 - 1.2

1.9 TLS maximum version

- One of:
 - 1.0
 - 1.1
 - 1.2

1.10 Identifier

- Enter the local Identifier of the IKEv2 client
- Required

1.11 NAT Keepalive interval

- Enter the frequency in seconds at which gateway sends NAT Keepalive packets to its peer to keep the NAT session alive, so that the peer can access the device
- Minimum value is 20
- Maximum value is 1400
- Required

1.12 Enable NAT Keepalive offload

- If checked, Keepalive packets will be offloaded to hardware while the device is asleep

1.13 Remote identifier

- Enter the Remote Identifier of the IKEv2 client
- Required

1.14 User configuration attribute internal IP subnet

- If checked, split tunnel configurations won't be communicated via traffic selectors during IKE negotiation

1.15 Per App VPN

- If checked, allows to use VPN configuration per application

2 Child SA Params

2.1 Diffie-Hellman group

- Diffie-Hellman groups determine the strength of the key used in the key exchange process
- One of:
 - 1
 - 2
 - 5
 - 14
 - 15
 - 16
 - 17
 - 18
 - 19
 - 20
 - 21
 - 31

2.2 Encryption algorithm

- Type of encryption algorithm. Defines how strong security will be.
- One of:
 - DES
 - 3DES
 - 3DAES-128ES
 - AES-256
 - AES-128-GCM
 - AES-256-GCM
 - ChaCha20Poly1305

2.3 Integrity algorithm

- Type of integrity algorithm. Defines how strong security will be.
- One of:
 - SHA1-96
 - SHA1-160
 - SHA2-256
 - SHA2-384
 - SHA2-512

2.4 Life time in minutes

- The duration of the lifetime of the Security Association
- Minimum value is 10
- Maximum value is 1440

3 IKE SA Params

3.1 Diffie-Hellman group

- Diffie-Hellman groups determine the strength of the key used in the key exchange process
- One of:
 - 1
 - 2
 - 5
 - 14
 - 15
 - 16
 - 17
 - 18
 - 19
 - 20
 - 21
 - 31

3.2 Encryption algorithm

- Type of encryption algorithm. Defines how strong security will be.
- One of:
 - DES
 - 3DES
 - 3DES-128ES
 - AES-256
 - AES-128-GCM
 - AES-256-GCM
 - ChaCha20Poly1305

3.3 Integrity algorithm

- Type of integrity algorithm. Defines how strong security will be.
- One of:
 - SHA1-96
 - SHA1-160
 - SHA2-256
 - SHA2-384
 - SHA2-512

3.4 Life time in minutes

- The duration of the lifetime of the Security Association
- Minimum value is 10
- Maximum value is 1440

4 Authorization Type - Certificate

4.1 Certificate type

- One of:
 - RSA
 - ECDSA256
 - ECDSA384
 - ECDSA512
 - Ed25519

4.2 Certificate

- Type of certificate that is created in Proget system
- One of:
 - Certificate
 - SCEP

4.3 Certificate profile

- Name of Certificate profile which will be used
- Required if 'Certificate: Certificate' is chosen

4.4 SCEP profile

- Name of SCEP profile which will be used
- Required if 'Certificate: SCEP' is chosen

4.5 Server certificate common name

- Enter a string containing the value of the Subject Common Name field of the IKEv2 server's certificate

4.6 Server certificate issuer common name

- Enter a string containing the value of the Subject Common Name field of the Certificate Authority certificate that issued the IKEv2 server's certificate.

4.7 Extended auth enabled

- If checked, allows to use extended authorization

4.8 Extended auth type

- One of:
 - User
 - Certificate
- Required if 'Extended auth enabled' is checked

4.9 User

- Enter the name of the user
- Required if 'Extended auth type: User' is chosen

4.10 Password

- Enter the user password
- Available if 'Extended auth type: User' is chosen

5 Authorization Type - Shared secret

5.1 Shared Secret

- Enter the common password for VPN connection
- Required

5.2 Extended auth enabled

- If checked, allows to use extended authorization

5.3 Extended auth type

- One of:
 - User
 - Certificate
- Required if 'Extended auth enabled' is checked

5.4 User

- Enter the name of the user
- Required if 'Extended auth type: User' is chosen

5.5 Password

- Enter the user password
- Available if, 'Extended auth type: User' is chosen

5.6 Certificate

- One of:
 - Certificate
 - SCEP
- Required if 'Extended auth type: Certificate' is chosen

5.7 Certificate profile

- Name of Certificate profile which will be used
- Required if 'Certificate: Certificate' is chosen

5.8 SCEP profile

- Name of SCEP profile which will be used
- Required if 'Certificate: SCEP' is chosen

6 Authorization Type - None

6.1 Extended auth enabled

- If checked, allows to use extended authorization

6.2 Extended auth type

- One of:
 - User
 - Certificate
- Required if 'Extended auth enabled' is checked

6.3 User

- Enter the name of the user
- Required if 'Extended auth type: User' is chosen

6.4 Password

- Enter the user password
- Available if, 'Extended auth type: User' is chosen

6.5 Certificate

- One of:
 - Certificate
 - SCEP
- Required if 'Extended auth type: Certificate' is chosen

6.6 Certificate profile

- Chose the name of Certificate profile which will be used
- Required if 'Certificate: Certificate' is chosen

6.7 SCEP profile

- Chose the name of SCEP profile which will be used
- Required if 'Certificate: SCEP' is chosen

7 IKEV2 Proxy

7.1 Proxy configuration

- One of:
 - Automatic
 - Manual
- Proxy servers act as relays between the website you're visiting and your device

7.2 URL of the proxy auto configuration

- Enter the URL through which all browser traffic will be rerouted
- Required if 'Proxy configuration: Automatic' is chosen

7.3 Name or IP address of the proxy auto configuration

- Enter the IP address or host name of the VPN server
- Required if 'Proxy configuration: Manual' is chosen

7.4 Proxy server port

- Enter the port number which is a part of the addressing information used to identify the receivers and senders of network messages
- Minimum value is 0
- Maximum value is 65535
- Available if 'Proxy configuration: Manual' is chosen

7.5 User

- Enter the name of user account for proxy authentication
- Available if 'Proxy configuration: Manual' is chosen

7.6 Password

- Enter the password of user Proxy authorization
- Available if 'Proxy configuration: Manual' is chosen

L2TP

Updated: Dec 3, 2024

Layer 2 Tunneling Protocol (L2TP) connections provide cost-effective access for remote users by allowing a corporate network systems to manage the IP addresses assigned to its remote users.

GENERAL

* Address:

Example address

* User:

Example user

Password:

* Shared Secret:

* Disconnect on idle timer (in seconds):

1

☐ Disconnect on idle

☐ Send all traffic through VPN

PROXY

Proxy configuration:

None

URL of the proxy auto configuration:

Name or IP address of the proxy server:

Proxy server port:

User: ⓘ

Password: ⓘ

1 L2TP General

1.1 Address

- IP address or host name of VPN server
- Required

1.2 User

- Enter the name of the user
- Required

1.3 Password

- Enter the user password

1.4 Shared Secret

- Enter the common password for VPN connection
- Required

1.5 Disconnect on idle timer

- Specifies the length of time to wait before disconnecting an on-demand connection
- Minimum value is 1
- Maximum value is 9007199254740991
- Required

1.6 Disconnect on idle

- If checked, disconnects after an on-demand connection idles

1.7 Send all traffic through VPN

- If checked, all network traffic will be send through VPN

2 L2TP Proxy

2.1 Proxy configuration

- One of:
 - Automatic
 - Manual
- Proxy servers act as relays between the website you're visiting and your device

2.2 URL of the proxy auto configuration

- Enter the URL through which all browser traffic will be rerouted
- Required if 'Proxy configuration: Automatic' is chosen

2.3 Name or IP address of the proxy auto configuration

- Enter the IP address or host name of the VPN server
- Required if 'Proxy configuration: Manual' is chosen

2.4 Proxy server port

- Enter the port number which is a part of the addressing information used to identify the receivers and senders of network messages
- Minimum value is 0
- Maximum value is 65535
- Available if 'Proxy configuration: Manual' is chosen

2.5 User

- Enter the name of user account for proxy authentication
- Available if 'Proxy configuration: Manual' is chosen

2.6 Password

- Enter the password of user Proxy authorization
- Available if 'Proxy configuration: Manual' is chosen

Custom SSL

Updated: Dec 3, 2024

A secure sockets layer VPN (SSL VPN) enables individual users to access an organization's network, client-server applications, and internal network utilities and directories without the need for specialized software.

* Identifier: Example Identifier	Provider type: App Proxy▼						
* Server: Example server	Disconnect on idle timer (in seconds): 1						
User:	☐ Per App VPN ☐ VPN on demand ☐ Send all traffic through VPN ☐ Exclude local network ☐ Disconnect on idle						
Provider bundle ID:							
Provider designated requirement:							
CUSTOM DATA							
Selected: 0 Deselect all							
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="width: 20px;">☐</th> <th style="width: 30%;">* KEY</th> <th style="width: 50%;">VALUE</th> </tr> </thead> <tbody> <tr> <td>☐</td> <td>Key</td> <td> Value </td> </tr> </tbody> </table>		☐	* KEY	VALUE	☐	Key	Value
☐	* KEY	VALUE					
☐	Key	Value					
Results: 1 << < 1 > >>							
Add							
AUTHORIZATION TYPE							
Certificate▼							
* Certificate profile: certificateVpn▼	Password: 👁️						
PROXY							
Proxy configuration: None▼							
URL of the proxy auto configuration:							
Name or IP address of the proxy server:	Proxy server port:						
User: ⓘ	Password: ⓘ 👁️						

1.1 Identifier

- The app's bundle ID. If the configuration is targeted at a VPN solution that uses a NetworkExtension provider, then this field contains the bundle identifier of the app that contains the provider. Contact the VPN solution vendor for the value of the identifier.
- Maximum length of the text is 255
- Required

1.2 Server

- Enter the server URL
- Maximum length of the text is 255
- Required

1.3 User

- Enter the name of the user
- Maximum length of the text is 255

1.4 Provider bundle ID

- Enter the bundle identifier for the VPN provider
- Maximum length of the text is 255

1.5 Provider designated requirement

- Use this field only when the VPN provider is implemented as a System extension
- Maximum length of the text is 255
- Required if the VPN provider is implemented as a system extension

2 Options CustomSSL

2.1 Provider type

- The type of VPN service
- One of:
 - App Proxy
 - Packet Tunnel
- If 'App proxy' is chosen, the service will tunnel traffic at the application level
- If 'Packet tunnel' is chosen, the service will tunnel traffic at the IP layer

2.2 Disconnect on idle timer

- Specifies how long a tunnel is active after its last session
- Minimum value is 1
- Maximum value is 9007199254740991
- Required

2.3 Per App VPN

- If checked, VPN configuration is only available per application

2.4 VPN on demand

- If checked, allows the system to automatically start or stop a VPN connection based on various criteria

2.5 Send all traffic through VPN

- If checked, all network traffic will route through VPN

2.6 Exclude local network

- If checked, routes all local network traffic outside the VPN

2.7 Disconnect on idle

- If checked, disconnects after an on-demand connection idles

3 Custom Data

3.1 Delete

- Removes selected key

3.2 Key

- Specific key-value pair settings
- A dictionary for configuration information specific to a given third-party VPN solution
- Refer to third-party VPN solution documentation to find out a configuration dictionary
- Refer to Proget Knowledge Base to find out an OpenVPN configuration dictionary

3.3 Value

- Specific key-value pair settings
- A dictionary for configuration information specific to a given third-party VPN solution
- Refer to third-party VPN solution documentation to find out a configuration dictionary
- Refer to Proget Knowledge Base to find out an OpenVPN configuration dictionary

3.4 Add

- Add new key

4 On Demand Rules

4.1 Delete

- Removes selected domain

4.2 Domain

- Enter the name of domain
- Required if on demand rules is added

4.3 Value

- One of:
 - Never
 - If needed
 - Always
- If 'Never' is chosen, the host name ends with one of these domain names, the VPN isn't started automatically. This is used to exclude a subdomain within an included domain.
- If 'If needed' is chosen, the host name ends with one of these domain names and a DNS query for that domain name fails, the VPN is started automatically
- If 'Always' is chosen, the associated domain names are treated as though they were associated with the 'If needed' key

4.4 Add

- Add new domain

5 Authorization Type

5.1 Type

- The authentication method to use
- One of:
 - Certificate
 - Password

5.2 Certificate profile

- Choose the Certificate profile which will be used
- Required if 'Type: Certificate' is chosen

5.3 Password

- Password which is required to authorize
- Available if 'Type: Password' is chosen

6 Proxy CustomSSL

6.1 Proxy configuration

- One of:
 - Automatic
 - Manual
- Proxy servers act as relays between the visited website and the device

6.2 URL of the proxy auto configuration

- Enter the URL through which all browser traffic will be rerouted
- Required if 'Proxy configuration: Automatic' is chosen

6.3 Name or IP address of the proxy auto configuration

- Enter the IP address or host name of the VPN server
- Required if 'Proxy configuration: Manual' is chosen

6.4 Proxy server port

- Enter the port number which is a part of the addressing information used to identify the receivers and senders of network messages
- Minimum value is 0
- Maximum value is 65535
- Available if 'Proxy configuration: Manual' is chosen

6.5 User

- Enter the name of user account for proxy authentication
- Available if 'Proxy configuration: Manual' is chosen

6.6 Password

- Enter the password of user Proxy authorization
- Available if 'Proxy configuration: Manual' is chosen

Wallpaper

Updated: Jun 3, 2026

Wallpaper profile allows to personalize your home screen and lock screen image on your Android and iOS devices. iOS devices must have supervisor mode enabled.

