PORSCHE

Porsche Korea IT Quick Start

Seoul, South Korea

2022

Porsche Korea IT Quick Start

1.1 Bitlocker / Windows Login

- Bitlocker

The hard disk of all PKO devices are encrypted with BitLocker. You have to enter BitLocker PIN before booting your devices. The PIN will be provided by IT.

After 4 times of failed attempts, you must enter BitLock recovery key which is maintained by PKO IT.
Please contact IT helpdesk to get the key.

- Windows Login data:
  User: **firstname.lastname**
  Password: **see PKO IT Initial Password document provided on first day**
  Password Rules: minimum 12 characters,
  Contain characters from **three** of the following four categories:
  English uppercase characters (A through Z)
  English lowercase characters (a through z)
  Base 10 digits (0 through 9)
  Non-alphabetic characters (for example, !, $, #, %)

You will then be asked to change your password.

If you are **not** requested to change your password, please wait until Windows started completely and press the following keys at the same time:

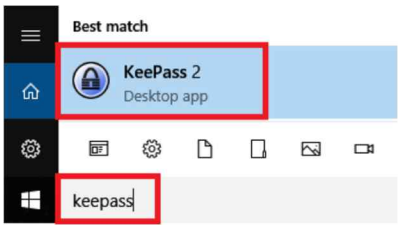
CTRL+ALT+DEL

You will then see a screen where you can click 'Change a Password…' and afterwards a screen to change your password.
If you have trouble to change your password, please contact us the IT help desk (see Chapter 0).

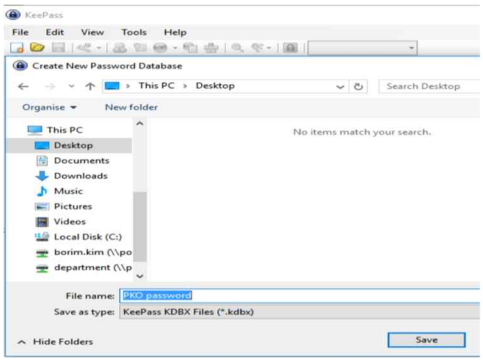
- Password Management (KeePass)

  Passwords can be stored in an encrypted database, which can be unlocked with one master key.

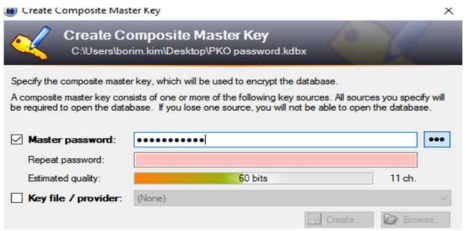
1. Run "KeePass 2" application on your laptop or desktop.



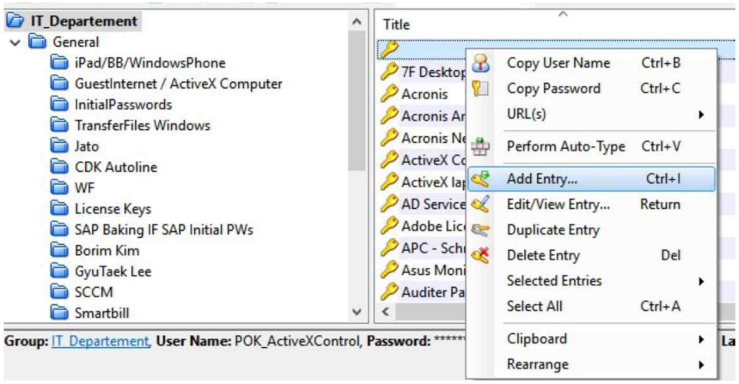
2. Create your own Key file and save it on local drive (C) or H drive.



3. Set the master password.



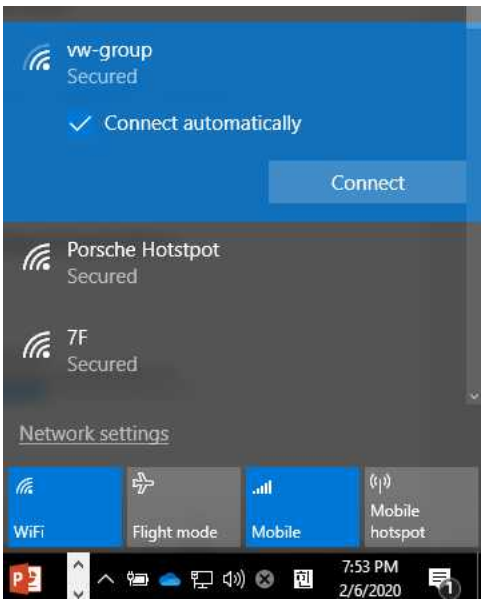
4. Add the system passwords by selecting "Add Entry"



1.2 Porsche Network / Wifi

To access to Porsche network, a wired LAN cable has to be connected to laptop or desktop.
The main cable is connected to desk phone and additional cable is connected from phone to laptop.

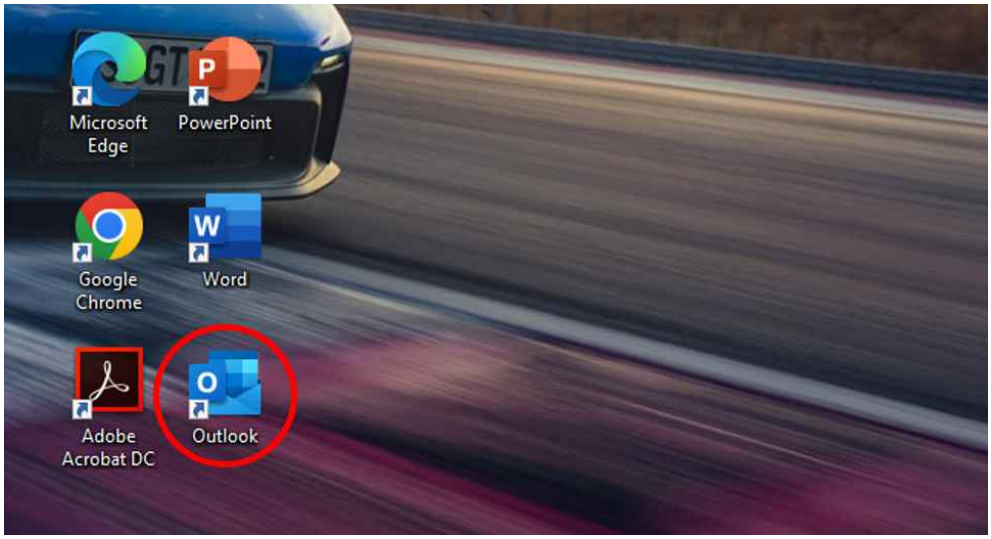
Corporate Wifi connection is available. Choose a SSID “vw-group” and it will be connected automatically without any credential.



