

2019/8

Ver. 1.7.0

BthLogon

Windows Logon Authentication using Android Device

RiBiG Inc.

<http://www.ribig.co.jp/bthlogon>

Contents

1. Introduction	4
1.1 Remote Desktop Support	5
1.2 Security	6
2. PC / Android Requiriements	7
3. Android Device Registration	8
3.1 Android Device Setup.....	8
3.2 PC	9
Device Name	11
Configuration PIN.....	11
Configuration PIN Lock	11
Login Pin	11
Pin Lock	11
Username (optional)	12
Password (optional)	12
Can omit CredInfo (optional)	12
ValidTill (optional)	13
3.3 Files created during the device configuration.....	13
2.4 Android Device Re-Configuration	14
3. BthLgon Installation.....	15
3.1 Deploying Public key and Device Registration Files	18

Windows Configuration for Autologon.....	21
4. While you are logged in	23
5. Disabling Credential Providers.....	24
6.1 Safe Mode.....	25
6. Remote Desktop.....	26
7.1 Setup For Remote Login.....	26
Pairing	26
Install the remote desktop plugin on the client	26
On RDT Server side.....	29
Disabling Network Level Authentication(NLA).....	30
7. Password Changes	33
8. Uninstalling BthLogon.....	34
9. Trouble Shooting.....	35

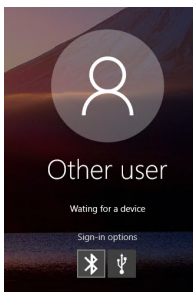
1. Introduction

BthLogon is a credential provider that logs you in to Windows by authenticating wirelessly your Android device. It communicates with Android devices via Bluetooth. BthLogon and Android devices securely authenticate each other and BthLogon will not log you log in, unless you have a device that has been configured by BthLogon system.

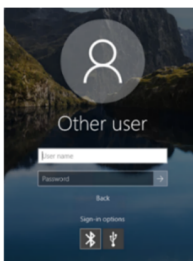
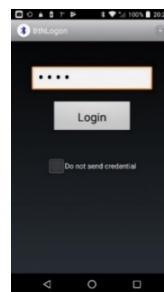
When you select BthLogon in Windows logon screen, you find the screen locked. BthLogon waits for a configured device to connect. On an Android device, enter PIN and tap [Login] button in BthLogon app. It wirelessly connects to PC and once the device is successfully authenticated, the screen gets unlocked and you can enter your Windows' user name and password.

If the app is configured to save your Windows credential on your Android device, you will be automatically logged in immediately after the screen is unlocked

BthLogon Locked Screen



Android App



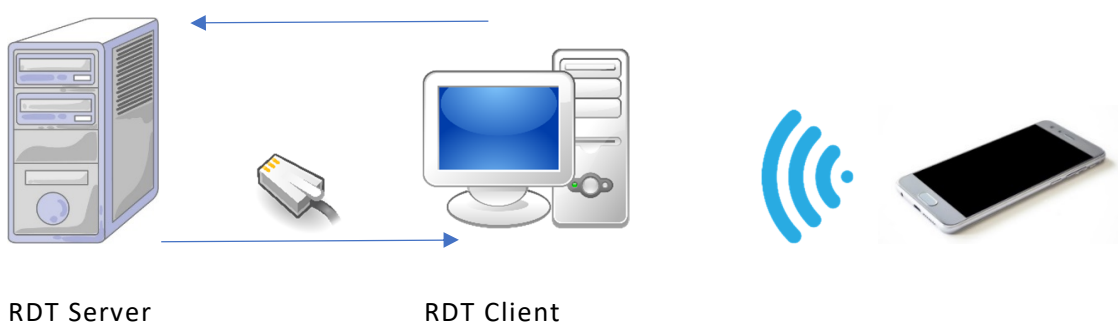
Unlocked

While you are logged in, BthLogon will continually query the login device for responses. If it does not receive several responses successively, the login session is automatically locked.



1.1 Remote Desktop Support

BthLogon installed on a remote server can be unlocked by Android device at the client side. The plugin for the terminal server client acts as a Bluetooth proxy for the remote server.



The remote server also continually queries the login device for responses through the client machine and will lock the session when no responses are returned.

1.2 Security

Since Bluetooth communication is wireless whose signal could reach any nearby devices, it must be secured the same way as Internet. This is especially so with BthLogon which could wirelessly transfer user credentials. BthLogon draws upon the industry standard security measures for data protection.

1. Windows and Android devices must be paired
2. BthLogon on PC and Android App exchange a secret key by DH protocol and encrypt the data by the shared key.
3. BthLogon and Android App must have their public keys signed by the other side and retain the signatures.



Public/Private Keys



Public/Private Keys

Public Key -----> signed by the private key
signature <-----

signed by the private key <----- public key
-----> signature

4. Before exchanging data, Android app asks BthLogon on PC for the public key and the signature by the app's private key. If BthLogon on PC cannot present the valid signature, Android app refuses to exchange data with the PC.

5. BthLogon on PC also requests Android app to present the public key and the signature. If the app does not have its public key signed by the private key of BthLogon, it stops communicating with the app.
6. After they find they can trust each other do they start data exchange.

2. PC / Android Requiriements

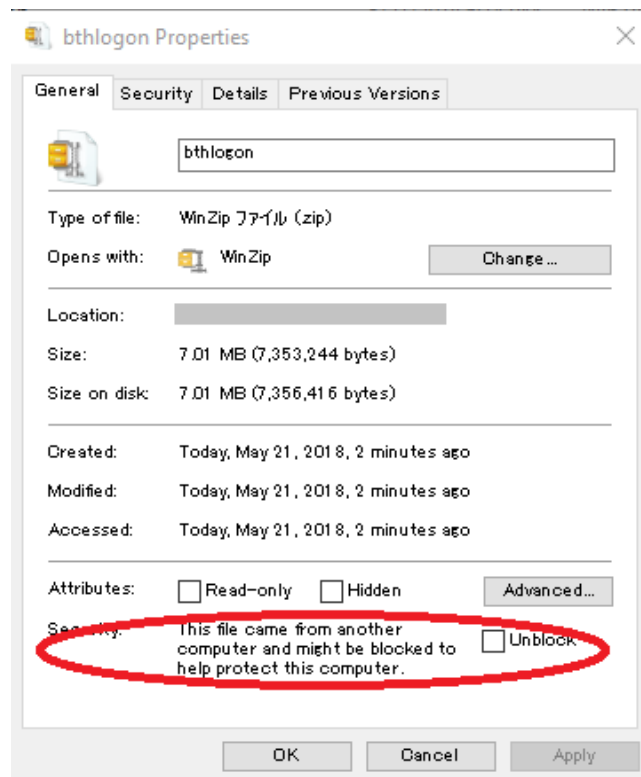
PC Requirements: You must have PC with Bluetooth embedded or Bluetooth adaptor detectable by Windows Bluetooth driver. Do not use non-Microsoft Bluetooth driver such as BlueSoleil. BthLogon will report an error with BlueSoleil.