Compatibility:

- Android
 - Android Enterprise Device Owner
 - iOS (supervisor mode)
-

- Preview the wallpaper on your device's home screen

4 Lock screen wallpaper

- Preview your wallpaper on your device's lock screen

5 Select file of home screen wallpaper

- Allowed file types: png
- Maximum file size: 10MB
- Required if 'Lock screen wallpaper' is empty

6 Select file of lock screen wallpaper

- Allowed file type: png
- Maximum file size: 10MB
- Required if 'Home screen wallpaper' is empty

Wi-Fi

Updated: Jun 3, 2026

Wi-Fi profile defines trusted wireless networks enabled in the corporate network as well as the manner of connecting and safe authorization.

Compatibility:

- Android (to android 9)
- Android Enterprise Device Owner
- Android Enterprise Profile Owner
- iOS
- macOS

* Name:

Example

CONFIGURATION

* SSID:

Wi-Fi Example SSID

☐ Hidden network

☐ Auto Join

☐ Set static MAC address ⓘ

Security type:

Enterprise▼

Preshared key:

ENTERPRISE

Authentication protocol:

EAP-PEAP▼

Domain: ⓘ

Example domain

CA:

Do not validate▼

Access certificate:

Certificate▼

Certificate profile:

Select▼

SCAP profile:

Select▼

* Username:

Example username

* Password:

*****ⓘ

☐ Use Per-Connection password

Outer identity:

Inner authentication:

None▼

☐ Use Protected Access Credential (PAC)

☐ Provision PAC

☐ Provision PAC anonymously

1 Name

- Enter the name of the Wi-Fi profile
- Maximum length of the text is 255

- Required

2

Wi-Fi data

2.1 SSID

- Enter the name that identifies the wireless network
- Required

2.2 Hidden network

- Required if the network for which we prepare configurations hides the SSID

2.3 Auto join

- Required if the device needs default network

2.4 Set static MAC address

- Required if the device needs an non-randomized MAC address

2.5 Type of security

- One of:
 - None
 - Personal WPA/WPA2
 - Personal WPA/WPA3
 - Enterprise
- If 'None' is chosen, the network will be without security
- If 'Personal WPA/WPA2' or 'Personal WPA/WPA3' is chosen, user authentication manage is via WPA pre-shared key
- If 'Enterprise' is chosen, user authentication manage is via Remote Authentication protocol

2.6 Preshared key

- Enter the preshared key to authenticate into Wi-Fi

- Available if "Security type: Personal WPA/WPA2" or 'Personal WPA/WPA3' is chosen

3 Wi-Fi Enterprise - 1

3.1 Authentication protocol

- One of:
 - EAP-TLS
 - EAP-TTLS
 - EAP-PEAP
 - EAP-FAST

3.2 Domain

- Multiple domains can be specified, separated by semicolons (e.g. example.org;example.com)

3.3 CA Certificate

- Choose Certificate created in Proget, which will be required to authenticate into Wi-Fi

3.4 Access Certificate

- One of:
 - Certificate
 - SCEP Profile
- Available if "Authentication protocol: EAP-TLS" is chosen

3.5 Certificate profile

- Choose the SCEP profile created in Proget, which will be required to authenticate into Wi-Fi
- Available if "Authentication protocol: EAP-TLS" is chosen
- Available if "Access certificate: Certificate" is chosen

3.6 SCEP profile

- Choose the SCEP profile created in Proget, which will be required to authenticate into Wi-Fi
- Available if "Authentication protocol: EAP-TLS" is chosen

- Available if "Access certificate: SCEP" is chosen

4 Wi-Fi Enterprise - 2

4.1 Username

- Maximum length of the text is 64
- Required

4.2 Password

- Available if "Authentication protocol: EAP-TTLS / EAP-PEAP / EAP-FAST" is chosen
- Maximum length of the text is 64
- Required

4.3 Use Per-Connection password

- If checked, the Per-Connection password is required
- Available if "Authentication protocol: EAP-TTLS / EAP-PEAP / EAP-FAST" is chosen

4.4 Outer identity

- Available if "Authentication protocol: EAP-TTLS / EAP-PEAP / EAP-FAST" is chosen
- Maximum length of the text is 256

4.5 Inner authentication

- Available if EAP-TTLS authentication protocol selected
- One of:
 - NONE
 - PAP
 - CHAP
 - MSCHAP
 - MSCHAPV2
 - GTC
 - EAP

- Available if "Authentication protocol: EAP-TTLS" is chosen

4.6 Use protected Access Credential (PAC)

- Available if "Authentication protocol: EAP-FAST" is chosen

4.7 Provision PAC

- Available if "Authentication protocol: EAP-FAST" is chosen
- Available if "Use protected Access Credential (PAC)" is checked

4.8 Provision PAC anonymously

- Available if "Authentication protocol: EAP-FAST" is chosen
- Available if "Use protected Access Credential (PAC)" is checked
- Available if "Provision PAC selected" is checked

Labels

Updated: Jun 3, 2026

Labeling groups and users allows you to assign devices to them.

Name:

[Reset filters](#)

Selected: 0 | [Deselect all](#) |

[Add](#)

☐	NAME	USERS	ROLES	LDAP	ENTR...	GROU...
☐	admin	0	1	0	0	1
☐	user	1	1	0	0	1

Results: 2 | Page limit: 50

[<<](#) [<](#) [1](#) [>](#) [>>](#)

1 Filter

- Use filters to find the right label

2 Links

- This action allows you to display all label links

3 Edit

- This action allows you to edit the selected label from the list

4 Delete

- This action allows you to remove selected labels from the list

5 Add label

5.1 Label name

- Set name to create new label
- Required

5.2 Color

- Choose label color
- Required

6 Label list

- List of labels, that have been created along with the number of associations with specific elements

Audit logs

Updated: Jun 3, 2026

A place intended for collecting and viewing information about events occurring on the server.

Audit logs

 Give feedback

Action: Select  

Status: Select  

Date of occurrence: From Select To Select  

Reset filtersBASICPQL

ACTION	STATUS	DATE OF OCCURRENCE 	PERFORMED BY	PERFORMED ON	DETAILS
user.authenticate	Success	2025-07-08 14:19:12	Ironman Ironman (...)	Ironman Ironman (...)	User authentication success. Authentication (l...

1

Filter

- Use filters to find the right log

2

Log list

- List of logs that were generated as a result of a specific action in the console

Tasks

Updated: Dec 3, 2024

Tasks sent to the devices created by system users or the system.

Action: Select ⌵ 🗑Serial number: Start typing... 🗑IMEI: Start typing... 🗑User: Start typing... 🗑 +

Reset filters

Selected: 0 | Deselect all 🔄 🗑

📄 ✓

☐	SENT DATE ⌵	COMPLETE DATE ⌵	ACTION	CREATED BY	MANUFACTURER	MODEL	USER	STATUS
☐	2024-08-31 14:52:37	2024-08-31 14:52:42	Change password	jdoe	SAMSUNG	SM-A225F	John Doe	Success
☐	2024-08-31 14:52:18	2024-08-31 14:52:25	Send message	jdoe	SAMSUNG	SM-A225F	John Doe	Success
☐	2024-08-31 14:52:03	2024-08-31 14:52:04	Install app 🔗	jdoe	SAMSUNG	SM-A225F	John Doe	Success
☐	2024-08-31 13:56:15	2024-08-31 13:56:15	Policy update 🔗	system	SAMSUNG	SM-A225F	John Doe	Success
☐	2024-08-31 13:56:15	2024-08-31 13:56:15	Refresh device data	system	SAMSUNG	SM-A225F	John Doe	Success

Results: 5 | Page limit: 50 ⌵

⏪ ⏴ 1 ⏵ ⏩

1 Filters

- Use filters to search for relevant tasks

2 Restart task

- This action allows you to restart selected tasks with failed status

3 Remove task

- This action allows you to remove selected tasks with created, pending, received, failed and canceled status

4 Tasks list

- List of all tasks with its parameters

Service

Updated: Jun 3, 2026

Service tab contains the data about devices that have ever been activated on a given server, even after deactivation, until the server is destroyed.

IMEI: 352946245353881 X Serial number: R0C7T714K038 X User: Start typing... Manufacturer: Select +

Reset filters

Selected: 1 Deselect all



 v

☒	MANUFACTURER	MODEL	IMEI	SERIAL NUMBER	USER	FILES	
☒	SAMSUNG	SM-G991B	352946245353881 352946245353881	R0C7T714K038	John Doe	example.csv - 169 B X	...

Results: 1 | Page limit: 50

 1 

1 Filter

- Use filters to search for relevant device

2 Actions

2.1 Update the data

- This action allows you to update the data of the selected device

2.2 Set comment

- This action allows you to set comment for the selected device

2.3 Device users history

- This action allows you to display device users history

2.4 Export data

- This action allows you to export the data from the selected device

2.5 Security codes

Deprecated

- This action displays security codes for the selected device

2.6 Upload files

- This action allows you to upload files to the files column of the selected device

2.7 Download files

- This action allows you to download files from the files column of the selected device

2.8 Delete files

- This action allows you to delete files from the files column of the selected device

3 Device list

- A list of devices that have ever been activated on a given server, even after deactivation, until the server is destroyed

Update

Updated: Jul 16, 2026

In the update device information view you can edit data about the given device.

Update device information

Device name:

SAMSUNG

Model:

SM-G991B

Serial number:

48562771544028

IMEI:

352049242521000, 352049242521000

User:

John Doe

Invoice No:

Example

Date of purchase:

Select date

Warranty:

Example

Operator:

Example

Agreement expiration date:

Select date

Address:

Example

Comment:

Insert text here...

(0 / 550 chars)

1 Device name

- Displays the device's name - manufacturer
- This field cannot be modified

2 Model

- Displays the device's model
- This field cannot be modified

3 Serial number

- Displays the device's serial number
- This field cannot be modified

4 IMEI

- Displays the device's IMEI
- This field cannot be modified

5 User

- Displays currently assigned user

- This field cannot be modified

6 Invoice No

- Enter the invoice no

7 Date of purchase

- Enter date of purchase

8 Warranty

- Enter warranty information

9 Operator

- Enter the operator information

10 Agreement expiration date

- Enter the agreement expiration date

11 Address

- Enter the address

12 Comment

- Enter any additional information

Service history

Updated: May 28, 2026

Device users history contains the data about previous users of the given device.

Device users history

Selected: 1

Deselect all

☒ USER	REGISTRATION TYPE	REGISTRATION DATE	DEREGISTRATION DATE	LOCATION	PHONE	
☒ John Doe	Android Enterprise Device Owner	2024-01-18 14:14:12	2024-01-18 15:53:33	-	-	...

Results: 1

Page limit: 50

<<

<

1

>

>>

1

Generate service password

- Generates service password for selected registration of the chosen device

2

List of device users history

- List of the device users history with the registration type, registration date, registration date, location and phone

Service password

Updated: Jun 9, 2026

NEW

The Service password panel available in the Service section allows the administrator to generate an emergency service password for any device. The password is linked to a specific device and has a defined validity period (default 24 hours, minimum 5 minutes, maximum 30 days). It works even when the device has no internet connection or the local database is damaged. Available actions and their behavior depend on the device activation type - some options may be unavailable or behave differently on COPE and Android MDM activations. After use, the device enters a 60-minute privileged window, after which it returns to the state required by policies. The password can be entered manually or scanned as a QR code on the device.



Service password

* Select actions: ⓘ

- ☐ Unblock device
- ☐ Disable Kiosk
- ☐ Remove network restrictions ⓘ
- ☐ Allow developer options
- ☐ Allow deactivation
- ☐ Allow factory reset
- ☐ Emergency Database Reset ⓘ
- ☐ Set Password ⓘ

* Service password expiration date (on device):

2026-05-07 10:23



Time to expire: in about 24 hours

- ☒ Generate QR code
- ☒ Send service password via email

* Email:

example@domain.com

Message language:

English



Cancel

Generate

1 Unlock device

- If checked, the service password will unlock the device from Lost Mode
- Behavior depends on the device activation type

2 Disable Kiosk

- If checked, the service password will exit the device from Kiosk mode
- Available only on activations that support the Kiosk profile

3 Remove network restrictions

- If checked, the service password will temporarily remove network restrictions imposed by network-related policies on the device

4 Allow developer options

- If checked, the service password will temporarily enable developer options on the device

5 Allow deactivation

- If checked, the service password will allow deactivation of the Proget MDM application on the device

6 Allow factory reset

- If checked, the service password will allow the user to perform a factory reset on the device

7 Emergency Database Reset

- If checked, the service password will authorize an emergency reset of the Proget MDM application database on the device
- It cannot be combined with other actions

8 Set Password

- If checked, the service password will allow setting a new device password in the Direct Boot scenario (after device restart)
- It cannot be combined with other actions
- Behavior depends on the device activation type

9 Service password expiration date (on device)

- Set the date and time when the service password will expire on the device
- Default validity is 24 hours, minimum 5 minutes, maximum 30 days

10 Generate QR code

- If checked, a QR code will be generated along with the service password for easier scanning on the device

11 Send service password via email

- If checked, the generated service password will be sent to the specified email address

12 Email

- Enter the email address to which the service password will be sent
- Required if 'Send service password via email' is checked

13 Message language

- Select the language in which the email message with the service password will be sent

14 Generate

14.1 Service password generated for device

- Displays the generated service password for the device
- The password can be copied to clipboard using the copy icon

14.2 QR code

- Displays the QR code containing the service password for scanning on the device
- Visible only if 'Generate QR code' was checked

Security

Updated: Dec 3, 2024

Here you can find a table with list of security events on the devices.