Guest Wifi can be also available with SSID “Porsche Hotspot” and it will be connected automatically without any credential.

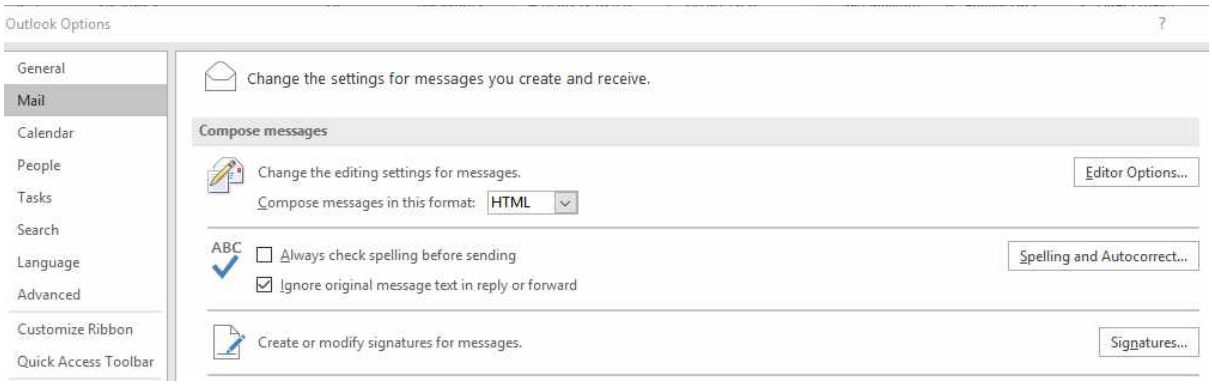
1.3 Outlook

Outlook is the Porsche's email application.

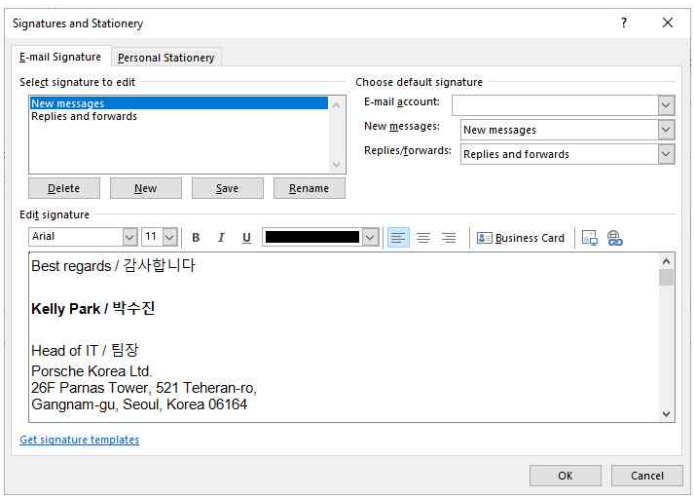


To set up your email signature, click:

File-> Options-> Mail -> Signatures



Add your signature.



1.4 Network Storage

Porsche Korea uses a network drive to share and save/backup all your department and personal data.

You should be able to access your department's folder, as well as the *PKO_Pool* drive and your personal storage area. If you are missing access permissions, please contact us.

If you double-click *This PC icon*  , you should see two network locations, your own and the department drive.

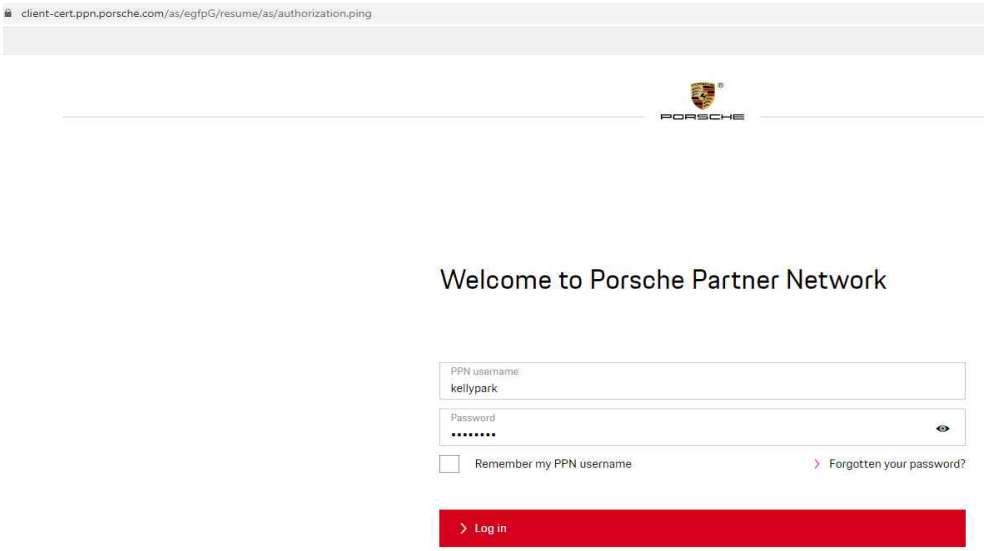
The screen depends on your department association, but you should see *PKO_POOL*.

Please save all data on these network drives. Your personal computer will not be backed up and your data will get lost if there are problems with your computer.