Android OS Requirements: Android OS must be version 5.x or higher.

Clock Requirements: PC clock and Android clock must be synchronized. They verify the time of the commands sent by the other side. If the difference between the current time and the command time is beyond a threshold, the commands will fail.

Once BthLogon on PC and Android App are installed, no Internet connection is required.

You need a copy of BthLogon distribution file. The access to a file downloaded from Internet is blocked. Be sure to unblock by right-clicking the file, selecting "Property" and enabling "Unblock" check box in [General] tab.

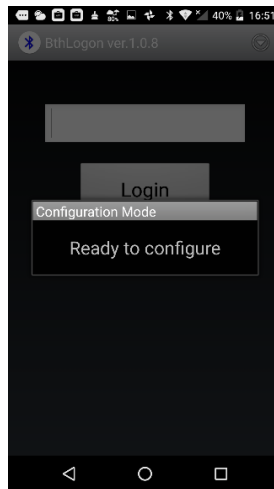


3. Android Device Registration

First, you need to set up Android device(s).

3.1 Android Device Setup

1. Turn on Bluetooth and pair the device with Windows PC
2. Install BthLogon app from Play Store
3. Run the app; it will be in the configuration mode



3.2 PC

Once the device is ready for configuration, run the configuration program on PC.

1. Copy “conf” folder in the distribution file to a fixed disk
2. The destination folder must be writable.
3. The critical data (private key) will be created in the folder. Set the access permission of the folder to be accessible only by authorized users.
4. Run device_config.exe in the destination folder.

You always need to run the program in this destination folder. It can be a shared folder or one on a removable disk.

Configuration Program

The image shows a 'Device Configuration' window. On the left, there is a vertical button labeled 'Find Devices' which is highlighted with a blue rectangular border. To the right of this button is a large, empty rectangular list box. Below the list box, there are several input fields arranged in two columns. The left column contains: 'Device Name' (text box), 'Setup PIN' (text box), 'Confirm Setup PIN' (text box), 'Setup PIN Lock' (spin box with '7'), 'Login PIN' (text box), 'Confirm Login PIN' (text box), and 'Login PIN Lock' (spin box with '7'). The right column contains: 'Username' (text box), 'Password' (text box), 'Confirm Password' (text box), 'Can omit CredInfo' (checkbox), and 'ValidTill' (text box). At the bottom right of the window is an 'OK' button.

Click on [Find Devices]. The names of the available devices will be displayed in the list box. The names of unregistered devices will be prefixed with “**” (two asterisks).

This image shows the same 'Device Configuration' window after the 'Find Devices' button has been clicked. The 'Find Devices' button remains highlighted with a blue border. The previously empty list box is now populated with three entries, each on a new line: '**[redacted]', '**[redacted]', and '**[redacted]'. The rest of the window, including the input fields and the 'OK' button, remains the same as in the previous image.

Enter configuration values

Device Name

An arbitrary string identifying an Android device. Give a name with which you can pinpoint the device

Configuration PIN

Pin required to set Android App in the configuration mode. If you lose this PIN, you will not be able re-configure the device.

You must connect a license USB key to run Device_config.exe as the commercial version. Without a valid USB key, it will run in the evaluation mode.

**** Evaluation Mode****

PIN must be 4 digits long and all the numbers must be the same
e.g. 1111, 7777

Configuration PIN Lock

Max. number of successive false Pin entries.

Pin will lock upon the pin error count's reaching the number

Login Pin

Pin for the App to start communicating with BthLogon on PC

****Evaluation Mode****

PIN must be 4 digits long and all the numbers must be the same
e.g. 2222, 3333

Pin Lock

Max. number of successive false Pin entries.

Pin will lock upon the pin error count's reaching the number and you no longer can use the device to unlock BthLogon

Username (optional)

Windows username in the format you normally enter as username (UPN, downcast, username only, etc.)

Domain\user, user@domain

If this is set, the value will be entered to the username field in the unlocked login screen

Password (optional)

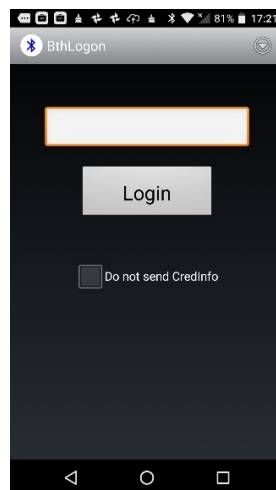
Password for the username. Set password only when username is set.

When both username and password are set, BthLogon will automatically log you in to Windows.

When only username is set, BthLogon will allow you to login only as the specified user in the unlocked screen.

Can omit CredInfo (optional)

When checked, the app will show a check box not to send username/password to BthLogon on PC

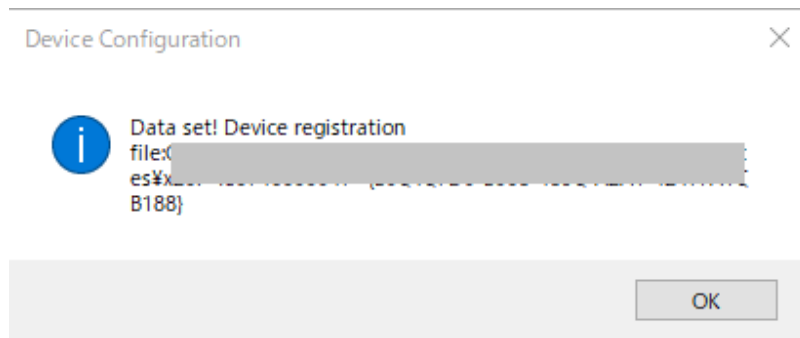


With the check box enabled, the app will not send out username/password. If neither is set, leave this checkbox unchecked.

ValidTill (optional)

Expiration date of the configuration data. If left empty, the configuration will not expire.