Status: Select

Name: Select

User: Start typing...

Event status: Select

+

Reset filters

STATUS	NAME	DATE	USER	MANUFACT...	MODEL	DEVICE STA...	EVENT STA...
Safe	Access to Wi-Fi management	2024-08-31 14:33:45	John Doe	SAMSUNG	SM-A225F	Active	Current
Information	Access to device usage data	2024-08-31 14:33:45	John Doe	SAMSUNG	SM-A225F	Active	Current
> Safe	No password on the device	2024-08-31 14:24:49	John Doe	SAMSUNG	SM-A225F	Active	Archival
Safe	Proget Remote installed	2024-08-31 13:57:38	John Doe	SAMSUNG	SM-A225F	Active	Current
Safe	Play Integrity verification status	2024-08-31 13:56:20	John Doe	SAMSUNG	SM-A225F	Active	Current
Safe	Root status	2024-08-31 13:56:11	John Doe	SAMSUNG	SM-A225F	Active	Current

Results: 6 | Page limit: 50

<<

<

1

>

>>

1 Security filter

- Security filter allows you to search for information by data, such as:
 - Status
 - Name
 - Date
 - User
 - Manufacturer
 - Model
 - Device status
 - Event status

2 List of security events on devices

- List of all security events that occurred on the device along with their parameters

Reports

Updated: Jun 3, 2026

Here you can configure and generate reports containing all important information about devices in the system.

ListConfiguration

Name: Insert text here...

Type: Select

Date: From Select ... To Select date

Reset filters

Selected: 1

Deselect all

Download

Delete

Generate

☒	NAME	TYPE	DATE	SIZE	
☒	Example	Custom	2024-09-04 13:10:20	16.73 KiB (17.13 KB)	...

Results: 1

Page limit: 50

1

1 Reports list

- The report list displays all the reports you have generated that contain information about the devices

2 Configuration

- Configuration is used to create your own report with specific variables. The report can be run cyclically and be linked to a distribution list in the form of email addresses.

List

Updated: Jul 16, 2026

Here you can find a list of generated reports containing all important information about devices in the system.

List

Configuration

Name: Insert text here...

Type: Select

Date: From Select ... To Select date

Reset filters

Selected: 1

Deselect all

Download

Delete

Generate

☒	NAME	TYPE	DATE	SIZE	
☒	Example	Custom	2024-09-04 13:10:20	16.73 KiB (17.13 KB)	...

Results: 1

Page limit: 50

<<

<

1

>

>>

1 Filters

- Report filter allows you to search for reports by data, such as:
 - Name
 - Type
 - Date

2 Download

- This action allows you to download single or more generated reports

3 Delete

- This action allows you to delete single or more generated reports

4 Generate

- This action will take you to the view where you can generate a report of your devices according to your preferences

5 Generated reports list

- List of all generated reports with its parameters

Generate report

Updated: Dec 3, 2024

Here you can generate report containing selected information about devices in the system.

* Report name:

* Format:

PDF

* Orientation:

Vertical

* Type:

Custom

Groups:

Select

☒ Send report via email

* Add recipient(s):

example@mail.com

Add

* Data generated in the report:

☒ Device ID
 ☐ Device alias
 ☐ Device vendor
 ☒ Device model
 ☐ Operating system
 ☐ Language
 ☐ Serial number
 ☐ IMEI 1
 ☐ IMEI 2
 ☐ Last contact
 ☐ Last contact (days)
 ☐ Storage (bytes)
 ☐ Available storage (bytes)
 ☐ Activation date
 ☐ Battery health

1 Report name

- Set the report name
- Required

2 Format

- In the dropdown, select the file format
- File format available:
 - CSV
 - PDF
- Required

3 Orientation

- In the dropdown, select the orientation
- Orientation available only with PDF format:
 - Vertical
 - Horizontal
- Required if selected PDF format

4 Type

- In the dropdown, select the type
- Type available:
 - Custom
 - Business application assigned to device
 - Business applications installed on device
 - Device locations
 - Devices
 - Devices last location
 - Devices security status
 - Export of users from the list
 - Inactive devices
 - Last contact with devices
 - Proget app on devices
 - User devices
- Required

5 Groups

- In the dropdown you can select the group

6 Send report via email

- If the checkbox is checked the report will be sent by email
- For this feature to work properly, SMTP must first be configured in the Settings tab

7 Add recipient(s)

- Add the email address of the recipient(s) to whom the report will be sent

8**Data generated in the report**

- If a custom type is selected, you will be able to manage what information about the device will be included in the generated report

Configuration

Updated: Jul 16, 2026

Here you can add report configuration. Setup report execution cycle, specific data and recipient(s). Reports will be generated automatically and sent via email (SMTP required). You can download generated reports from Reports tab.

[List](#) **Configuration**

Configuration is used to create your own report with specific variables. The report can be run cyclically and be linked to a distribution list in the form of email addresses.

Name: Start typing...

Type: Select 

[Reset filters](#)

Selected: 1 | **Deselect all**

[Add](#)

☒	NAME 	TYPE
☒	Example	Custom

Results: 1 | Page limit: 50 

  **1**  

1 Configuration filter

- Report filter allows you to search for reports by data, such as:
 - Name
 - Type

2 Edit

- This action allows you to edit selected configuration

3 Generate

- This action allows you to generate a report when a configuration from the configuration list is selected

4 Delete

- This action allows you to delete single or more configuration from the list

5 Add configuration

- This action will take you to the view where you can configure your own configuration

6 Configuration list

- List of all created configurations

Add report configuration

Updated: Dec 3, 2024

Here you can add report configuration. Setup report execution cycle, specific data and recipient(s). Reports will be generated automatically and sent via email (SMTP required) or you can download them from Reports tab.

* Name:

Example

REPORTS DATA

* Format:

PDF

* Orientation:

Vertical

* Type:

Custom

Groups:

Select

* Select the data to be included in the report

-

Q

☒ Device ID

☐ Device alias

☒ Device vendor

☒ Device model

☐ Operating system

☐ Language

☐ Serial number

☐ IMEI 1

☐ IMEI 2

☐ Last contact

REPORT SCHEDULER

* Recurrence:

☐ Once a day

☒ Interval

Hour:

00:00

Scheduled day(s):

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

☐ Sunday

* Hour:

00:00

* Interval (in days, 1-30):

1

REPORTS HISTORY

* Automatically delete reports older than
(in days, 1-360):

180

OTHER SETTINGS

☒ Send report via email ⓘ

* Add recipient(s):

example@mail.pl

Add

1 Name

- Set configuration name
- Required

2 Add data

2.1 Format

- In the dropdown, select the file format
- File format available:
 - CSV
 - PDF
- Required

2.2 Orientation

- In the dropdown, select the orientation
- Orientation available only with PDF format:
 - Vertical
 - Horizontal
- Required if selected PDF format

2.3 Type

- In the dropdown, select the type
- Type available:
 - Custom
 - Business application assigned to device
 - Business applications installed on device
 - Device locations
 - Devices
 - Devices last location
 - Devices security status
 - Export of users from the list
 - Inactive devices
 - Last contact with devices

- Proget app on devices
- User devices
- Required

2.4 Groups

- In the dropdown you can select the group

2.5 Select the data to be included in the report

- If a custom type is selected, you will be able to manage what information about the device will be included in the generated report
- Required

3 Add scheduler

3.1 Once the day

- If selected, you have to select the time and days in which the report will be generated

3.2 Interval

- If selected, you have to set the time and daily cycle of report generation

4 Add history

4.1 Automatically delete reports older than

- Select the number of days after which generated reports will be deleted
- Required

4.2 Send report via email

- If the checkbox is checked the report will be sent by email
- For this feature to work properly, SMTP must first be configured in the Settings tab

4.3 Add recipient(s)

- Add the email address of the recipient(s) to whom the report will be sent

Settings

Updated: Jul 16, 2026



Access control

Restrict management access to specific network addresses



Allowed SIM Cards

Manage which SIM cards are allowed on devices



Audit and logging

Record audit logs of admin activity and device interactions



Microsoft Entra ID

Manage connection and sync with Microsoft Entra ID



Certificate Manager

Manage certificates used in profiles and app configurations



Connector

Set up an LDAP connection to the Proget Cloud



Gateway

Secure gateway encrypting traffic to internal email systems



General

Organization, server, application, and TURN configuration



LDAP

Manage LDAP connections for directory synchronization



SMTP

Configure SMTP for activation emails and notifications



Roles

Configure administrative privileges for console functions



Theme

Customize the console's logo, colors, and layout



Updates

Manage manual or automatic Proget server updates

Access control

Updated: Jun 3, 2026

Option allows you to define access rules for Proget management services only from specific network addresses.

Allowed IPs:



1 Allowed IP

- Enter the IP address through which manage Proget will be allowed

2 Remove

- Remove chosen IP address

3 Add

- Add IP address

4 Disable access control

- Remove all added IP addresses

5 Submit

- Save chosen settings

Allowed SIM Cards

Updated: Jun 3, 2026

NEW

Manage the allowed SIM cards that can be used on device

Updated

Example Example

2026-05-11 12:30:19

List

Operations

1

List

- Displays the list of all allowed SIM cards (ICCID) added to the system, with the ability to search by part of the ICCID number and export the list to a CSV file

2

Operations

- Displays the history of bulk operations performed on the allowed SIM card list (add, remove, remove all), along with their status, creation and completion date, number of processed records, and operation details

List

Updated: Jun 3, 2026

The List view displays all allowed SIM cards (ICCID numbers) added to the system. It allows you to search for a specific ICCID by part of its number, manage the list through bulk operations, export the list to a CSV file, and refresh the data.

The screenshot shows a web interface for managing SIM cards. At the top, there are two tabs: 'List' (active) and 'Operations'. Below the tabs is a search bar labeled 'ICCID: Start typing...'. To the left of the search bar is a 'Reset filters' link. To the right are two tabs: 'BASIC' (active) and 'PQL'. Below the search bar is a button labeled 'Manage Allowed SIM Cards' and two icons: a square with a plus sign and a circular arrow. Below these elements is a table with one column header 'ICCID' and one row containing the value '123000123000123000'.

1 Filter

- This action allows you to filter the list of allowed SIM cards by entering a part of the ICCID number

2 Manage Allowed SIM Cards

- Use the filter to filter the list of available SIM cards by using a portion of the ICCID number.

3 Export

- This action allows you to export the current list of allowed SIM cards (ICCID numbers) to a CSV file

4 Refresh

- This action allows you to refresh the list of allowed SIM cards to display the latest data

5**List of ICCID numbers**

- Displays all ICCID numbers added to the allowed SIM cards list

Manage Allowed SIM Cards

Updated: Jun 3, 2026

The Manage Allowed SIM Cards wizard allows you to perform bulk operations on the list of allowed SIM cards (ICCID numbers). You can add new entries, remove selected ones, or remove all entries from the list. New ICCID numbers can be added from a CSV file or entered manually.

Operation type:

☒ Add

☐ Delete

☐ Delete all

☐ From file

☐ Manual input

1 Add

- This action allows you to add new ICCID numbers to the allowed SIM cards list either by importing them from a CSV file or by entering them manually

2 Delete

- This action allows you to remove selected ICCID numbers from the allowed SIM cards list either by importing them from a CSV file or by entering them manually

3 Delete all

- This action allows you to remove all ICCID numbers from the allowed SIM cards list at once

4 From file

4.1 Select file

- This action allows you to select a CSV file containing the list of ICCID numbers to be added or removed
- A sample CSV file can be downloaded from the wizard

5 Manual input

5.1 Set ICCID SIM number

- Enter the ICCID number of the SIM card to be added to or removed from the allowed SIM cards list

5.2 Add

- This action allows you to add another field for manually entering the ICCID number

Operations

Updated: Jun 3, 2026

The Operations view displays the history of bulk operations performed on the allowed SIM cards list (add, remove, remove all). For each operation it shows the type, creation and completion date, number of processed records, status, and operation details. The list can be filtered by status and refreshed to display the latest data.

ListOperations

Status: Select

Reset filters

BASICPQL

TYPE	CREATION DATE	COMPLETION DATE	PROCESSED	STATUS	DETAILS
Adding	2026-05-11 12:30:18	2026-05-11 12:30:19	1/1	Succeeded	-
Deleting	2026-05-11 04:37:40	2026-05-11 04:37:41	1/1	Succeeded	-
Deleting all	2026-05-11 04:36:56	2026-05-11 04:36:57	3/3	Succeeded	-
Adding	2026-05-11 04:36:35	2026-05-11 04:36:36	0/3	Failed	Show errors
Adding	2026-05-11 04:36:15	2026-05-11 04:36:16	3/3	Succeeded	-

1Filter

- Use the filter to filter the list of operations by status

2Refresh

- This action allows you to refresh the list of operations to display the latest data

3List of operations with their parameters

- Displays the list of bulk operations performed on the allowed SIM cards list, including operation type, creation and completion date, number of processed records, status, and operation details

Audit and logging

Updated: Feb 12, 2025

Proget has the ability to record audit logs that you can use to examine any administrative activities and interactions between the server and devices.