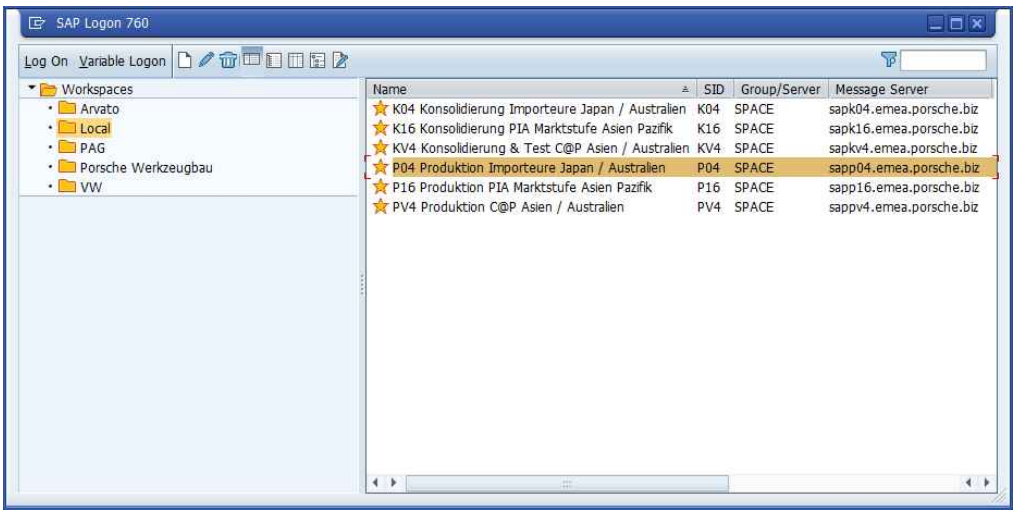
(So please avoid storing too many documents on the desktop and local documents folder)

1.5 PPN Portal and SAP

Porsche Partner Network Portal is a web-based communication platform, as well as a SingleSignOn Service to various Porsche IT systems. It can be the communication channel to our dealers, so instead of writing emails to a group of dealers, think about publishing the information on the PPN Portal.



Some of the **SAP** Systems can be accessed via PPN. Sometimes you will need to login directly to the SAP systems. In this case, please open *SAP Logon*, located on your desktop.



Please keep in mind, before you can use any SAP System, your manager needs to request a new user setup.

1.6 Data Security

As already mentioned in the employee handbook, you have to ensure data security and confidentially by working after Porsche's data security best practices:

Clearly classify and tag all documents (confidentiality levels and retention requirements)

Ensure that nothing is left after the meeting – and remove the information on your flipchart and whiteboard.
Conversations can be overheard - be aware of your environment! Be critical when inquiring about official content from unknown persons!

Close down all files containing confidential information when leaving the office.
Especially lock the computer.

In compliance with legal requirements and deadlines:
- Confidential documents should be placed in closed document disposal containers
- Disposal of 'Secret' documents with the appropriate specification shredder.

The desk becomes a "clean desk" – confidential information never goes away, it's stored in lockable furniture. The room is closed when leaving.

Be sure to encrypt volumes containing confidential documents. Only use certified media.

- Employees are required to lock (Ctrl+Alt+Del) their notebook whenever absent from workplace.
- Clean Desk Policy to be applied
- Documents have to be filed away after usage/work.
- Drawers have to be locked after work.
- Save your work on the department drive, your private information on the private folder and limit the information on the C-drive.
- Sending or downloading offensive material is not acceptable.
- Excessive and inappropriate personal use of email and internet is not endured. Access is intended to be used for business purposes.
- Do not disclose your passwords under any circumstances.
- Use only software which has been approved/certified by Porsche for your work. The use of software from other sources like the internet is not allowed.
- The use of equipment and storage media (e.g. USB sticks, smartphones, external hard disks) which has not been approved/certified by Porsche is not allowed.

Rules on storing and transmitting data

You can transmit data with the approved USB sticks only.

Approved USB sticks for data exchange between	
Approved USB (Read & Write)	Unapproved USB (Read only)
	

You have to save digital data according to table 1. If you have questions on how to request Approved USB sticks and use the encryption software, please contact us.

Table 1: Data must be stored as follows depending on the confidentiality level:

	Project and internal department network drives	Portable storage media (e.g. USB sticks, CDs) or in IT systems	Internal exchange platform (e.g. Data exchange server)	Porsche internally accessible Porsche network drives	External exchange platform (e.g. Dropbox) or Cloud services (e.g. Google Docs)
Public					
Internal					⊘
Confidential				⊘	⊘
Secret				⊘	⊘

Legend: Not encrypted | Encrypted | ⊘ Not permissible

Notes:

- Currently, the hard disk of a Porsche desktop PC is not automatically encrypted. If you want to store secret data on this equipment, you can use a container encryption software.
- Use the encrypted area on the Porsche USB stick for storing data which is worthy of protection.
- If available use LanCrypt (to be requested from your PC coordinator) for storing encrypted data on a Porsche network drive.

Further, you have to apply the following rules while transmitting electronic data according to table 2.

Table 2: Data must be transmitted as follows depending on the confidentiality level:

	To internal	To external	Screen-sharing application (e.g. NetViewer)
Public			
Internal			
Confidential			⊘*
Secret			⊘

Legend: Not encrypted | Encrypted | ⊘ Not permissible

*For „Confidential" in planning.

Notes:

- In order to encrypt internal Porsche e-mails using Lotus Notes, activate the "Encrypt" security option under the Delivery Options.
- For sending encrypted e-mails externally, use PGP encryption (to be requested via Porsche SecureMail Workflow in Notes).
- For sending encrypted content externally in an unencrypted e-mail, use a password-protected, encrypted ZIP file (the password must be transmitted using an alternative route).
- Basically external web mailers (e.g. GMX, Google, Telekom) are not permitted for company-related information.

Data Loss Prevention Solution

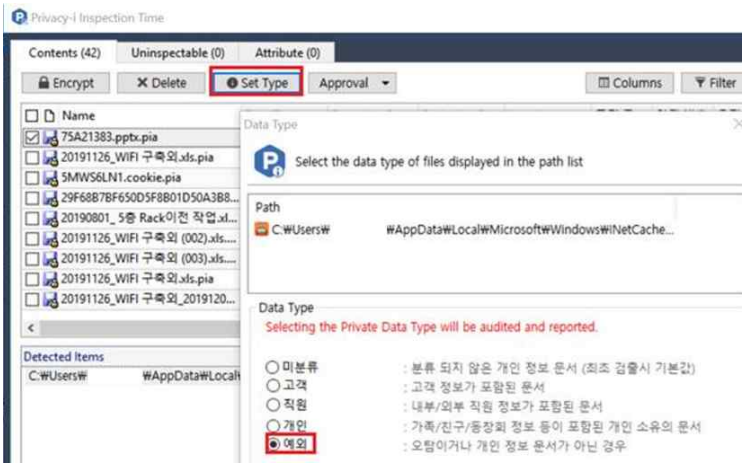
DLP identifies, monitors and protects data stored in our network or on desktops.
It detects and prevents the unauthorized use and transmission of corporate data such as sending a web mail, copying a file to a USB or leaking data.