To start configuring a device, select the corresponding device in the list box and click on [OK] button. Upon successful configuration, a file will be created for the configured device and its path is displayed.



Tap on Android screen to exit the configuration mode. This completes a device setup.

When an error is reported after the program starts setting the device, be sure that the device is in the configuration mode. Re-try a few times. If an error persists, refer to the trouble shooting section of this manual.

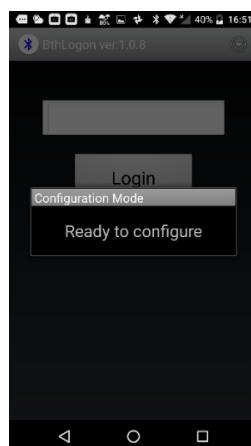
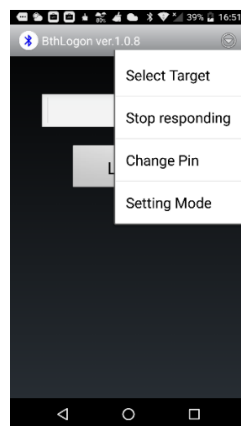
3.3 Files created during the device configuration

1. In the same folder as device_config.exe, a pair of private key and public key will be created if they do not exist. The file names are public.key and private.key. These files are critical; we suggest that you create their backup. You will need these key files to configure other devices.

2. In the same folder, a folder named “devices” will be created and under the folder, the device registration file is placed. The file name begins with the device name you have set.

2.4 Android Device Re-Configuration

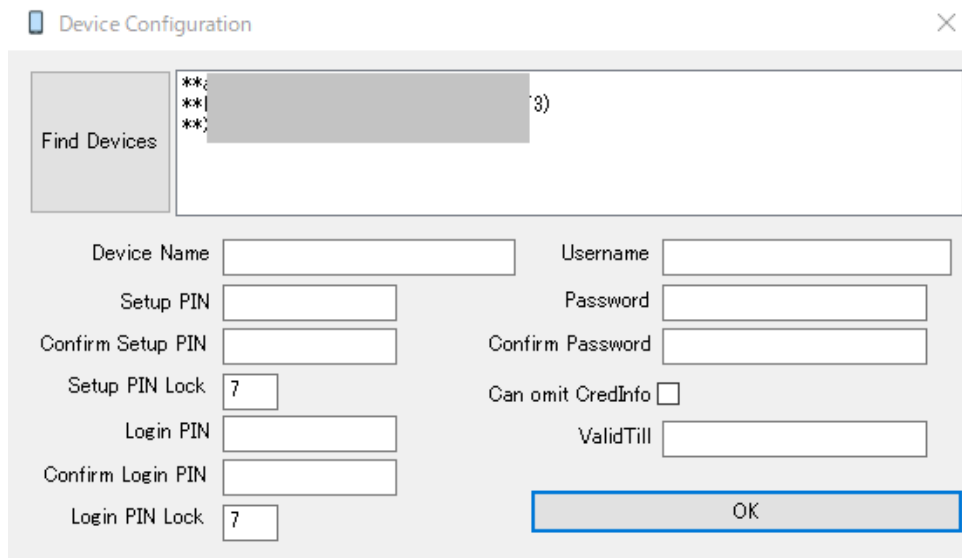
Set Android app in the setting mode by entering the configuration Pin and select “Setting Mode” in the menu



If you lose the configuration Pin, you will not be able to set the app in the setting mode. If this is the case, you have only one option; uninstall the app and install it again.

No function is provided to retrieve data on Android device from PC. You have to re-set the configuration values. The only difference from the fresh configuration is, the device name will not change no matter what value you give to it unless you specifically indicate that you want to change the device name by prefixing “#” .

1. After running device_config.exe, click on [Find Devices] button.

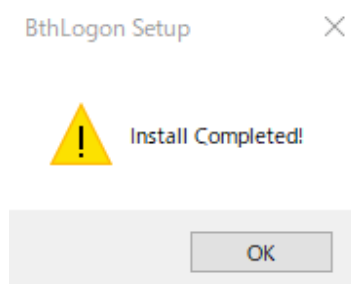
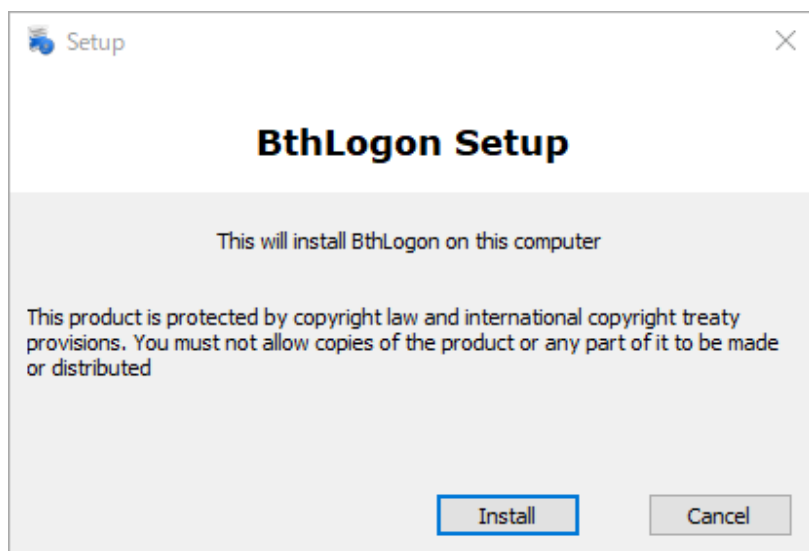


2. The name of the configured devices will have no “***” prefixed. Select one with no “***” prefixed.
3. Fill the configuration values, select a configured device in the list box and click on [OK]. Device name can be anything; unless you prefix it by “#”, the existing name will be retained.

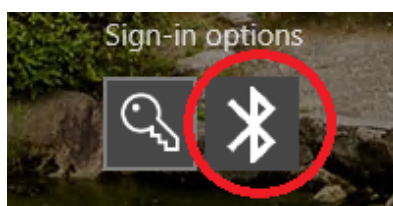
3. BthLgon Installation

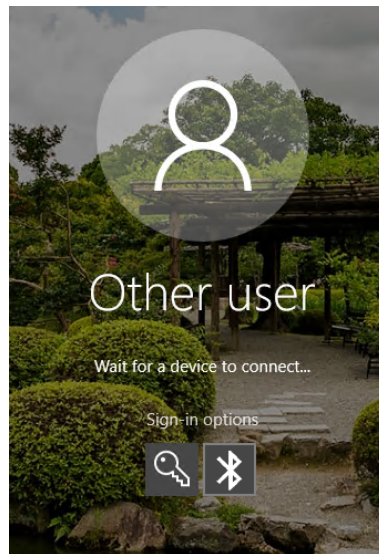
Once Android device is configured, you are ready to install BthLogon on PC.