List

ListConfiguration

Date: Select date

Reset filters

Selected: 0 | Deselect all

Download

Delete all

☐	FILENAME	DATE	SIZE
☐	audit-2024-10-22.log	2024-10-22	809.46 KIB (828.88 KB)
☐	request-2024-10-22.log	2024-10-22	11.56 KIB (11.84 KB)

Results: 2 | Page limit: 50

<<

<

1

>

>>

1List

- List of created audit logs

2Download

- Download selected audit logs

3Delete all

- Delete all audit logs

Configuration

1 Configuration

- Configuration of audit logs

2 Save audit logs

- If checked, audit logs will be saved and visible in 'List' tab

3 Delete audit logs

- Select the time after which the saved audit logs will be deleted
- Required

Certificate Manager

Updated: Dec 3, 2024

Certificate Manager allows to manage device and user certificates that will be used in profiles and apps configurations.

CASUser certificatesExternal certificates

Name: Start typing...

Common name: Start typing...

Issuer: Start typing...

Created by: Start typing...

Reset filters

Selected: 0

Deselect all

Add

☐	NAME	COMMON NAME	ISSUER	CREATED BY
> ☐	Example 1	A	Self-signed	John Doe
> ☐	Example 2	AK	Example 1	John Doe

Results: 2

Page limit: 50

<<

<

1

>

>>

1 CAs

2 User certificates

3 External certificates

CAs

Updated: Mar 14, 2025

A CA is an internal CA that independently issues and signs the root and intermediate certificates. It enables the generation and signing of certificates for servers, users within an organisation's closed systems to ensure connection trust. By supporting the signing of internal certificates, the CA allows the management of public key infrastructures (PKI), the issuing of TLS/SSL certificates, the authentication of users and the securing of communications in private networks.

CAsUser certificatesExternal certificates

Name: Start typing...

Common name: Start typing...

Issuer: Start typing...

Created by: Start typing...

Reset filters

Selected: 1Deselect all

Download

Refresh

Add

☒	NAME	COMMON NAME	ISSUER	CREATED BY
☒	Example CA	Example CN	Self-signed	Ironman Ironman

Certificate

CN=Example CN

- CN: Example CN

```
{
  "hash": "a46973c4",
  "name": "/CN=Example CN",
  "validTo": "341119171722Z",
  "version": 2,
  "purposes": {
    "1": [
      true,
      true,
      true,
      "sslclient"
    ],
    "2": [
      true,
      true,
      "sslsrvr"
    ]
  }
}
```

Results: 1 | Page limit: 50

<<

<

1

>

>>

1Export

- Export selected CAs certificates

2Generate server certificate

2.1 Name

- Name of the selected CA

2.2 Key length

- Choose key length
- One of:
 - 1024
 - 2048
 - 3072
 - 4096

2.3 Encryption signature

- Choose type of encryption signature
- One of:
 - SHA-1
 - SHA-256
 - SHA-384
 - SHA-512

2.4 Common Name

- Enter the CA common name
- Maximum length of the text is 64
- Required

2.5 Validity (in days)

- Enter CA certificate name
- Minimum value is 30
- Maximum value is 730
- Required

2.6 Password

- Enter password which will be used to open the file

2.7 Type

- Choose the type of custom attributes, which are pieces of data that are embedded only in the CSR
- One of:
 - Distinguished_Name
 - NT_principal_Name
 - RFC822_Name
 - DNS_Name

2.8 Value

- Enter the value of type
- Global variables available
- Required

2.9 Remove

- Remove chosen custom attribute

2.10 Clear

- Remove all custom attributes

2.11 Add

- Add custom attribute

3 CA certificate info

- Main information contained in the CA certificate

4 CAs create

4.1 Name

- Enter CA certificate name
- Maximum length of the text is 64
- Required

4.2 Common name

- Enter common name
- Maximum length of the text is 64
- Required

4.3 Country code

- Enter country code
- Maximum length of text is 2

4.4 State or province

- Enter state or province name
- Maximum length of the text is 128

4.5 City

- Enter city name
- Maximum length of the text is 128

4.6 Organization

- Enter organization name

- Maximum length of the text is 64

4.7 Organization unit

- Enter organization unit name
- Maximum length of the text is 64

4.8 Key length

- Select one of available key lengths
- Required

4.9 Encryption signature

- Select encryption signature
- One of:
 - SHA-1
 - SHA-256
 - SHA-384
 - SHA-512
- Required

4.10 Certificate validity (in days)

- Enter number of days of certificate validity
- Maximum value is 3650
- Required

4.11 Signing certificate

- Select one of available signing certificates

User certificates

Updated: Dec 3, 2024

User certificates specify which resources a given user can have access to.

CAsUser certificatesExternal certificates

User: Start typing...

Profile: Start typing...

Issuer: Start typing...

Revoked: Select

Reset filters

Selected: 1

Deselect all

	USER	PROFILE	ISSUER	VALIDITY	REVOKED	
✓	John Doe	Example cert	Example 1	2025-09-06 13:40:04	-	...
Certificate CN=jdoe@proget.pl CN: jdoe@proget.pl { "hash": "ed074d66", "name": "/CN=jdoe@proget.pl", "validTo": "250906114004Z", "version": 2, "purposes": { "1": [true, false, "sslclient"], "2": [false, false, "sslserver"] }						

Results: 1 | Page limit: 50

1

1

Renew

- Renews selected certificate

2

Revoke

- The revocation of a certificate will result in the discontinuation of functionality that uses that certificate.
- The selected action is irreversible.

3

User certificate info

- Main information contained in the user certificate

External certificates

Updated: Dec 3, 2024

External certificate type here is always set as S/MIME. S/MIME stands for Secure/Multipurpose Internet Mail Extensions. This type of digital certificate enables users to secure the integrity and privacy of their emails.

CASUser certificatesExternal certificates

User: Start typing...Edited by: Start typing...

Reset filters

Selected: 1Deselect all

Add

☒	USER	TYPE	EDITED BY	VALIDITY	
☒	John Doe	S/MIME	Ironman Ironman	2025-03-07 08:40:27 2025-03-07 08:40:27	...

Signing certificate

CN=test2@bes.pl

CN: test2@bes.pl

{

"hash": "8cd37a72",

"name": "/CN=test2@bes.pl",

"validTo": "250307074027Z",

"version": 2,

"purposes": {

"1": [

false,

false,

"sslclient"

],

"2": [

false,

false,

"sslsrvr"

]

}

Encryption certificate

CN=test2@bes.pl

CN: test2@bes.pl

{

"hash": "8cd37a72",

"name": "/CN=test2@bes.pl",

"validTo": "250307074027Z",

"version": 2,

"purposes": {

"1": [

false,

false,

"sslclient"

],

"2": [

false,

false,

"sslsrvr"

]

}

Results: 1 | Page limit: 50

<<

<

1

>

>>

1

Edit

- Edit selected certificates

2 Delete

- Delete selected certificates

3 External certificate info

- Main information contained in the external certificate

4 External certificates create

4.1 Type

- Unselectable external certificate type - always set as S/MIME

4.2 User

- Select one of available users
- To find user, enter at least 3 first letters of username

4.3 Select signing certificate file

- Select file
- Allowed file type: .pfx

4.4 Delete signing certificate

- Deletes selected signing certificate

4.5 Signing certificate password

- Enter signing certificate password

4.6 Select encryption certificate file

- Select file
- Allowed file type: .pfx

4.7 Delete encryption certificate

- Deletes selected encryption certificate

4.8 Encryption certificate password

- Enter encryption certificate password

Connector

Updated: Dec 3, 2024

Connector is a module that allows you to set up an LDAP connection from a local network to a server located in the Proget Cloud.

* Name:	* Address:	* Port:
Example	example.url	123

1 Name

- Enter the name of the Connector
- Maximum length of the text is 255
- Required

2 Address

- Enter the address of server
- Maximum length of the text is 255
- Required

3 Port

- Enter the port number which is a part of the addressing information used to identify the receivers and senders of network messages
- Minimum value is 0
- Maximum value is 65535
- Required

Gateway

Updated: Dec 3, 2024

Secure email access gateway that encrypts and protects traffic between the mobile device and internal email systems.

* Gateway name: Example	* Access server address: Example Access server address * Access server port: ⓘ 443 * Email server address: Example Email Server Address * Email server port: 443	* Authentication: Local CA SCEP: Select Root certificate: ⓘ Select CA: Select
---	--	---

1

Name

1.1

Name

- Name of the Gateway
- Maximum length 255
- Required

2

Credentials

2.1 Access server address

- Enter the access server address
- Maximum length of the text is 255
- Required

2.2 Access server port

- Enter the access server port
- Maximum value is 65535
- Required

2.3 Email server address

- Enter the email server address
- Maximum length of the text is 255
- Required

2.4 Email server port

- Enter the email server port
- Maximum value is 65535
- Required

3 Credentials

3.1 Authentication

- Choose the authentication method
- One of:
 - Local CA
 - Enterprise CA
 - Certificate Manager
- Required

3.2 SCEP

- Choose one of available SCEP profiles
- Available if selected authentication method is Enterprise CA
- Required if selected authentication method is Enterprise CA

3.3 Root certificate

- Choose one of available Certificate profiles
- Available if selected authentication method is Enterprise CA
- Required if selected authentication method is Enterprise CA

3.4 CA

- Choose one of available CA certificates
- Available if selected authentication method is Certificate Manager
- Required if selected authentication method is Certificate Manager

General

Updated: Jun 3, 2026

Organization, server, application, TURN info and configuration.

Organization

Server

Application

TURN

* Organization name:

Example Company

Email address:

mail@example.com

Phone:

+48 123 123 123

* Country: ⓘ

United Kingdom

▼

* City:

Example city

* Street:

Example

* Postal Code:

12-345

* House number:

123

1.1 Organization name

- Enter the organization name
- Maximum length of the text is 128
- Required

1.2 Email address

- If entered, will be visible in Proget app
- Maximum length of the text is 128

1.3 Phone

- If entered, will be visible in Proget app
- Maximum length of the text is 64

1.4 Country

- Choose one of the countries
- Selecting a country will adjust the maps displayed in the console
- Required

1.5 City

- Enter city name
- Maximum length of the text is 64
- Required

1.6 Postal Code

- Enter postal code
- Maximum length of the text is 64
- Required

1.7 Street

- Enter street name
- Maximum length of the text is 64
- Required

1.8 House number

- Enter house number
- Maximum length of the text is 64
- Required

2 Server

2.1 Time zone

- Choose one of the time zones
- Required

2.2 Default language

- Choose default language - the default language defines what language the default policies will be in and information from application stores should be downloaded
- One of:
 - Polish
 - English
 - German
 - Russian
 - Romanian

2.3 Enable Cloudflare captcha on login

- This option allows you to enable the Cloudflare Captcha mechanism during system login

2.4 Actions for inactive devices

- Select the action that will be sent to an inactive device trying to connect to the server. Available for Windows and Android devices. iOS, macOS devices will always receive actions to wipe corporate data.
- One of:
 - Take no action
 - Wipe company data
 - Wipe device
- Required

2.5 Restore business data in case of Proget application synchronization error

- In case of a Proget app synchronization error, the user can manually restore their business data. With this functionality, there will be no need to reset the device to factory settings to re-register with the Proget console.
- One of:
 - Always allow
 - Allow after entering the security code
 - Do not allow **Deprecated**
- Required

2.6 Console SSL certificate

- Select the SSL certificate for the console from your device's resources. You will be asked to enter the certificate password and user password.

3 Application

3.1 Address to the Android application

- Enter address to the Android application
- Maximum length of the text is 255

3.2 Location of the app store

- Choose one of the countries - the location of the app store determines the country/region for searching applications in the app store. The function may affect the lack of access to applications not available in a given country/region.