You may see the following icon on your PC.

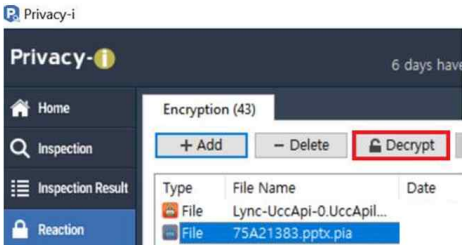
There are 3 policies defined.

- Detection
  - Monthly inspection is scheduled at 11:30 am on the 15th of every month.
  - Resident registration number, Foreign Registration Number, Driving license number and passport number will be detected.
  - Once the inspection is done, you will see the completion message with the number of patterns or files were found.

    It may have a false positive. You can set an exception rule by setting the Data Type as below.



Please delete or encrypt the detected files if they contain personal or confidential information.
If you'd like to decrypt files at once, you can select all files in "Reaction" tab and click Decrypt.



- Prevention
  - USB : Data read and write is available on the PKO registered USB sticks.

    Data read-only for the unregistered USB. If you'd like to copy files into the unregistered one, you can ask approval for the one time use.

    It will be also applied when you are not connected to the PKO network.

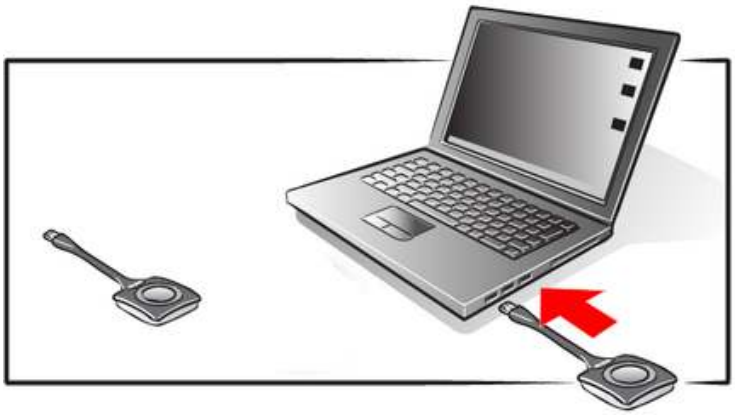
  - Upload : File upload to webmail(e.g. Naver, Gmail…) or blog will be monitored. If you upload a file contains personal information, it will be blocked.

- Retention
  - Monthly inspection is scheduled at 11:30 am on the 10th of every month.
  - The files are older than 4 years will be encrypted. You have to review the files and delete the unnecessary ones.

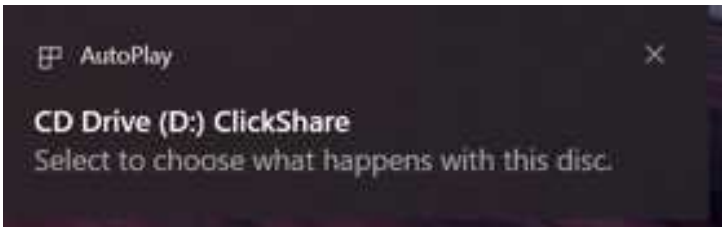
1.7 Meeting Environment

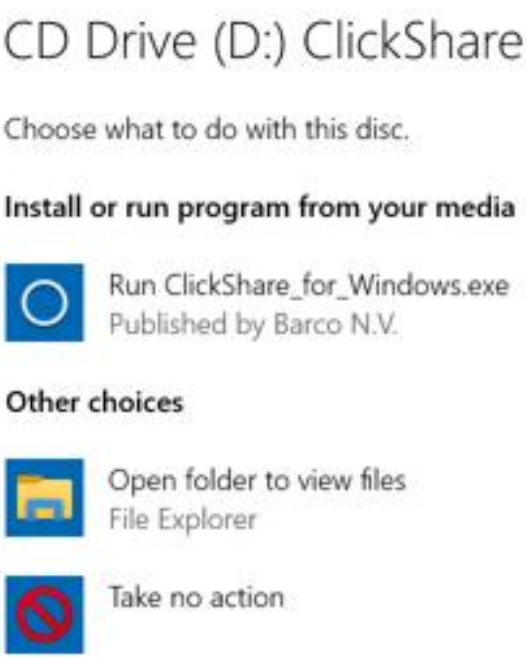
- Wireless presentation
  - Clickshare at all meeting-rooms

1. Connect a USB dongle to your laptop.

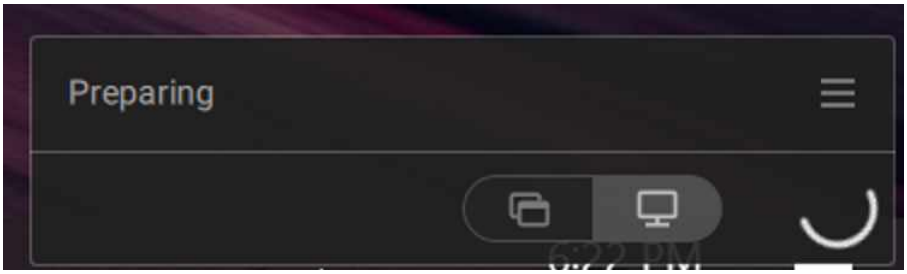


2. you will see the following pop-up. Please run ClickShare_for_Windows.exe.