Run auto-setup.exe in the distribution file. It detects the OS version and executes the setup program for the current OS. Press [Install] and it will complete in a few seconds.



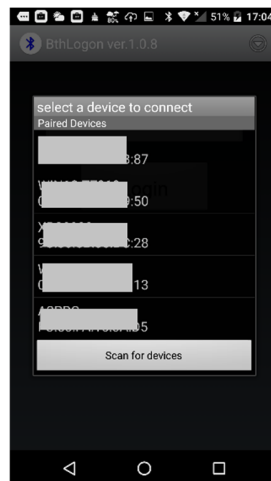
Sign out and select BthLogon icon in "Sign-in options"





BthLogon Lock Screen

In the app on Android device, enter Login Pin and tap on [Login] button.

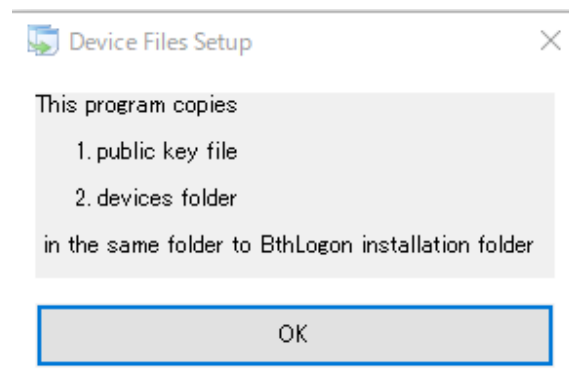


The app has not connected to any computer before and does not know to which computer to connect. It will show a list of paired devices. Select the PC you want to connect to.

The app will successfully connect to the specified PC, but the PC screen will not be unlocked. Why? You have not yet deployed the public key and the device registration file for BthLogon.

3.1 Deploying Public key and Device Registration Files

Run “InstallRegfiles.exe” in “config” folder. In the folder, there must be “devices” folder and device_config.exe you have used to configure the device.



Press [OK] and it will deploy the necessary files. Every time you configure a new device, run this program for the device registration file deployment.

Alternatively, you can manually deploy the files.

1. Copy Public.key to %ProgramFiles%\RiBiG\BthLogon folder
2. Copy “devices” folder to %ProgramFiles%\RiBiG\BthLogon folder

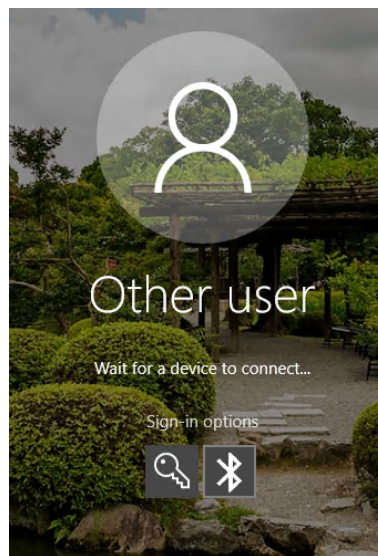
After “InstallRegFile.exe” installs the files, it will open “devices” folder under BthLogon installation folder(%ProgramFiles%\RiBiG\BthLogon). A device’s registration file must be in this folder for the device to unlock BthLogon screen.

You can copy “public.key” and “devices” folder to other computers with BthLogon installed.

To disable a device for unlocking BthLogon, remove the registration file for the device.

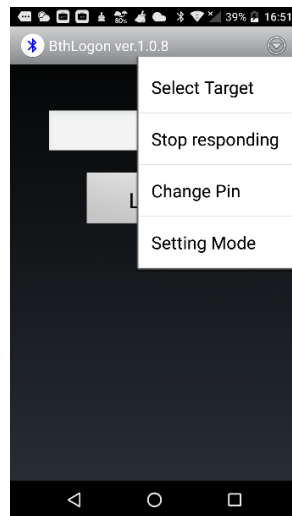
Sign-in in via BthLogon

Now you are really ready to login via BthLogon. Select BthLogon in the login screen.



On an Android device, enter Login Pin and tap on [Login] button. It shows a list of devices it can connect to. Select the PC with BthLogon waiting for connection. The app does not present the device list when it has previously connected to a device successfully. It saves its address and try to re-use it as the next connection target.

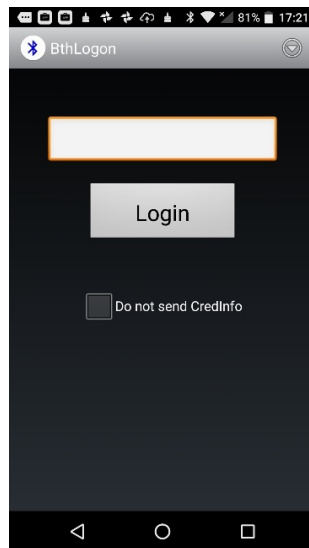
You can change the connection target from the saved one to another by selecting “Select Target” in the menu. Enter the login PIN and select the menu item. It will display the device list. Select a new connection target.



When the app connects to BthLogon on PC, the PIN field is cleared; it may take a few second. When everything works out successfully, the screen is unlocked and shows the user/password entry fields.



When you have set username and password when configuring the app, it will send the credential to BthLogon and you will not see the username/password entry screen; you will be automatically logged in to Windows.



When you enable “Can omit CredInfo” checkbox in the app configuration, the app shows a checkbox “Do not send CredInfo”. If you turn on this option, the app will not send out username/password to BthLogon. You will always be prompted to enter username and password after the PC screen is unlocked.