3.3 Emergency number

- Entered number will be visible as emergency number on the lock screen of the device
- Maximum length of numbers is 16
- Required

4 Turn

4.1 URL

- Enter TURN URL
- Correct URL is required if administrator of Proget console wants to use Proget Remote
- Maximum length of the text is 128
- Required

4.2 Username

- Enter TURN username
- Correct TURN username is required if administrator of Proget console wants to use Proget Remote
- Required

4.3 Change password

- Enter new password
- Maximum length of the text is 256
- Available if checkbox checked
- Required if checkbox checked

4.4 Restore default

- Restores default values

5 Select certificate

5.1 Select file

- Select file you want to upload
- Allowed file type: .pfx

5.2 Certificate password

- Enter certificate password
- Required

5.3 User password

- Enter user password
- Required

1 Name

- Name of the LDAP
- Maximum length of the text is 64
- Required

2 Server and encryption

2.1 Active Directory

- If checked, LDAP will be configured as Active Directory

2.2 Domain

- Enter the domain address
- Maximum length of the text is 64
- Required if Active Directory is checked

2.3 Host name

- Enter the host name
- Maximum length of the text is 255
- Required

2.4 Port

- Enter the server port
- Maximum value is 65535
- Required

2.5 Base dn

- Enter the base dn
- Maximum length of the text is 255

2.6 Search Filter

- Enter the search filter
- Maximum length of the text is 255

2.7 Search Scope

- Choose the search scope
- One of:
 - All Levels
 - One Level
- Required

2.8 Encryption

- Choose the encryption
- One of:
 - None
 - SSL
 - TLS
- Required

2.9 Connector

- Choose one of the given connectors

2.10 Accept untrusted connection

- If checked, untrusted connections will be allowed

2.11 Choose file

- Uploads CA certificate file (LDAP SSL/TLS)

3 Credentials

3.1 User

- Enter user credentials

3.2 Password

- Enter password

3.3 User attributes

- Enter user attributes
- Available if Active Directory is checked

3.4 Remove

- Remove selected user attributes

3.5 Add

- Add more user attributes

4 Synchronization

4.1 Sync users

- If checked, users will be synchronized

4.2 Sync everyone

- If checked, all users will be synchronized

4.3 Sync existing

- If checked, existing users will be synchronized

4.4 Tolerance

- Choose the tolerance of synchronization (in hours)
- Minimum value is 1
- Maximum value is 24
- Required

4.5 Assign label

- Choose one of the available labels
- Available if checkbox Sync users is checked

4.6 Send notifications

- If checked, system will send notification to users about adding an account in the Proget system
- For this feature to work properly, SMTP must first be configured in the Settings tab
- Available if checkbox Sync users is checked

4.7 Send notifications about changes

- If checked, notifications about changes will be send
- For this feature to work properly, SMTP must first be configured in the Settings tab

- Available if checkbox Sync users is checked

4.8 Send activation to users

- If checked, activations will be send to selected below type of activation users
- For this feature to work properly, SMTP must first be configured in the Settings tab. If you want to send Android Enterprise, iOS or macOS activation proper configuration is required in the Integrations tab.
- Available if checkbox Sync users is checked

4.9 Actions on deleting a user

- If checked, actions on deleting a user will be performed
- Available if checkbox Sync users is checked

4.10 Activation selection

- Select activation type
- One of:
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - Android
 - iOS
 - macOS
 - Windows
- Available if checkboxes Sync users and Send activation to users are checked
- Required if checkbox Send activations to users is checked

4.11 Actions

- If checked, actions on deleting a user will be performed
 - Unassign devices
 - Remove user

- Wipe device
 - Wipe company data
 - Unassign labels
 - Lock user
- Available if checkboxes Sync users and Actions on deleting a user are checked
 - Required if checkbox Actions on deleting a user is checked

Microsoft Entra ID

Updated: Dec 3, 2024

Manage connection and synchronization with Microsoft Entra ID.

Users configurations

Settings

1

Users configurations

2

Settings

2.1 Microsoft Entra ID Application

- Choose one of the available application
- Available only Microsoft Entra ID applications with permissions assigned: Group.Read.All, User.Read.All
- Required

2.2 Filter

- Filter by:
 - All users
 - Group users
 - User attributes

2.3 Group ID

- This filter restricts the addition and synchronization of Microsoft Entra ID users to those who are members of a specific group. To filter users belonging to a particular Microsoft Entra ID group, enter the Group ID. Example: e15b8ad0-d4c1-11ed-b7a7-e8d8d1e95e11. You can find the Group ID by logging into <https://portal.azure.com>, then going to Microsoft Entra ID > Groups > choose group > Overview > Object ID. Click 'i' to go to Portal Microsoft Entra ID.

2.4 User attributes

- This filter allows you to limit Microsoft Entra ID users' addition and synchronization to those with specific attributes. Create a filter using supported user's attributes and operators. Example: department eq 'Marketing Department'. Click 'i' to go to the Microsoft documentation.

2.5 Sync users

- If checked, users are synchronized

2.6 Send notification to users about adding an account in the Proget system

- If checked, notifications are sent to users
- For this feature to work properly, SMTP must first be configured in the Settings tab

2.7 Assign label

- Choose one of the available labels

2.8 Send activation to users

- Choose activation type
- One of:
 - Android
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - iOS
 - macOS
 - Windows
- For this feature to work properly, SMTP must first be configured in the Settings tab. If you want to send Android Enterprise, iOS or macOS activation proper configuration is required in the Integrations tab.

2.9 Actions on deleting a user

- Choose the action to be performed after deleting the user
- One of:
 - Remove label and clear business data from devices
 - Remove label and wipe devices
 - Remove label

2.10 Send notifications about changes

- If checked, notifications about changes are sent

- For this feature to work properly, SMTP must first be configured in the Settings tab

3 Users mapping

3.1 Field in Proget Console

- Field in Proget console used for users mapping from Microsoft Entra ID

3.2 Field in Microsoft Entra ID

- Choose one of fields available in Microsoft Entra ID used for users mapping into Proget console
- Required

3.3 Remove

- Removes corresponding line with fields for users mapping
- Unlocked only for users mapping added by user

3.4 Add

- Adds new line with fields for users mapping

3.5 Map local users

- If checked, local users are mapped

Settings

Updated: Jun 3, 2026

Users configurations

Settings

☒ Enable sign-in with Microsoft Entra ID

Devices synchronization application: ⓘ

Select

During verification, you will be redirected to Microsoft Entra ID. To authorize your access ensure account you are using has Global Admin Rights. Otherwise, you will be able to send only a request to the Microsoft Entra ID administrator.

 Verify Proget application

1 Enable sign-in with Microsoft Entra ID

- If checked, you can sign-in to the Proget console with Microsoft Entra ID service

2 Devices synchronization application

- Select one of the available application
- Available only Microsoft Entra ID applications with permissions assigned: Device.ReadWrite.All

3 Verify Proget application

- Verify the selected Proget application on the Microsoft Entra ID portal. Make sure you have Global Admin Rights.

Roles

Updated: Jun 3, 2026

Roles allow you to configure administrative privileges, to view and manage content, for each of the console functions

Selected: 0 | Deselect all



Add

☐	NAME	LABELS
☐	Admin	admin
☐	User	user

Results: 2 | Page limit: 50

<<

<

1

>

>>

1 Copy

- This action allows you to copy the selected role from the list

2 Edit

- This action allows you to edit the selected role from the list

3 Delete

- This action allows you to remove selected roles from the list

4 Add

- By clicking this button, you will be taken to the steps of creating a new role

5 Roles list

- List of roles, that have been created and their assigned labels

Add Role

Updated: Jun 3, 2026

Add role

* Name:

Enable two-factor authentication: ☒

Allow multiple sessions: ☒

Inactivity time:

Labels: X

Back

Submit

1 Name

- Enter the name of the role
- Maximum length of the text is 32
- Required

2 Enable two-factor authentication

- Check the checkbox, if you want to enable two-factor authentication for logging in to the console

3 Allow multiple sessions

- Check the checkbox, if you want to allow multiple sessions at the same time

4 Inactivity time

- Set the inactivity time, after which the user will be logged out of the console
 - 15 minutes
 - 30 minutes
 - 45 minutes
 - 1 hour
 - 1 hour 15 minutes

- 1 hour 30 minutes
- 1 hour 45 minutes
- 2 hours

5 Labels

- Select a label, to associate with a role

6 Back

- This action allows you to return to the previous view, without saving the entered values

7 Submit / Role settings

7.1 Name

- Enter the name of the role
- Maximum length of the text is 32
- Required

7.2 Role configuration

- Here you can assign labels to role, for which the configuration has been created and manage its basic parameters

7.3 Roles management

- Here you can manage roles by specifying the user's access level to the Proget console functions. Each selected checkbox grants a greater permission

SMTP

Updated: Oct 9, 2025

Configure the SMTP service for sending activation messages and notifications to the user using email.

☐	Default configuration
☐	Basic authentication
☐	Modern authentication (Google)
☐	Modern authentication (Microsoft 365)

- 1 Default configuration
- 2 Basic authentication
- 3 Modern authentication (Google)
- 4 Modern authentication (Microsoft 365)

Default configuration

Updated: Oct 9, 2025

The default configuration configured by Proget allows sending an e-mail when creating a new user in the system and for resetting the password of a local user

 Default configuration

 The SMTP default configuration allows the local user's password to be reset and emails to be sent when the user is created.

1 Default configuration

- If enabled, the default SMTP configuration configured by Proget, will apply to the server

Basic authentication

Updated: Dec 3, 2024

SMTP Authentication, often abbreviated SMTP AUTH, is an extension of the Simple Mail Transfer Protocol (SMTP) whereby a client may log in using any authentication mechanism supported by the server.

Basic authentication

Displayed sender name:

Example

* Sender's email:

user@example.com

* SMTP server:

mail.example.com

* SMTP port:

123

User:

Example

Password:

.....

☐ Allow untrusted connections

Encryption type:

TLS

1

Sender informations

1.1 Displayed sender name

- Enter the name which will be visible in e-mails as a sender

1.2 Sender's email

- Enter the e-mail which will be visible in e-mails as a senders e-mail
- Maximum length of the text is 64
- Required

1.3 SMTP server

- Enter the SMTP server
- Maximum length of the text is 64
- Required

1.4 SMTP port

- Enter the SMTP port
- Number required
- Required

2 User credentials

2.1 User

- Enter the user e-mail from which e-mails will be send

2.2 Password

- If checked, change password will be available

2.3 Change password

- Enter the e-mail password from which e-mails will be send

3 Additional settings

3.1 Allow untrusted connections

- If checked, untrusted connections will be allowed

3.2 Encryption type

- Enter the type of encryption which will secure emails
- One of:
 - None
 - SSL
 - TLS

Modern authentication (Google)

Updated: Dec 3, 2024

SMTP Modern Authentication (Google) is an advanced method of authenticating SMTP clients using Google accounts, replacing traditional username and password authentication with more secure and flexible mechanisms such as OAuth 2.0, providing enhanced security and integration with Google's authentication infrastructure.

 Modern authentication (Google)

Displayed sender name:

* Sender's email:

 Sign in with Google

1 Displayed sender name

- Enter the name which will be visible in e-mails as a sender

2 Sender's email

- Sign in with your Google account from which the created emails will be send from the Proget console
- Required

Modern authentication (Microsoft 365)

Updated: Dec 3, 2024

SMTP Modern Authentication (Microsoft 365) is an enhanced method of authenticating SMTP clients using Microsoft 365 Active Directory (Microsoft Entra ID) credentials, allowing users to authenticate with Microsoft Entra ID tokens instead of traditional username and password, providing stronger security and integration with Microsoft Entra ID's advanced features.

 Modern authentication (Microsoft 365)

Displayed sender name:

* Sender's email:

 Microsoft 365

1 Displayed sender name

- Enter the name which will be visible in e-mails as a sender

2 Sender's email

- Sign in with your Microsoft 365 account from which the created emails will be send from the Proget console
- Required

Theme

Updated: Dec 3, 2024

Themes allow you to freely modify the graphic layout of the Proget console. The option allows, among other things, to insert your own logo and modify the colors throughout the console. This allows the system to be adapted to the needs of the company.

COLOR:

#5c1a51

Set default

LOGO: ⓘ



Select file

Set default

DARK THEME LOGO: ⓘ



Select file

Set default

FAVICON: ⓘ



Select file

Set default

Submit

1 Color

1.1 Color choice

- Choose the color of the Proget system

1.2 Set default

- Restores to default settings

2 Logo

2.1 Logo preview

- Shows the preview of chosen file

2.2 Select file

- Updates logo from the selected file

2.3 Set default

- Restores to default logo

3 Dark theme logo

3.1 Dark theme logo preview

- Shows the preview of chosen file

3.2 Select file

- Updates logo from the selected file

3.3 Set default

- Restores to default logo

4 Favicon

4.1 Favicon preview

- Shows the preview of chosen file

4.2 Select file

- Updates favicon from the selected file

4.3 Set default

- Restores to default favicon

Updates

Updated: Feb 12, 2025

Updates is a module that allows you to manage Proget server updates. You can be perform updates manually or you can set up automatic updates.

Setting up updates

UPDATE TYPE

☒ Manual

* Version:

Select version

▼

* Update at:

2025-01-01

☐ Automatic

Days:

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

☐ Sunday

Hour:

00:00

1

Manual

1.1 Manual

- If checked, set settings manually

1.2 Version

- Choose which version of console Proget will be used

1.3 Update at

- Choose at which date and time the update will happen

2 Automatic

2.1 Automatic

- If checked, set settings automatically

2.2 Days

- Choose at which day the update will happen if new version of Proget console is available

2.3 Hour

- Choose at which hour the update will happen if new version of Proget console is available

Scheduled update

1 Update now

- Updates the Proget console to the newest version
- Available if new version of Proget console is accessible

2 Submit

- Submits changes through adding configuration
- Available if adding new configuration

3 Delete

- Deletes the current configuration
- Available if configuration is saved

Integrations

Updated: Jul 16, 2026



Android Enterprise

Enhanced security, management, and app support for Android



Android zero-touch

Seamless zero-touch deployment for corporate Android devices



Apple Business Manager

Auto-activate Apple devices and enable supervisor mode remotely



Apple Push Notification Service

Enable the MDM protocol for remote management commands



Apps and Books

Bulk-purchase and distribute apps without an iTunes account



Microsoft Entra ID Applications

Bind Proget to Entra ID and import users



Samsung KME

Fast automated bulk enrollment via IMEI or serial number

Android Enterprise

Updated: Dec 3, 2024

Integration with Android Enterprise provide enhanced security, management and application support.