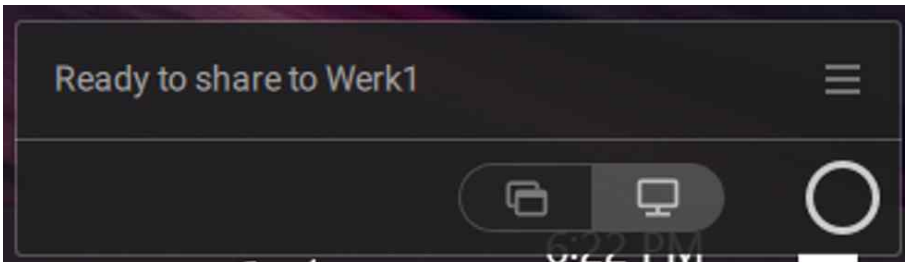




3. Please wait for a while until your laptop is connected to ClickShare.



4. Now you are ready to share your screen.

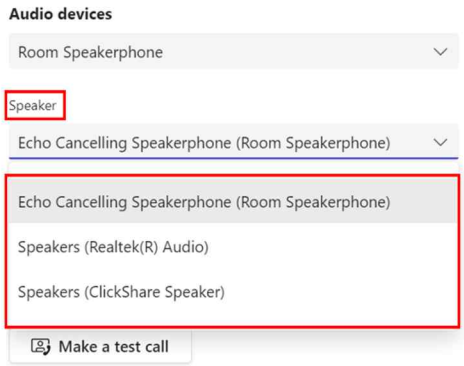


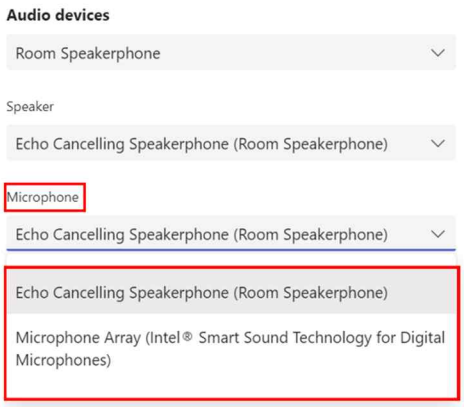
5. You can just click the button to share your screen.

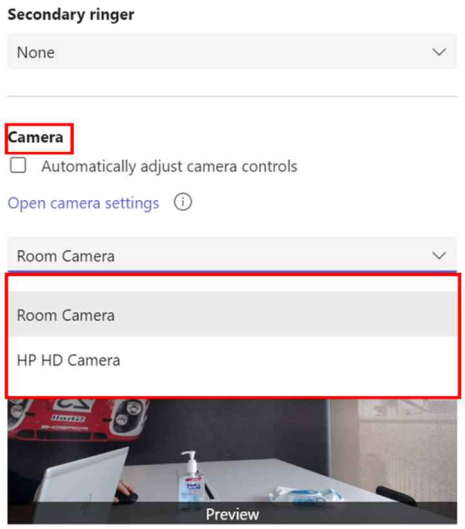
- Conference system
  - Web conference (MS Teams)

1. Connect a Clickshare to your laptop.

2. Select the devices which you'd like to use on conference call. the default.
   Settings -> Devices -> Audio Devices / Camera

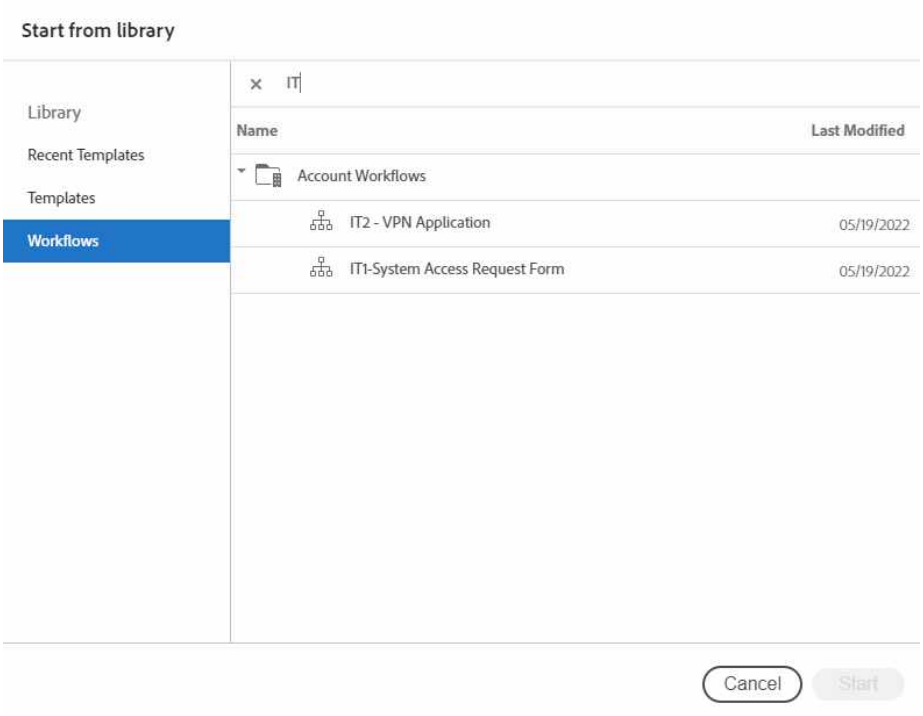






1.8 IT Request Forms

You will find IT Request Forms on the Adobe Sign:



1.9 Telephone, Printer and Scanner

Telephone

If you want to make an internal call, you have to dial the last four digits of the phone number

Last 4 digits (e.g. 9153)

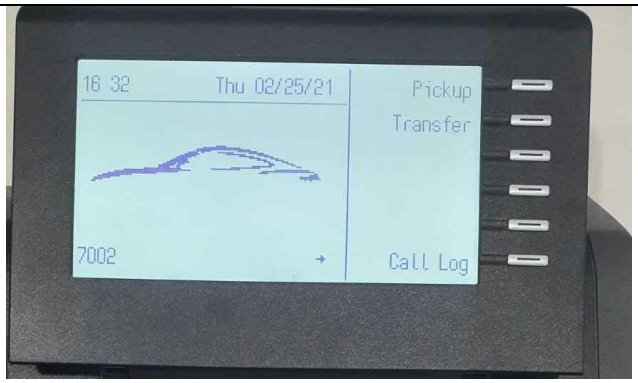
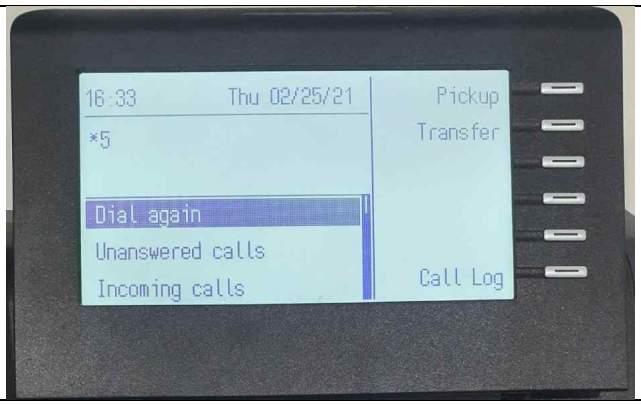
If you want to make an external call **within Korea**, you have to dial