Windows Configuration for Autologon

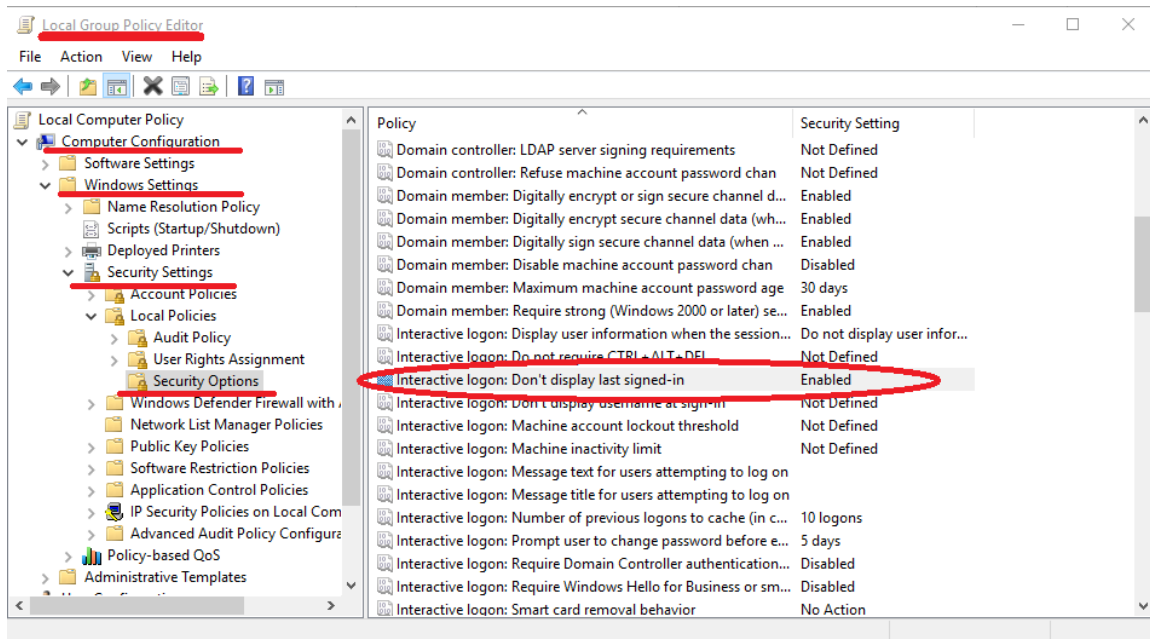
When you save username and password in the app, we strongly recommend that you configure Windows to prevent user names from being displayed in the login screen. This enables you to login as “Other User” where you are required to enter both username and password; you can always log in as an arbitrary user.

If Windows shows usernames in the login screen, you can only log in as the displayed user. You need to know in advance the saved username and select the right user in the login screen.

To hide usernames in the login screen, you can use the group policy editor or issue a command in the command prompt.

Group Policy Editor

Enable "Don't display last signed-in"



Administrator Command Prompt

Issue the following command to hide / show usernames in the login screen.

Hide usernames in the login screen

```
reg add
```

```
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"  
/v "dontdisplaylastusername" /t REG_DWORD /d "1" /f
```

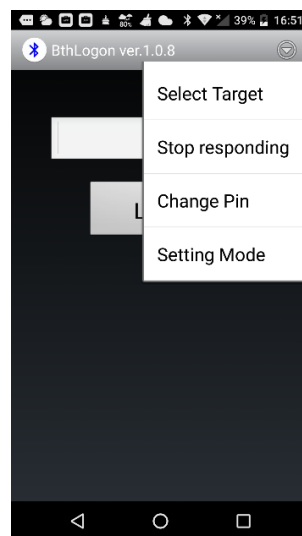
Show usernames in the login screen

reg add

```
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"  
/v "dontdisplaylastusername" /t REG_DWORD /d "0" /f
```

4. While you are logged in

After BthLogon logs you in to Windows, it starts to query the login device for responses. If it does not receive several responses successively, as when the device goes beyond Bluetooth range, BthLogon locks you out (optionally, signs you out). You can also cause the app not to respond to queries from PC by tapping “Stop responding” in the menu. Once the app stops responding to PC queries, it will be in that state until you leave the app once and come back to the app. For this, selecting the home screen or another app will do.



By default, BthLogon locks you out when Android app does not return responses. Optionally you can configure BthLogon to sign you out or to do nothing. Give the

following value to “ActionOnDisconnect” key under “Options” section in bthlogon.ini located in BthLogon installation folder: %ProgramFiles%\RiBiG\bthlogon

Sign out

[Options]

ActionOnDisconnect=signout

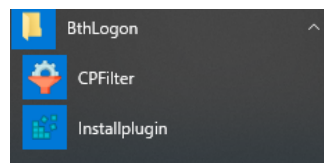
Do nothing

[Options]

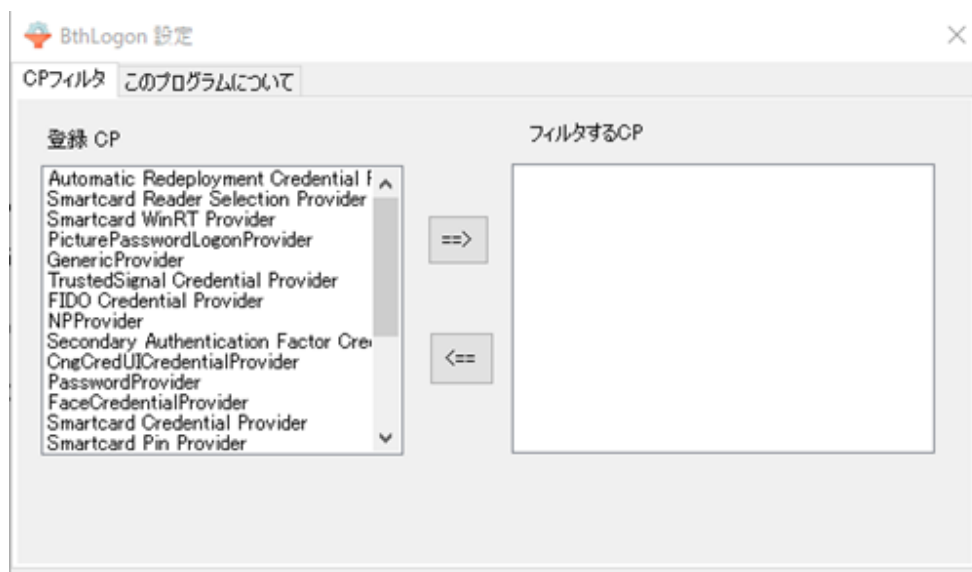
ActionOnDisconnect=none

5. Disabling Credential Providers

After installing BthLogon, you can still log on using various login provider bundled with Windows; Password provider, Windows Live ID provider, Pin Provider to name a few. You can disable those providers that you do not want to appear in the login screen by filtering them.



Select BthLogon –CPFilter in Start menu. Or you can run CPFilter.exe in BthLogon installation folder.