Android Enterprise Status: Configured	Organization ID: c273a2b6d2	Android Enterprise Email: pagan.dawson@gmail.com
--	--------------------------------	---

Remove configuration

DEVICE OWNER  Download QR code Show content	PROFILE OWNER ⓘ Available since Android 10  Download QR code Show content
--	--

☐ Automatically connect to the network ⓘ

SSID:

☐ Hidden network

Security type:

None

Password:

HOW TO ACTIVATE?

1

 Activate the device with a QR code by scanning chosen code.

2

 Launch of a QR code scanner is possible from the device setup start screen ("Welcome!" screen).

3

 Activate the QR code scanner with a few clicks on the welcome screen (any of empty space).

1 Remove configuration

- Removes Android Enterprise configuration

2 Download QR code

- Downloads QR code in .pdf format for Device Owner activation

3 Show content

- Displays the information contained in the QR code for Device Owner activation

4 Download QR code

- Downloads QR code in .pdf format for Profile Owner activation

5 Show content

- Displays the information contained in the QR code for Device Owner activation

6 Automatically connect to network

- Allows you to add Wi-Fi credentials to the QR code, in order to automatically connect to the Wi-Fi network during registration. The QR code will contain an unencrypted Wi-Fi password.

7 SSID

- Enter the name that identifies the wireless network.

8 Hidden network

- Required if the network for which we prepare configurations hides the SSID

9 Type of security

- One of:
 - None

- Personal WPA/WPA2
- If 'None' is chosen, the network will be without security
- If 'Personal WPA/WPA2' is chosen, user authentication manage is via WPA pre-shared key

10 Password

- If 'Personal WPA/WPA2' is chosen, enter the password to the wireless network.

11 How to activate?

- The following instruction will help you download Proget app on your Android mobile device in chosen mode.
- One way to activate your device is by scanning the QR code in chosen activation type, this action will download and install the Proget app (after scanning the QR code, you cannot change the activation type). To run the QR code scanner, the device must be restored to factory settings. Activating the QR code scanner is possible by clicking several times on the welcome screen (any empty place on the screen).
- To complete the activation of the device, scan the small QR code for the previously selected activation or add the device to automatic registration. A small QR code can be generated by clicking on the 'Generate Activation' button on the user card.

Android zero-touch

Updated: Dec 3, 2024

Android zero-touch enrollment offers a seamless deployment method for corporate-owned Android devices making large-scale rollouts fast, easy, and secure for organizations, IT, and employees. Zero-touch makes it simple to configure devices online and have them shipped with enforced management, so employees can open the box and get started. To activate the zero-touch device enrollment service in the Proget console, follow the instructions

About zero-touch enrollment

Simplifying zero-touch registration requires a few steps.

- ① Sign in to the zero-touch enrollment portal (<https://partnerdash.google.com/zerotouch>) and create a configuration profile.
- ② Fill in the required fields of the form.
 - Configuration name: <name of your configuration>
 - EMM DPC: Proget
 - DPC - additional information:

```
{
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
  }
}
```
 - Company name: <shown on the boot screen of the Android device in the help section>
 - Support email address: <shown on the boot screen of the Android device in the help section>
 - Support phone number: <shown on the Android device boot screen in the help section>
- ③ Set the created configuration as default.
- ④ Purchase an Android device from an authorized reseller who will add it to your zero-touch console ([Android Enterprise Solutions Directory - Resellers](#)).
- ⑤ Turn on your Android device and start setting it up. Zero-touch will force remote device management by Proget. Add the Device auto enrollment in the Proget console to further automate the device registration.

If you need help or want more details, please visit the [Technical Support](#) page for more resources.

Apple Business Manager

Updated: Feb 12, 2025

Program allows you to automatically activate Apple devices on the Proget server when you start up your device or factory reset. Program allows you also to define the stages of the first start up and remotely activate the supervisor mode.

Status: Connected	Expiration date: 2025-01-15
Renew the Proget server communication with the Apple Business Manager account Remove the account association Synchronize	

1 Renew the Proget server communication with the Apple Business Manager account

- This action allows to renews the Proget server communication with Apple Business Manager

2 Remove the account association

- This action removes the account association

3 Synchronize

- This action synchronizes the Proget server and the Apple Business Manager account
-

1 Go to the Apple portal

- This action redirects to the Apple portal where you can create an account

2 Download server public key

- This action allows you to download the server public key that will be used in the Apple console to generate token. This token will be required in step four.

3 Apple Business Manager server file (.p7m)

- This action allows you to upload the Apple Business Manager token downloaded from the Apple console in order to connect the Proget server and the Apple server

Apple Push Notification Service

Updated: Feb 12, 2025

Apple Push Notification service integration provides the ability to use the MDM protocol, which allows you to perform remote management commands.

Apple Push Notification service status: Apple Push Notification service certificate installed	Expiration date: 2025-01-15 10:57:22	Uid: com.apple.mgmt.External.c4753e35-7e47-4db7-86ce-20d916b2926b	Apple ID: No info
Renew certificate Remove integration Edit Apple ID			

1

Renew certificate

- This action renews certificate

2

Remove integration

- This action removes the integration

3

Edit Apple ID

- This action edits your Apple ID
-

1 Generate Apple Push Notification service certificate signing request

- This action generates and download Apple Push Notification service certificate signing request

2 Go to Apple Push Certificates Portal

- This action takes you to the Apple Push Certificate Portal

3 Import Apple Push Notification service certificate

- This action imports the Apple Push Notification service certificate file from your device

Apps and Books

Updated: Jun 3, 2026

Apps and Books Integration allows company and institutions to purchase apps and distribute them to employees. The program allows purchase free and payable apps in bulk. Assigning app license to device allows you to install app without iTunes account.

Name: Start typing...
Organization: Start typing...
Expiration date: Select date

Reset filters

Selected: 1
Deselect all

Add

NAME	ORGANIZATION	DATE OF ADDING	EXPIRATION DATE	LAST SYNC DATE
Example	Proget Sp. z o.o.	2024-08-27 13:04:25	2025-04-25 14:17:59	2024-08-27 13:04:38

Results: 1
Page limit: 50

<<

<

1

>

>>

1 Show details

- This action allows you to check the details of the added Apps and Books integrations, such as:
 - What apps are added to the list
 - The usage status of the license
 - The license availability for application

2 Edit

- This action allows you to edit data of the added Apps and Books integration, such as:
 - Create new name of licences
 - Add new token of Apps and Books

3 Synchronize licenses

- This action allows you to synchronize the up-the-date information about licenses

4 Delete

- This action allows you to delete the Apps and Books integration

5 Add

- This action allows you to add new Apps and Books integration
-

2 Add a Apps and Books integration

2.1 Name

- Example name of the added integration
- Required

2.2 Apps and Books token

- Enter generated token of Apps and Books
- How to get token:
 - Log in to a Volume Purchase Program account (<https://business.apple.com>)
 - Log in to your account
 - Generate a token and then upload it to the MDM system
- Required

2.3 Add

- This action allows you to add downloaded token from your device

2.4 Add macOS applications

- If selected, iOS apps available on macOS (Apple Silicon) will also be added to the console as macOS apps
-

3 Details of the Apps and Books account

3.1 Show license usage

- This action allows you to check the usage of licenses
- Then you know:
 - What device is using the license
 - What user is using the license

3.2 Back

- This action allows you to return to the previous view

3.3 List of the integrations

- List of the Apps and Books integrations

Microsoft Entra ID Applications

Updated: Jun 3, 2026

Integration with Microsoft Entra ID allows to bind Proget to your Microsoft Entra ID. Thanks to this, it will be available to add new connections enabling the import of users to the Proget console.

Selected: 1 | Deselect all

Add

☒	NAME	CLIENT ID	TENANT ID	DATE ADDED	CLIENT SECRET EXPIRATION DATE
> ☒	Example name	00000000-0000-0000-0000-000000000000	00000000-0000-0000-0000-000000000000	2024-10-22 08:09:44	-

Results: 1 | Page limit: 50

<<

<

1

>

>>

1 Edit

- This action allows you to edit selected integration

2 Synchronize

- This action allows you to synchronize selected integration

3 Remove

- This action allows you to remove selected integration

4 Add Microsoft Entra ID Integration

4.1 Name

- Maximum length of the text is 255
- Required

4.2 Client ID

- The client ID is the unique Application (client) ID assigned to your app by Microsoft Entra ID when the app was registered.
- Required

4.3 Client Secret

- A client secret is an authentication technique that uses a string value in the Microsoft Entra ID application instead of a certificate for identity.
- Required

4.4 Tenant ID

- A Tenant ID (tenant identifier) is a unique identifier or alias for the tenant and is based on the tenant name. The tenant ID is assigned to the tenant's resources (such as envelopes, maps, and outbound documents).
- Required

4.5 Client Secret expiration date

- Select the date when the client secret should expire

Samsung KME

Updated: Jun 3, 2026

Knox Mobile Enrollment is the quickest and most automated way to enroll a large number of devices. Once an IT admin registers a device with the service (using IMEI or Serial Number), the device's user initiates the MDM registration process during the initial device configuration process.

* Customer ID:

00000000

* Region:

EU

Knox custom JSON:

1 Customer ID

- Enter customer ID
- Maximum length of the text is 255
- Required

2 Region

- Select region
- One of
 - EU
 - US
- Required

3 Knox custom JSON

- Enter Custom JSON Data

File Manager

Updated: Jun 3, 2026



The module allows you to manage files on iOS and Android devices. It requires the File Manager application to be installed and configured. The available storage space for uploaded and downloaded files is limited – once it is exceeded, further file operations will not be possible. To restore the ability to manage files, selected items must be removed from the table.

14%

Total capacity: 2.00 GiB (2.15 GB) Remaining capacity: 1.72 GiB (1.85 GB)

Files

Path: Start typing...

Vendor: Insert text here...

Model: Insert text here...

+

Reset filtersBASICPQL

Selected: 0Deselect all

	NAME	DIRECTORY	SIZE	USER	VENDOR	CREATION DATE	CREATED BY
☐	Gmail_2024.07.14.65324615...	/Directory	141.09 MiB ...	Example User	XIAOMI	2026-05-22 10:03:08	Example User
☐	Microsoft OneDrive_7.29_AP...	/Directory	99.29 MiB ...	Example User	XIAOMI	2026-05-22 10:02:50	Example User
☐	Android Auto_12.3.642634-r...	/Directory	43.19 MiB ...	Example User	XIAOMI	2026-05-22 10:00:07	Example User

1 Disk percentage full

- Displays the current storage usage as a progress bar with the percentage of used space, total capacity and remaining capacity

2 Filters

- The file filter allows you to search for available files using basic filters such as:
 - Path
 - Vendor
 - Model
 - Use the '+' button to add additional filter criteria

3 Download

- This action allows you to download the selected files from the list to your computer
- Select one or more files from the list to enable this action

4 Delete

- This action allows you to delete the selected files from the File Manager storage, freeing up disk space
- Select one or more files from the list to enable this action

5 List of uploaded files

- Displays all files uploaded from devices to the File Manager storage, including file name, directory, size, user, device vendor, creation date, and the user who created the entry

Changelog

Updated: Jul 6, 2026

× 2.20.4

2026-07-06

- Fixed reinstalling an app in Proget Store

× 2.20.3

2026-06-29

- Fixed the Apple app update using an action

× 2.20.2

2026-06-26

- Changed maximum number of characters for the 'Send message' action

× 2.20.1

2026-06-24

- Optimizations and other improvements

× 2.20.0

2026-06-16

- Added File Manager functionality - remote file management on Android and iOS devices
- Added Proget Notifier app support
- Added dependency graph (label view, user card, device card)
- Added 'Allowed SIM cards' tab
- Added PQL keys: device.SIM1, device.SIM2
- Added PQL reference: ALLOWED_SIM_CARDS
- Added SCEP type in Certificate profile
- Added uploading certificate from file to Windows devices
- Added new 'No Internet' action in MTP profile

- Added optional phone number and custom header in 'Lock work profile' reaction in MTP profile
- Added system error report generation on Android devices
- Added bulk editing of app settings in group
- Added macOS apps in Apps and Books integration
- Added remote account removal from device in 'User accounts' tab
- Added 'Remove Android Enterprise account' action in Devices tab
- Added AE integration removal when no active accounts exist on Android Enterprise devices
- Added text formatting and clickable links in messages to device
- Added pending actions column on lists
- Added fixed row height in tables
- Added Kiosk exit configuration options
- Added Kiosk PIN configuration options
- Added Proget settings in single app mode in Kiosk
- Added Kiosk position configuration relative to lock screen
- Added automatic logout time configuration in Kiosk
- Added new intent types in Kiosk: user logout, direct kiosk exit
- Changed service password for Android devices - mechanism expansion
- Changed custom attributes behaviour regarding Entra ID synchronization
- Marked SCEP profile as deprecated
- Marked 'Service password' policy as deprecated
- Marked 'Allow clearing of application data' policy as deprecated
- Marked security codes for Android devices in Service as deprecated
- Fixed displaying Wi-Fi MAC address in Devices tab

+ 2.19.12

2026-04-20

+ 2.19.11

2026-04-13

[+ 2.19.10](#)

2026-03-31

[+ 2.19.9](#)

2026-03-25

[+ 2.19.8](#)

2026-03-10

[+ 2.19.7](#)

2026-02-23

[+ 2.19.6](#)

2026-02-10

[+ 2.19.5](#)