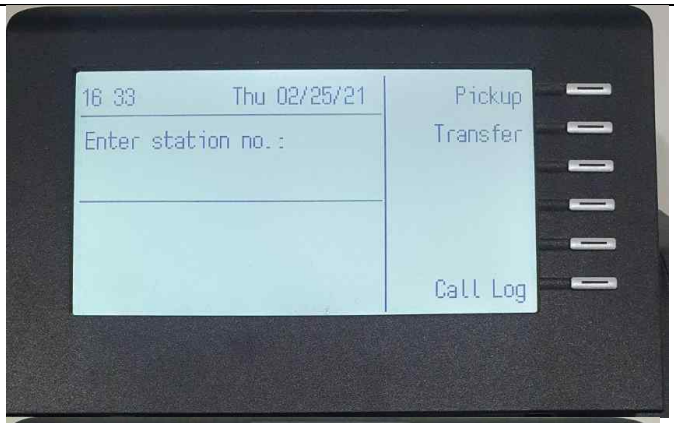
8 + Telephone number (e.g. 8-2-2055-9153)

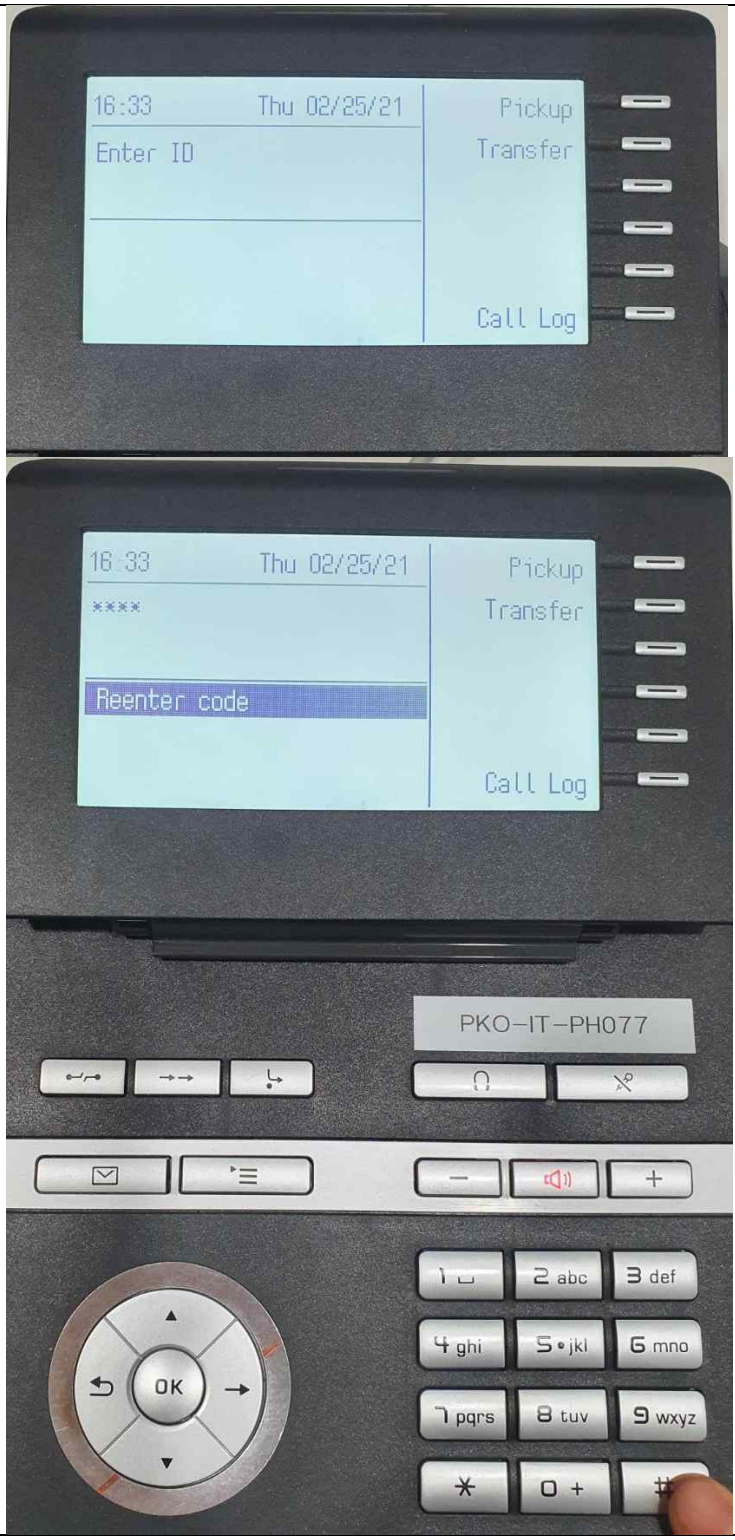
If you want to make an external call **outside Korea**, you have to dial