The left list box shows all the available providers on the system. Select the ones you want to disable in the left list box and press [==>] button; this moves the item to the right list box.

On Windows 8/10, we suggest that you filter at least those 4 providers.

PasswordProvider

PinLogonProvider

PicturePasswordProvider

WLIDCredentialProvider

6.1 Safe Mode

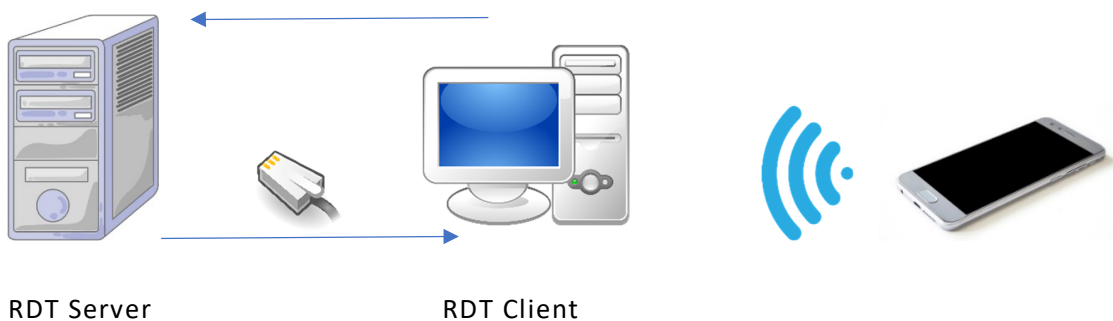
In Safe Mode, Windows Bluetooth driver is disabled and BthLogon does not work.

To secure Windows sessions under Safe Mode, consider using a solution like our SimplePCLock which requires a valid USB key to be plugged in to log in to Windows

session. When no valid key is connected, you will be forced to log out immediately after logging in. You may use any login providers and can sign in to Windows.

6. Remote Desktop

You can log in to a remote computer running BthLogon from a client machine using an Android device at the client side.



Android device communicates with the client machine via Bluetooth. The remote desktop plugin on the client relays the packets to and from the server.

7.1 Setup For Remote Login

On RDT Client side,

Pairing

Pair Android device with RDT client computer

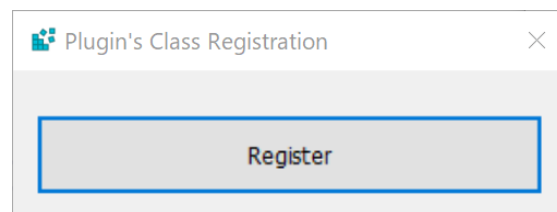
Install the remote desktop plugin on the client

Microsoft remote desktop client, `mtsc.exe`, loads the programs that are registered as plugin when it is executed. A plugin delivers additional features which an application program requires. For BthLogon running on a remote computer to communicate with a

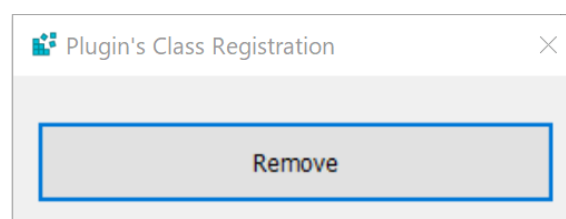
local Android device, it expects the remote desktop client to act as a communication agent on behalf of BthLogon. It comes with the plugin, RDTPlugin.DLL, that provides this feature.

You need 2(two) files, RDTPlugin.dll and InstallPlugin.exe, to install the plugin. On a computer with BthLogon installed, you can find the files in BthLogon installation folder: %ProgramFiles%\RiBiG\BthLogon. You can also extract 32bit or 64bit version of the files from the distribution ZIP file. They must be placed in the same folder.

1. An administrative user must register the plugin class for the plugin to be available for use on a computer. For that, run “InstallPlugin.exe” as administrator.



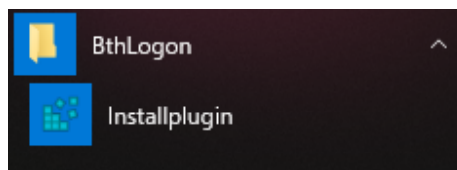
When the plugin class has not been registered, the button is labelled as “Register”. Click on the button and, if the class is successfully registered, the label changes to “Remove”



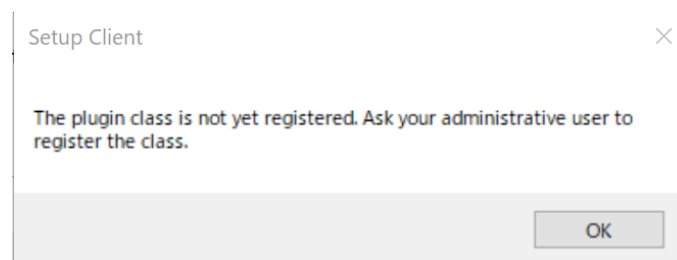
To de-register the plugin class, click on [Remove] button. It may take a few clicks for the class to be removed successfully. Keep clicking on the button till the label changes to “Register”

2, Each user who wants to use the plugin must enable the plugin. After it is enabled, Microsoft remote desktop client, `mtsc.exe`, will load the plugin. One user enabling the plugin will not enable it for another user.

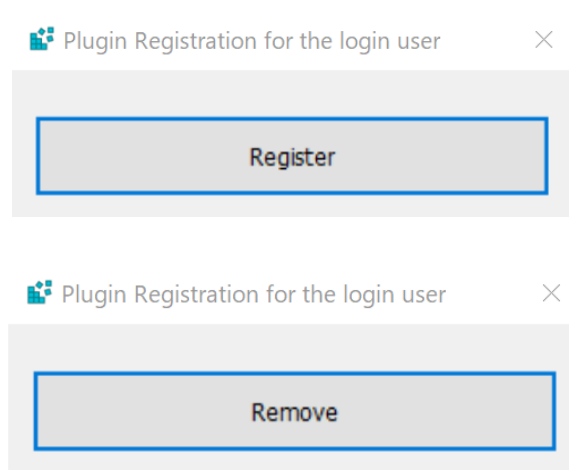
Run “InstallPlugin.exe” normally. If BthLogon is installed, you can find InstallPlugin under BthLogon in Start Menu.



If the plugin class has not been registered, you will get the error message.



The main window of the program shows a button whose label is “Register” when the plugin is not enabled and “Remove” when enabled.