2026-02-09

[+ 2.19.4](#)

2026-02-04

[+ 2.19.3](#)

2026-01-19

[+ 2.19.2](#)

2026-01-14

[+ 2.19.1](#)

2026-01-12

[+ 2.19.0](#)

2026-01-07

[+ 2.18.5](#)

2025-10-08

[+ 2.18.4](#)

2025-09-17

[+ 2.18.3](#)

2025-08-25

[+ 2.18.2](#)

2025-07-22

[+ 2.18.1](#)

2025-07-14

[+ 2.18.0](#)

2025-07-09

[+ 2.17.10](#)

2025-05-20

[+ 2.17.9](#)

2025-05-14

[+ 2.17.8](#)

2025-04-29

[+ 2.17.7](#)

2025-04-16

[+ 2.17.6](#)

2025-04-02

[+ 2.17.5](#)

2025-03-25

[+ 2.17.4](#)

2025-03-19

[+ 2.17.3](#)

2025-03-10

[+ 2.17.2](#)

2025-03-05

[+ 2.17.1](#)

2025-02-26

[+ 2.17.0](#)

2025-02-19

+ 2.16.4	2025-02-03
+ 2.16.3	2025-01-15
+ 2.16.2	2024-10-19
+ 2.16.1	2024-10-13
+ 2.16.0	2024-10-15
+ 2.15.10	2024-09-03
+ 2.15.9	2024-08-19
+ 2.15.8	2024-07-23
+ 2.15.7	2024-07-17
+ 2.15.6	2024-07-16
+ 2.15.5	2024-07-01
+ 2.15.4	2024-06-25
+ 2.15.3	2024-06-05
+ 2.15.2	2024-05-27

[+ 2.15.1](#)

2024-05-13

[+ 2.15.0](#)

2024-05-08

[+ 2.14.6](#)

2024-03-18

[+ 2.14.5](#)

2024-03-14

[+ 2.14.4](#)

2024-03-13

[+ 2.14.3](#)

2024-02-27

[+ 2.14.2](#)

2024-01-31

[+ 2.14.1](#)

2024-01-25

[+ 2.14.0](#)

2024-01-22

[+ 2.13.4](#)

2023-11-21

[+ 2.13.3](#)

2023-10-24

[+ 2.13.2](#)

2023-09-07

[+ 2.13.1](#)

2023-09-06

[+ 2.13.0](#)

2023-09-04

[+ 2.12.3](#)

2023-07-12

[+ 2.12.2](#)

2023-06-20

[+ 2.12.1](#)

2023-06-13

[+ 2.12.0](#)

2023-06-12

[+ 2.11.3](#)

2023-03-22

[+ 2.11.2](#)

2023-03-08

[+ 2.11.1](#)

2023-02-27

[+ 2.11.0](#)

2023-02-08

[+ 2.10.3](#)

2023-01-11

[+ 2.10.2](#)

2022-12-29

[+ 2.10.1](#)

2022-12-01

[+ 2.10.0](#)

2022-10-25

[+ 2.9.11](#)

2022-09-12

[+ 2.9.10](#)

2022-09-05

[+ 2.9.9](#)

2022-09-01

[+ 2.9.8](#)

2022-08-29

[+ 2.9.7](#)

2022-08-24

[+ 2.9.6](#)

2022-07-26

[+ 2.9.5](#)

2022-07-05

[+ 2.9.4](#)

2022-06-29

[+ 2.9.3](#)

2022-06-22

[+ 2.9.2](#)

2022-06-01

[+ 2.9.1](#)

2022-05-18

[+ 2.9.0](#)

2022-05-16

[+ 2.8.14](#)

2022-04-25

[+ 2.8.13](#)

2022-04-25

[+ 2.8.12](#)

2022-04-21

[+ 2.8.11](#)

2022-04-07

[+ 2.8.10](#)

2022-02-15

[+ 2.8.9](#)

2022-01-25

[+ 2.8.8](#)

2022-01-13

[+ 2.8.7](#)

2021-12-15

[+ 2.8.6](#)

2021-12-13

[+ 2.8.5](#)

2021-12-01

[+ 2.8.4](#)

2021-11-29

[+ 2.8.3](#)

2021-10-14

[+ 2.8.2](#)

2021-10-13

[+ 2.8.1](#)

2021-09-28

[+ 2.8.0](#)

2021-09-21

[+ 2.7.3](#)

2021-07-07

[+ 2.7.2](#)

2021-06-29

[+ 2.7.1](#)

2021-06-24

[+ 2.7.0](#)

2021-06-22

[+ 2.6.2](#)

2021-05-27

[+ 2.6.1](#)

2021-05-13

[+ 2.6.0](#)

2021-04-19

[+ 2.5.3](#)

2021-03-31

[+ 2.5.2](#)

2021-03-09

[+ 2.5.1](#)

2021-03-01

[+ 2.5.0](#)

2021-02-24

[+ 2.4.9](#)

2021-02-02

[+ 2.4.8](#)

2021-01-26

[+ 2.4.7](#)

2021-01-19

[+ 2.4.6](#)

2020-12-14

[+ 2.4.5](#)

2020-12-04

[+ 2.4.4](#)

2020-11-30

[+ 2.4.3](#)

2020-11-24

[+ 2.4.2](#)

2020-11-03

[+ 2.4.1](#)

2020-10-30

[+ 2.4.0](#)

2020-10-26

[+ 2.3.5](#)

2020-07-13

[+ 2.3.4](#)

2020-07-07

[+ 2.3.3](#)

2020-07-02

[+ 2.3.2](#)

2020-06-30

[+ 2.3.1](#)

2020-06-26

[+ 2.3.0](#)

2020-06-25

Known Issues

Updated: Jan 28, 2025

+ **Samsung E-Mail application**

+ **Problem with running Remote Desktop**

+ **The Apple Business Manager page is not available**

+ **The device does not disappear from the user card**

+ **Duplicate occurrence after restoring contacts on Google Pixel (Device Owner)**

+ **Problem with synchronization on Windows activation**

+ **Password policy on Windows activation**

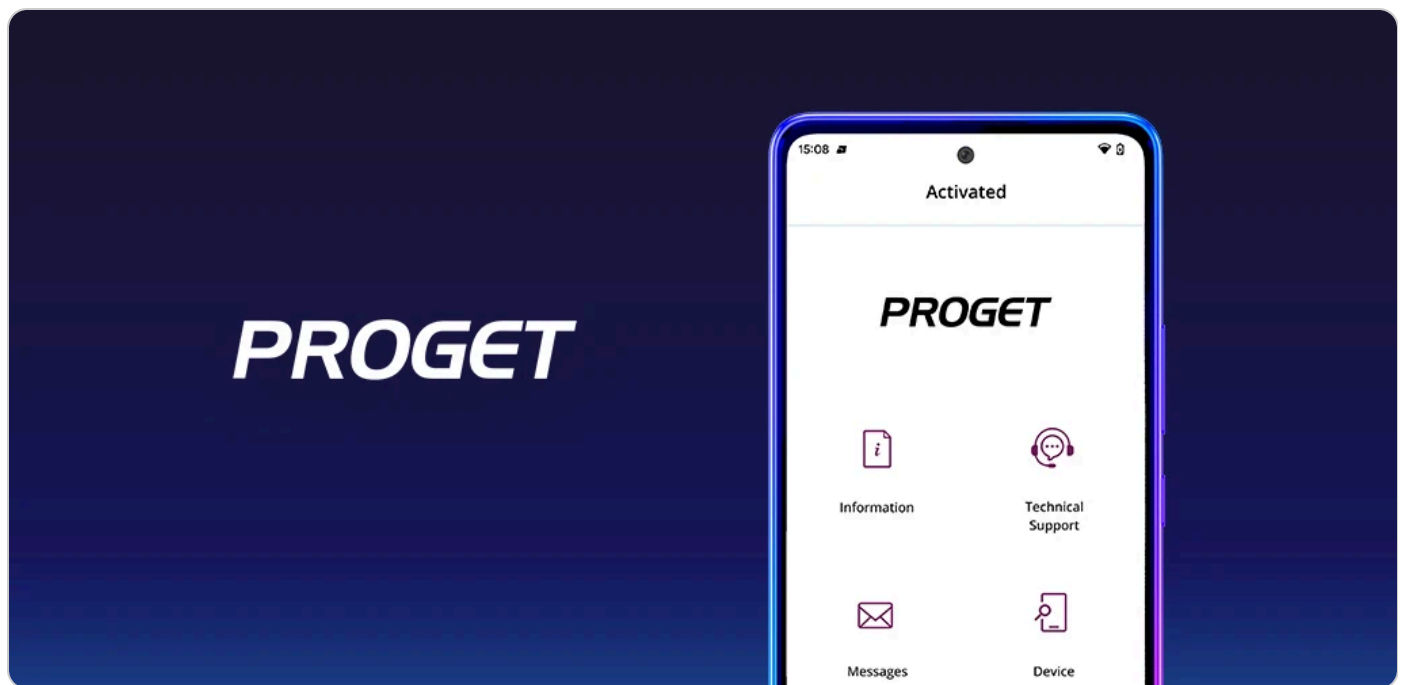
+ **Profile Wallpaper on iOS activation**

+ **Notifications on Pixel devices with Do not disturb mode on**

Proget Mobile App

Updated: Mar 4, 2025

Proget is a solution enabling management and administration of mobile devices in the company. Proget protect corporate and private data: e-mail, calendar, notes and files thanks to the function of performing and restoring a backup of contacts, sms/mms and call logs. The solution also secure mobile data transmission using the highest encryption standards, creating a secure tunnel between the smartphone and internal company resources. Proget allows you to implement devices in many models: BYOD, COPE or devices fully managed by the company.



Changelog



Known Issues

Changelog

Updated: Jun 22, 2026

× 2.20.3

2026-06-22

- Fixed SMS permissions for COPE activation

× 2.20.2

2026-06-12

- Fixed notifying about SIM card changes on the device
- Fixed the password setting on the Lost Mode screen
- Fixed the behaviour of automatic time zone, date and time policies after restarting the device
- Other fixes and improvements

× 2.20.1

2026-05-18

- Other fixes and improvements

× 2.20.0

2026-05-12

- Wi-Fi settings in the Kiosk profile have been improved
- Fixed connecting to a WPA3 Wi-Fi network in the Kiosk profile settings
- Fixed displaying notification of data usage access

+ 2.19.8

2026-04-21

+ 2.19.7

2026-03-26

+ 2.19.6

2026-03-25

+ 2.19.5

2026-03-02

+ 2.19.4

2026-02-03

+ 2.19.3

2026-01-19

+ 2.19.2

2026-01-12

+ 2.19.1

2025-12-02

+ 2.19.0

2025-11-27

+ 2.18.8

2025-10-20

+ 2.18.7

2025-09-10

+ 2.18.6

2025-08-19

+ 2.18.5

2025-08-14

+ 2.18.4

2025-08-06

+ 2.18.3

2025-07-29

+ 2.18.2

2025-07-16

+ 2.18.1	2025-07-15
+ 2.18.0	2025-06-30
+ 2.17.7	2025-05-20
+ 2.17.6	2025-04-14
+ 2.17.5	2025-04-06
+ 2.17.4	2025-04-02
+ 2.17.3	2025-03-24
+ 2.17.2	2025-02-27
+ 2.17.1	2025-02-21
+ 2.17.0	2025-02-10
+ 2.16.4	2025-01-27
+ 2.16.3	2025-01-08
+ 2.16.2	2024-12-10
+ 2.16.1	2024-11-28

+ 2.16.0

2024-10-14

+ 2.15.12

2024-09-02

+ 2.15.11

2024-08-08

+ 2.15.10

2024-08-07

+ 2.15.9

2024-07-30

+ 2.15.8

2024-07-03

+ 2.15.7

2024-06-25

+ 2.15.6

2024-06-14

+ 2.15.5

2024-06-13

+ 2.15.4

2024-05-20

+ 2.15.3

2024-05-06

+ 2.15.2

2024-05-02

+ 2.15.1

2024-04-26

+ 2.15.0

2024-04-25

[+ 2.14.3](#)

2024-03-27

[+ 2.14.2](#)

2024-03-12

[+ 2.14.1](#)

2024-01-25

[+ 2.14.0](#)

2024-01-15

[+ 2.13.5](#)

2023-11-28

[+ 2.13.4](#)

2023-11-07

[+ 2.13.3](#)

2023-10-17

[+ 2.13.2](#)

2023-09-04

[+ 2.13.1](#)

2023-08-25

[+ 2.13.0](#)

2023-08-23

[+ 2.12.0](#)

2023-06-05

[+ 2.11.1](#)

2023-02-28

[+ 2.11.0](#)

2023-02-20

[+ 2.10.3](#)

2022-11-25

[+ 2.10.2](#)

2022-10-27

[+ 2.10.1](#)

2022-10-26

[+ 2.10.0](#)

2022-10-25

[+ 2.9.3](#)

2022-07-07

[+ 2.9.2](#)

2022-06-22

[+ 2.9.1](#)

2022-05-27

[+ 2.9.0](#)

2022-05-16

[+ 2.8.10](#)

2022-02-24

[+ 2.8.9](#)

2022-01-20

[+ 2.8.8](#)

2022-01-19

[+ 2.8.7](#)

2022-01-03

[+ 2.8.6](#)

2021-12-02

[+ 2.8.5](#)