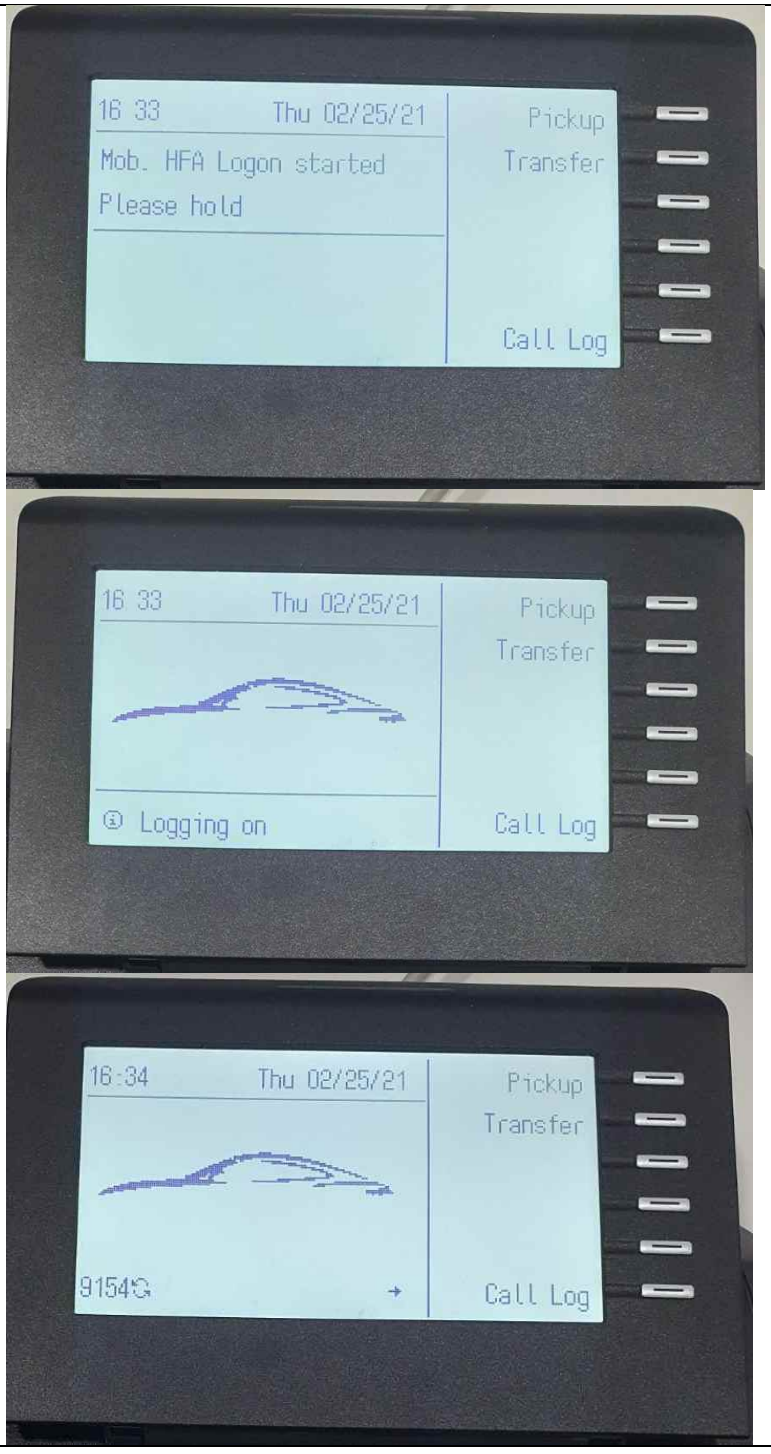
8001 + Country Code + Telephone number (e.g. 8001-49-711-911-29600)

How to log in to the desk phone before work

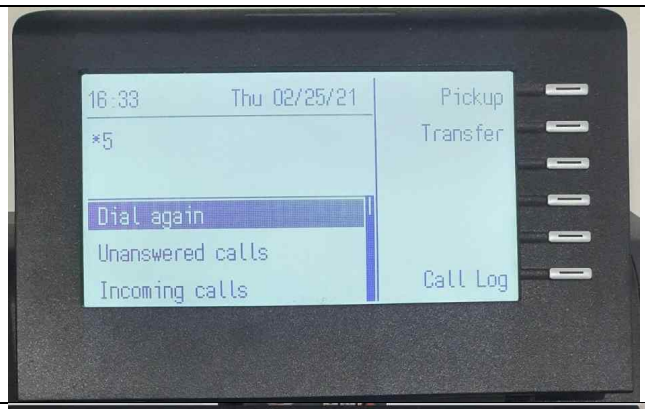
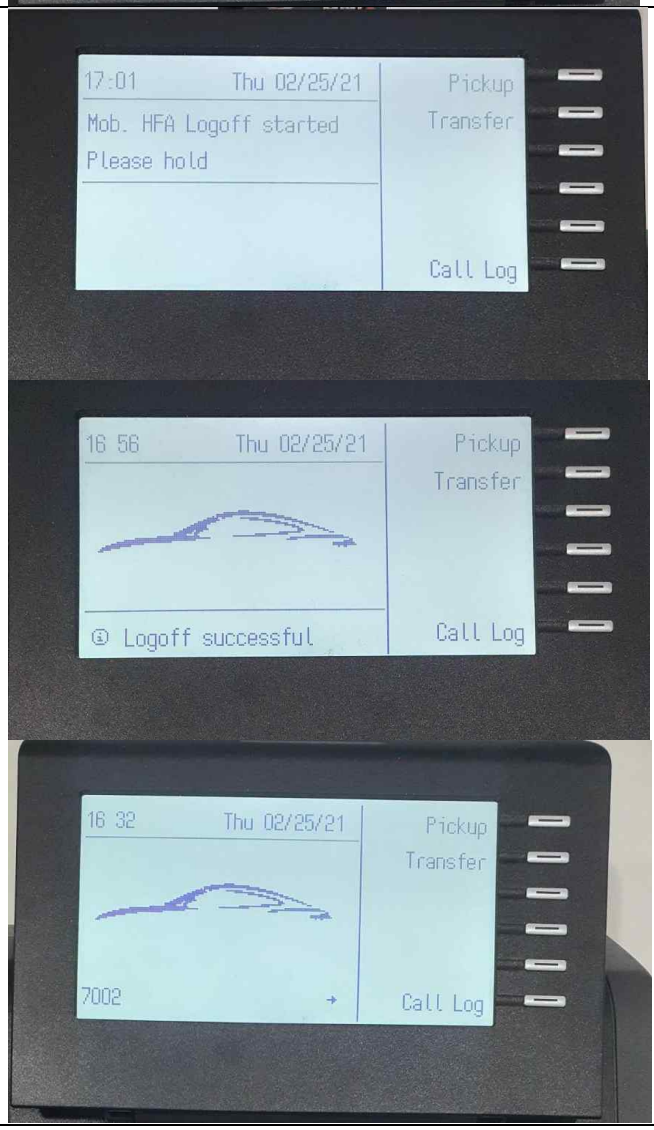
1. Check a virtual phone number between 7000~7100 on your desk phone's display panel. Note. If you see a number start with 9***, you should log out of the desk phone and log in with your office phone number	
2. Press *50 on your dial panel.	