On RDT Server side

First, enable Remote access and see if you can log in from a remote client using username / password provider. By default, the network level authentication (NLA) is enabled; it authenticates you at the client side before connecting you to the remote server. The credentials entered at the client side are encrypted and sent to the server.

If you have set Username and Password on your Android device for auto-login, you do not want NLA to ask you to enter a remote credential. In this case, you want to disable NLA. This topic will be covered in the next section.

If you have not set Username and Password on your Android device, you want NLA. Once NLA is successful, you want the login screen of the remote computer to be shown, to perform the device authentication and to log in to the remote computer as the NLA authenticated user.

The login screen of the remote computer shows “sign-in option” link and you can use the link to switch to another provider, thus, bypassing BthLogon device authentication. If you want to enforce BthLogon device authentication for the remote login, other providers must be filtered so that they will not appear in the login screen.

There are 2 ways to disable Password provider.

- 1 . Filter it using CPFilter.exe. This will filter Password provider for both local and the remote login
- 2 . It is possible to filter Password provider only for the remote login, while keep it enabled for the local login. For this, give the value TRUE to the key “FilterPassProviderInRemoteOnly” under “Options” session in bthlogon.ini file located in BthLogon installation folder.

[Options]

FilterPassProviderInRemoteOnly = TRUE

*Since %ProgramFiles% folder is not writable, copy bthlogon.ini to the desktop, edit it and copy it back.

Once Password provider is filtered, connect to the server again and see if the login screen shows “sign-in option” link. A local Android device should be able to unlock the screen, provided that the public key file and the device registration files are correctly deployed on the server side. Once unlocked, BthLogon will use the pre-collected credential to log you in automatically.

Disabling Network Level Authentication(NLA)

With NLA enabled, you are always prompted to enter your credential at the client side when trying to connect to a remote computer. You can disable NLA; this will prevent the credential prompt from appearing when connecting to a remote server.

To disable NLA, you need the following configuration at the client and server sides.

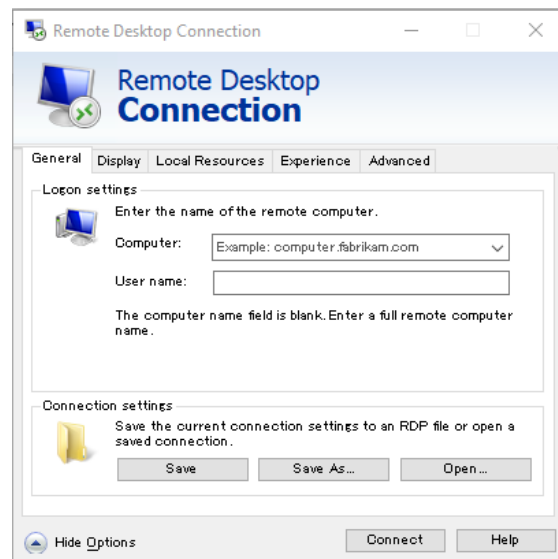
Client Side

The client needs to connect to the server as not supporting NLA. You can disable NLA support by specifying

enablecredsspsupport:i:0

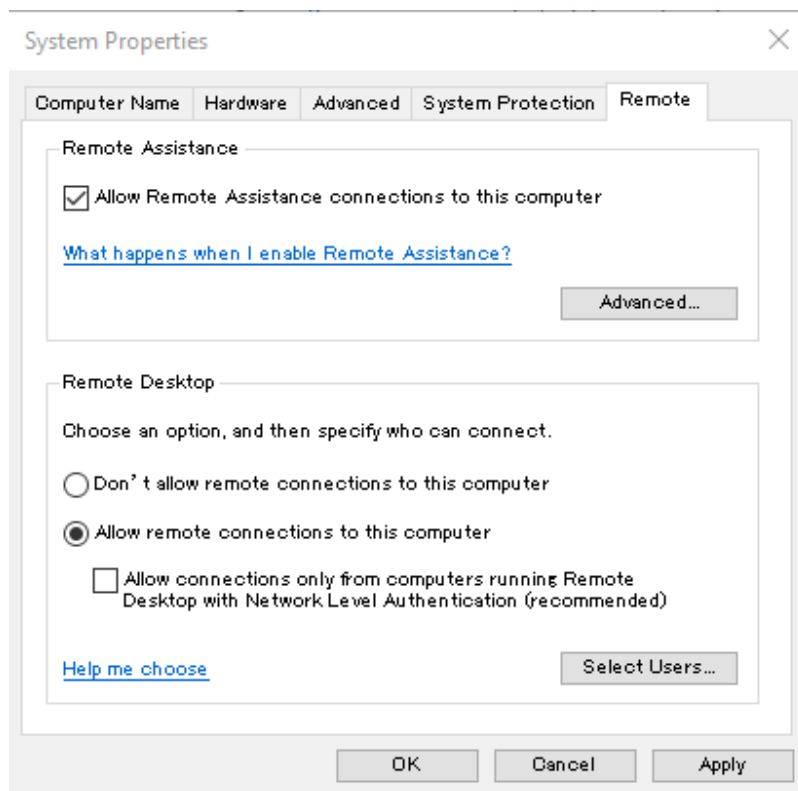
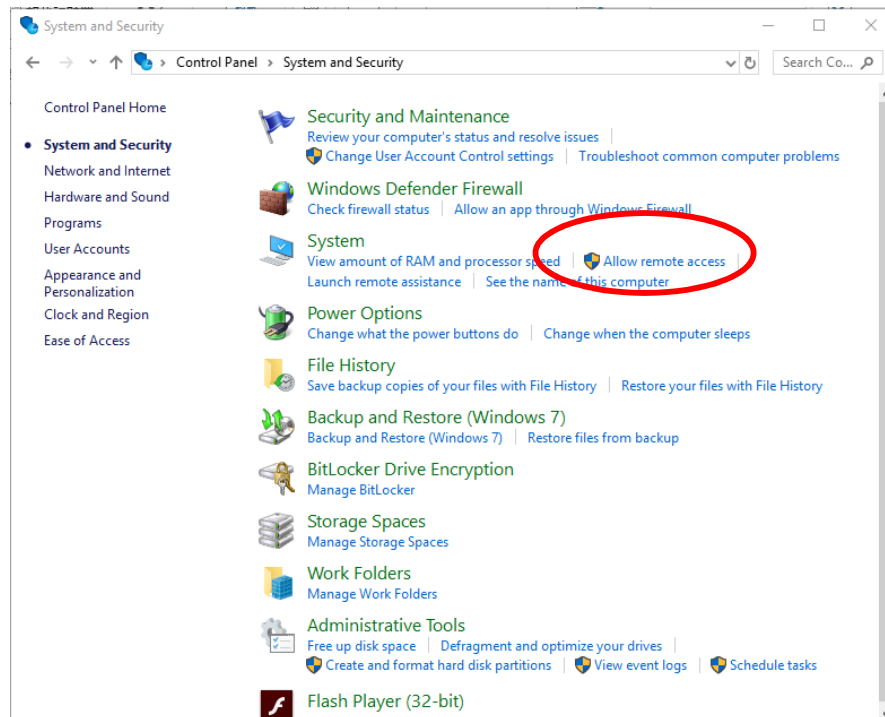
in the connection setting file, .rdp file. Add “enablecredsspsupport:i:0” to the bottom of the file, using a text editor.