2021-11-30

[+ 2.8.4](#)

2021-11-08

[+ 2.8.3](#)

2021-11-03

[+ 2.8.2](#)

2021-10-13

[+ 2.8.1](#)

2021-10-04

[+ 2.8.0](#)

2021-09-21

[+ 2.7.6](#)

2021-09-01

[+ 2.7.5](#)

2021-07-11

[+ 2.7.4](#)

2021-07-07

[+ 2.7.3](#)

2021-07-06

[+ 2.7.2](#)

2021-06-24

[+ 2.7.1](#)

2021-06-22

[+ 2.7.0](#)

2021-06-22

[+ 2.6.4](#)

2021-05-12

[+ 2.6.3](#)

2021-05-07

[+ 2.6.2](#)

2021-04-27

[+ 2.6.1](#)

2021-04-21

[+ 2.6.0](#)

2021-04-19

[+ 2.5.4](#)

2021-03-16

[+ 2.5.3](#)

2021-03-04

[+ 2.5.2](#)

2021-03-03

[+ 2.5.1](#)

2021-03-01

[+ 2.5.0](#)

2021-02-19

[+ 2.4.11](#)

2021-01-25

[+ 2.4.10](#)

2021-01-11

[+ 2.4.9](#)

2021-01-04

[+ 2.4.8](#)

2020-12-29

[+ 2.4.7](#)

2020-12-21

[+ 2.4.6](#)

2020-12-09

[+ 2.4.5](#)

2020-11-27

[+ 2.4.4](#)

2020-11-26

[+ 2.4.3](#)

2020-11-25

[+ 2.4.2](#)

2020-11-20

[+ 2.4.1](#)

2020-10-30

[+ 2.4.0](#)

2020-10-26

[+ 2.3.6](#)

2020-08-21

[+ 2.3.5](#)

2020-08-11

[+ 2.3.4](#)

2020-07-03

[+ 2.3.3](#)

2020-06-30

[+ 2.3.2](#)

2020-06-26

[+ 2.3.1](#)

2020-06-25

[+ 2.3.0](#)

2020-06-25

Known issues

Updated: Jan 28, 2025

- + **Android Enterprise Device Owner – Allows add Wi-Fi connections policy**
- + **Android Enterprise Device Owner – installing application from file for Xiaomi devices**
- + **Android Enterprise Profile Owner – self-changing passwords on Huawei devices with Android 8 or 8.1**
- + **Android Enterprise – Device Owner on Nokia devices with android 8**
- + **Running applications on HUAWEI devices**
- + **Can't choose the Proget application when restoring SMS / MMS messages in the activation of the Android Profile Owner**
- + **Android Enterprise Profile Owner – it is currently not possible to restore contacts from a backup on Huawei devices**
- + **POP/IMAP profile not working with GMAIL**
- + **Xiaomi – unable to install application from file**
- + **HUAWEI EML-L29 Android 10 – No automatic registration using Enterprise QR**
- + **Xiaomi – MIUI interface**
- + **Contact with administrator and emergency call on devices without SIM card**

+ Action Turn off Wifi on MTP Profile

+ Taking photos during Lost Mode on weaker Android devices

+ Allowed Input methods policy on DO and PO activation

+ Set timezone automatically – DO policy on Samsung devices

+ Prohibit removing added Wi-Fi networks – DO policy on Samsung devices

+ Profile Owner activation via QR from Integration tab

+ Proget Backup – MMS restoring

+ DO activation via Enterprise QR on Android 10

Proget Notifier App

Updated: Jul 16, 2026

NEW

Proget Notifier app is a fully configurable communication layer between the Proget management console and the device user. With our application you can display configurable screens with messages, images, and interactive buttons on the device. The app supports actions such as sending data to an external endpoint, opening the phone dialer, or exiting the application. All content including texts, images, and buttons is configurable per language and managed remotely via the Proget management console. The app can also work in Kiosk mode as a single application, and provides access to Wi-Fi settings directly from its interface. This app is an integral part of the Proget solution. We recommend using it only in an environment managed by the Proget system.



[Changelog](#)

Changelog

Updated: Jun 8, 2026

× 1.0.0	2026-05-28
First release	

Proget File Manager App

Updated: Jul 16, 2026

NEW

Proget File Manager app enables secure file transfer between mobile devices and the Proget management console. With our application you can upload files from the device to the console and manage them remotely. The available storage space is limited once it is exceeded, further file operations will not be possible until selected items are removed. This app is an integral part of the Proget solution. We recommend using it only in an environment managed by the Proget system. The app can be configured manually or remotely using the Proget management console.

PROGET
FILE MANAGER



Changelog

Changelog

Updated: Jul 16, 2026

× 0.1.1	2026-07-15
Other fixes and improvements	
× 0.1.0	2026-06-29
First release	

Proget Remote App

Updated: Mar 4, 2025

Proget Remote is an application that allows you to remotely access the screen of your Android device from the Proget server. No matter where you are at the moment, by establishing a secure connection: get quick help from your administrator, repair or troubleshoot your device, share your screen and hand over control.



Changelog

Changelog

Updated: Mar 26, 2025

× **3.1.1**

2024-07-15

- Connection stability has been improved

× **3.1.0**

2024-01-18

- Changed app UI
- Added support for using the keyboard during a Proget Remote connection
- Added support for rotation during a Proget Remote connection

+ **3.0.1**

2023-11-07

+ **3.0.0**

2023-05-08

+ **2.4.4**

2022-02-07

+ **2.4.3**

2022-01-19

+ **2.4.2**

2021-10-21

+ **2.4.1**

2021-03-19

+ **2.4.0**

2021-03-18

+ **2.3.0**

2020-10-08

+ 2.2.0

2020-06-02

+ 2.0.0

2019-05-05

Proget Geofencing App

Updated: Mar 4, 2025

Proget Geofencing is an application that allows to manage your mobile device based on preconfigured business zones. Thanks to it, Proget system admins have ability to provide you various functionalities and restrictions on your mobile device. The application does not work alone. To proper operation of Proget Geofencing you have to use Proget application which is connected to the server. It also require delivered configuration of the Geofencing profile. All configurations and restrictions are fully configured by the administrator of Proget system.



Changelog

Changelog

Updated: Mar 26, 2025

×	1.4.1	2024-07-23
	• Changed app UI • Fixed link to terms of use	
×	1.4.0	2023-06-12
	• Changed app UI • Bug fixes and other improvements	
+	1.3.1	2021-03-26
+	1.3.0	2021-03-18
+	1.2.0	2020-10-09
+	1.1.0	2020-06-25
+	1.0.0	2019-12-04

Proget Backup App

Updated: Mar 4, 2025

Proget Backup is part of Proget system. It can run in local (dedicated for personal use only) and remote mode (dedicated for enterprises). User can create backup of contacts, SMS, MMS, call logs and then restore it when needed. Backup data is securely stored in application dedicated storage. Can not be moved to other device. To use remote mode application require Proget app to be enrolled on Proget server. Proget Backup application allows Proget system administrator to create and restore backup of contacts, SMS, MMS and call log. All data is downloaded and securely stored on the Proget server managed by the administrator in your company.



[Changelog](#)

Changelog

Updated: Dec 16, 2025

× 1.6.3

2025-12-15

- Fixed scheduled backup make after app restart

× 1.6.2

2025-09-29

- Fixed setting Proget Backup as the default SMS application

× 1.6.1

2024-08-27

- Bug fixes and other improvements

× 1.6.0

2024-05-06

- Added the ability to send a backup copy to the server without registering the device in the Proget console

+ 1.5.0

2023-10-03

+ 1.4.3

2022-06-28

+ 1.4.2

2022-04-11

+ 1.4.1

2021-04-09

+ 1.4.0

2020-10-09

+ 1.3.0

2020-09-25

+ 1.2.0

2020-06-25

+ 1.1.0

2020-02-28

+ 1.0.0

2020-01-15

Proget File Sharing App

Updated: Mar 4, 2025

Proget File Sharing app secures access to corporate resources via FTP and SMB. With our application you can access your work resources via FTP and SMB. Get secure access to corporate data and work on it in accordance with the rules applicable in your organization. This app is integral part of the Proget solution. We recommend using it only in an environment managed by the Proget system. The app can be configured manually or remotely using the Proget management console.



[Changelog](#)

Changelog

Updated: Mar 26, 2025

×	1.5.1	2024-08-28
	Bug fixes and other improvements	
+	1.5.0	2024-04-16
×	1.4.0	2023-07-05
	- Changed app UI - Bug fixes and other improvements	
+	1.3.0	2021-12-13
+	1.2.3	2021-09-23
+	1.2.2	2021-08-31
+	1.2.1	2021-05-12
+	1.2.0	2021-05-07
+	1.1.1	2021-04-02
+	1.1.0	2021-03-31

+ 1.0.2

2021-03-18

+ 1.0.1

2021-03-15

+ 1.0.0

2021-03-05

Proget OpenVPN App

Updated: Mar 4, 2025

Proget OpenVPN is an OpenVPN client app that allows you to establish a secure access to a confidential data behind the firewall. The app supports the import of the ovpn profile and the managed configuration sent by the EMM server. To be able to fully use the solution, it is required to bind the application with an EMM server installed inside the company or in the cloud.

PROGET
OPENVPN



Changelog

Changelog

Updated: Mar 26, 2025

×	1.3.1	2024-01-17
	Updated app UI	
×	1.3.0	2024-01-16
	Changed app UI	
+	1.2.0	2023-06-29
+	1.1.2	2022-07-21
+	1.1.1	2022-07-15
+	1.1.0	2022-07-12
+	1.0.0	2022-01-21

FAQ

Updated: Jul 16, 2026

What is MDM? (Mobile Device Management)

MDM – Mobile Device Management – is a device lifecycle management technology that enables the IT team to implement, configure, manage, service and secure mobile devices through MDM profiles installed on devices. The MDM software provides a set of resources, remote configuration of e-mail, applications and Wi-Fi, remote problem solving and the ability to remotely lock and wipe to secure the device and company data stored on it. MDM is the basis of a comprehensive enterprise mobility management solution.

What is MAM? (Mobile Application Management)

MAM technologies – Management of Mobile Applications – apply management and policy controls to individual applications instead of to the entire device. MAM solutions usually offer a custom application store that allows you to control and deliver applications developed internally as well as third-party applications. IT administrators can add security, encryption and control to mobile applications by using the AppConfig Community standards or the Software Development Kit or App Wrapping solutions from the MAM provider.

What is EMM? (Enterprise Mobility Management)

EMM – Enterprise Mobility Management – is a device and platform independent solution that centralises the management, configuration and security of all devices in the organization, both those used in the BYOD model and the company model. EMM goes beyond traditional device management and includes management and configuration of the application and company content. The comprehensive EMM solution includes MDM, MAM, MCM (Mobile Content Management), identity management for access control and productivity applications to facilitate access to corporate e-mail, calendar, contacts, content repositories and intranet sites. A well-chosen EMM solution should provide both technical capabilities to simplify management as well as security for the IT team, as well as pleasant use for the employee.

What is UEM? (Unified Endpoint Management)

UEM – Unified Endpoint Management – allows the IT team to stop using separate tools for managing mobile, traditional and IoT devices. UEM solutions provide a comprehensive and user-

centric approach to managing all endpoints by combining traditional client management with desktop and PC using a modern Enterprise Mobility Management (EMM) platform. A comprehensive UEM solution enables the IT team to manage users and provide consistent experience at all endpoints, secure and manage the entire device lifecycle and make all of it using one comprehensive platform.

What is BYOD? (Bring Your Own Device)

BYOD – Bring Your Own Device – is a principle in the IT industry that allows employees to use their own devices for business purposes. EMM platforms allow organizations to implement BYOD strategies without compromising employee safety and privacy at the risk of separating company and personal data on the device. This separation allows the IT team to manage and secure only business data on the device owned by the employee. If the device is ever endangered or when the employee leaves the company, the IT team has the option of removing only work-related data and leaving personal items on the device intact.

Post profiles with which applications work?

The **Active Sync** or **IMAP / POP** mail profiles that are used in the Samsung Knox activation will require the Samsung Mail application. If we want to set up a mail profile on Android Enterprise Profile Owner or Android Enterprise Device Owner activation, we can do it via [application configuration](#).

What is supervisor – iOS?

Apple's supervised iOS mode provides administrators with more options when managing Apple devices, which is useful for large-scale company-owned devices. For example, you can restrict the AirDrop function, prevent users from changing the device name, or apply application rules. To add a device in supervised mode, Apple Business Manager profiles must be configured or used [Apple Configurator](#). In iOS 11 support for Apple Business Manager devices that are not supervised was deprecated. In iOS 11 and later, Apple Business Manager configured devices should always be supervised. And in a future release, the OS will ignore the Apple Business Manager is_supervised flag completely.

Where the application from the list of applications comes from?

After the device is activated, applications from the device are automatically added to the system. The user also has the option [adding an application](#).

How to get and use Apple Business Manager?

The **Device Enrollment Program** can be obtained through resellers. A list of resellers can be found on [this site](#).

Detailed information on how to use Apple Business Manager can be found on [this website](#).

What operating systems of mobile devices do we support?

Provides support for Android 8.0 and newer, iOS 10.3 and newer, and for Windows 10.

What ports on the network must be unlocked for the remote desktop to work?

443/TCP, 2222/TCP, 2222/UDP, 30000-59999/UDP – on the device and desktop side.