3. If you see the message (Enter station no.:), press your office number and #. i.e.) 9154#	 

4. If you see the message (Enter ID), press your office number and # one more time.	

5. You can see the messages in the following order and wait for 10 second. (1) Mon. HFA Logon started Please hold (2) Logging on Next, you can see your office number(i.e 9154) and the circular arrow appearance, then the login is complete.	

How to log out of the desk phone after work

1. Press *51 on your dial panel.	
2. You can see the messages in the following order and wait for 10 second. (1) Mon. HFA Logon started Please hold (2) Logoff successful Next, you can see the virtual number between 700~7100 (i.e 7002), then the logout is complete.	

Notes.

- If you miss a call after work hours, it will be saved and you can see it after login at your new seat. To see the missing calls d press the button next to 'Call Log' sign.
- If you see a number start with 9***, you should log out of the desk phone and log in with your office phone number

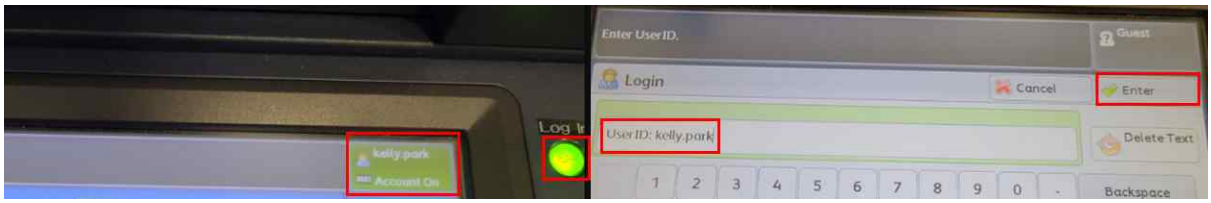
- Printer and Scanner

Touch your access card to the reader.

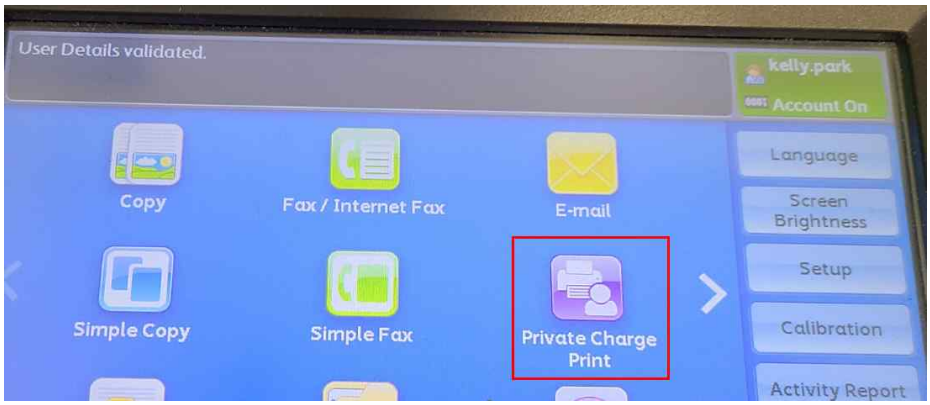
(This may not work if you have temporary access card. Use method mentioned below.)

Once logged in successfully, your windows ID will be displayed. Manual login (typing windows ID) is also available with Key button.

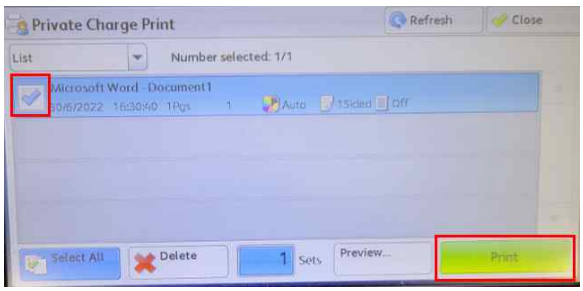
Your windows ID is ***"firstname.lastname"***



Select "Private Charge Print" to print out individual documents.

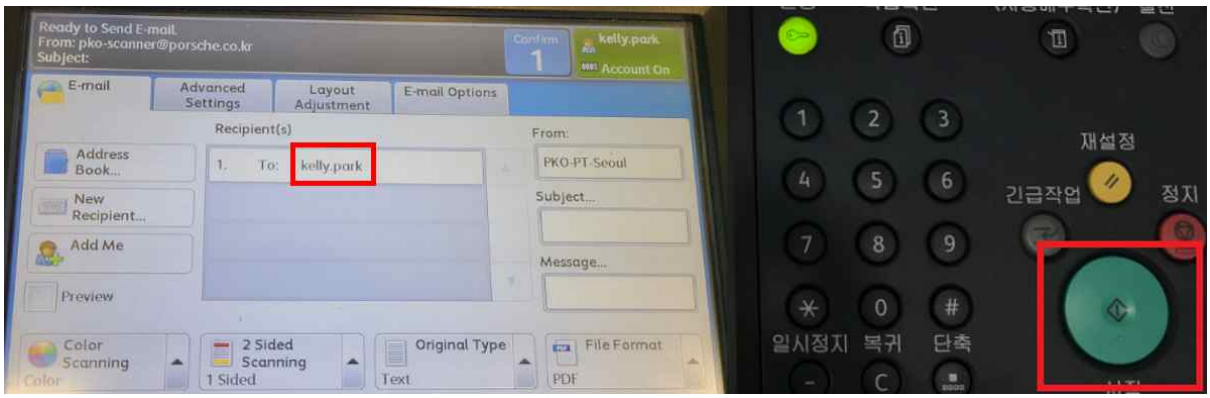


The spooled job will be purged every 24 hours which means unprinted job will be automatically deleted.



You can scan documents in E-mail menu.

Your ID will be automatically populated in recipient field. Therefore, you don't need to search your name or email address anymore. After documents are scanned, press a green button to send an email.



Contact Us – IT Help Desk PKO

Telephone internal: -9157
Email: PKO.ITHelp@porsche.co.kr