The default .rdp file is C:\Users\<User>\Documents\Default.rdp. If you are using another .rdp file, add the line to the effective file.



Server Side

Open Control Panel and select “Allow remote access” under System.



Uncheck “Allow connections only from computers running remote Desktop with Network Level Authentication”

With NLA disabled, you are not prompted for your credential when connecting to a remote computer. Once BthLogon unlocks the login screen, it will securely retrieve the user credentials from Android device to log you in automatically.

7. Password Changes

After you log in via BthLogon, you can change your account passwords by pressing CTRL+ALT+DEL and select “Change a password”. When no credential is saved to Android device, the process of changing passwords is manually entering the current password and a new password. But when Android device holds the user credential and the user is not expected to know username and password, the process is automatic; BthLogon automatically generates a new password, changes passwords and updates the password stored on the device. The user does not have to enter anything; all done automatically for the normal users. Administrative users are required to change password manually.

This also goes for the login time password change. If the password has expired when trying to sign in, you are prompted to change passwords. When Android device holds the credential, the passwords are automatically changed. During the login time password changes, even the administrative users’ passwords are automatically updated, because users are not yet logged in and there is no way to detect correctly whether the user is normal or administrative.

The automatic administrative password change during the login time raises a problem. Nobody can know the new password BthLogon auto-generates. What if the

administrative user's passwords are changed and it is the only administrative account on the computer? It could mean that the administrative user loses her password and cannot manually log in even in Safe Mode.

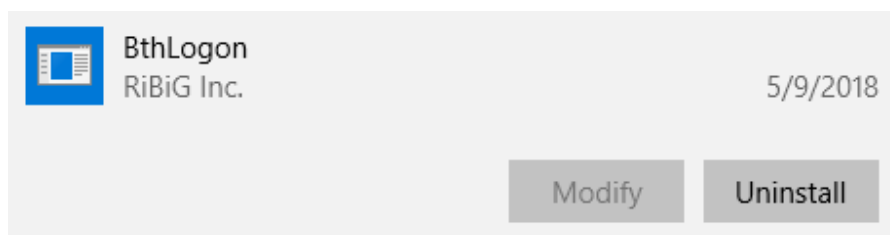
There are a few ways to avoid it. One is to keep pressing CTRL+SHIFT key just before automatic password changes are initiated. When BthLogon detects CTRL+SHIFT press when changing passwords, it does not change them automatically; it allows you to set a new password manually.

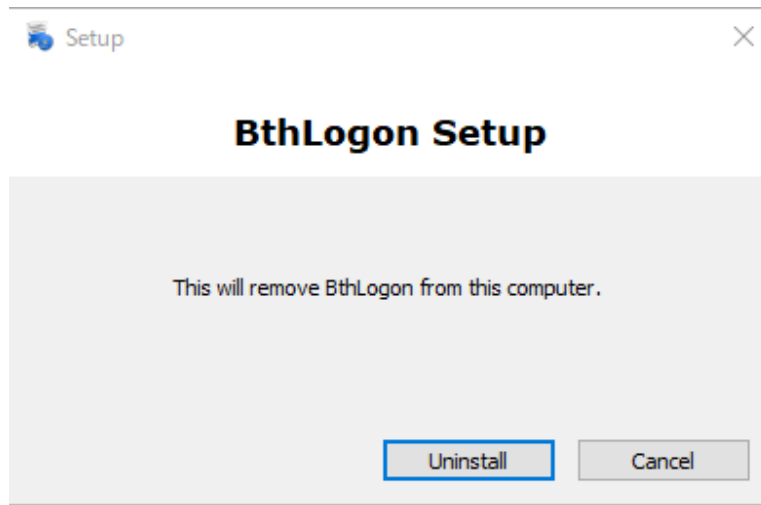
Another way is to set the administrative user's password not to expire, so that the password changes during the login time will never happen for them.

A third way is to create multiple administrative users' accounts and use one of them to log in under Safe Mode.

8. Uninstalling BthLogon

Select "App & Features" in Setting or "Add/Remove Program" in Control Panel. Select BthLogon and press "Uninstall" button.





Once the program finished, be sure to log out and log in again as the user administrative user. The first sign-in after the uninstallation will completely erase BthLogon.

9. Trouble Shooting

4.1 Device_config.exe reports an error while trying to communicate and to configure Android devices. Try the followings in the order indicated.

1. Disable Bluetooth of Android device and turn it on again
2. Terminate the app and launch it again
3. Restart Android device

4.2 BthLogon does not unlock even when you enter the right Pin and the app successfully connects to the device, showing "Connected to TargetName".

Be sure that the correct public.key and the device registration file for the device exist in their places. It may take a few seconds before the screen unlocks; just wait for a few more seconds.

- 4.3 Android may disable Bluetooth automatically to save battery when there is no Bluetooth activities for a certain length of time. When you get back to the app, it must re-enable Bluetooth and enter the mode to communicate with PC. The app could fail during the re-initialization. Please re-start the app.
- 4.4 Even when everything seems fine, BthLogon could not be unlocked. Try to log in again by specifying the target a few times.
- 4.5 Once you uninstall Android app and re-install it, it will create a new pair of private and public key. This requires the device to be re-configured fresh and its device registration file updated.
- 4.6 `device_config.exe` uses the existing pair of `public.key` and `private.key`. in the same folder. If it does not find either keys, it will create a new pair. It is possible to use multiple pairs of public and private key for different group of Android devices but unless you know how to do it, please avoid it and keep using the same pair. Once you use either keys, you will have to re-configure all the devices using the newly created keys.