MXLOGON2 MANUAL

2-Factor, 2-Step Windows Sign-in with USB Key

https://ribig.co.jp/mxlogon2
mxlogon2@ribig.co.jp
RIBIG INC.

1. About MxLogon2

MxLogon2 is a 2-factor, 2-step Windows sign-in solution. It requires you to have a valid USB key and to get it authenticated before you can enter username/password.

You must connect a valid, pre-configured USB key; otherwise, MxLogon2 will not detect one and will not show PIN entry field.

In the first step, you authenticate a USB key. You must enter the correct PIN to prove that you are the valid owner of the key.

After a successful USB key authentication, MxLogon2 shows the familiar Windows username/password login screen. You enter username and password as you would in Windows' standard login screen. Only after username/password are successfully authenticated, can you sign in to Windows.

At any time you plug off the key, MxLogon2 returns you to "Connect a token" screen.

This default 2-factor, 2-step authentication affords you the most secure way to sign in, using this program. But those who daily feel entering their username cumbersome find this program adding the drudgery of connecting a key and entering PIN. Do not worry; you can change the default MxLogon2 behavior by configuring USB key and MxLogon2 options.

1. You can bypass PIN entry; MxLogon2 authenticates a USB key and automatically switches to the second screen
2. You can auto-fill the username field in the second step.
3. You may also auto-fill the password field.

If you bypass PIN entry and auto-fill the username, you need to enter the password only. If you set the password auto-fill on top of that, connecting a key will log you in automatically.

Username auto-fill is not just for convenience; it expects you to log in as the user. You can edit and change the username field but MxLogon2 will not accept any other users than the one auto-filled.

Optionally, you can set a regular expression for the username auto-fill. In this case, MxLogon2 will not auto-fill the username field in the second screen; it matches the usernames you enter against the regular expression and accepts matched usernames as valid.

2. USB Key

Before installing MxLogon2, connect a USB key to a USB port of your computer or USB hub. Windows will automatically detect the key and load an appropriate driver. The driver is not proprietary; it is bundled with Windows and no network connection is required to load the driver. We ask you to dos this because some versions of Windows may not detect USB key in the login screen, if the USB key have never been connected to the USB port.

When USB key is not detected in the login screen, then, log in first, connect a key to the port and see if the driver loads.

3. Installing MxLogon2

MxLogon2 distribution file contains both 32bit and 64bit versions of MxLogon2

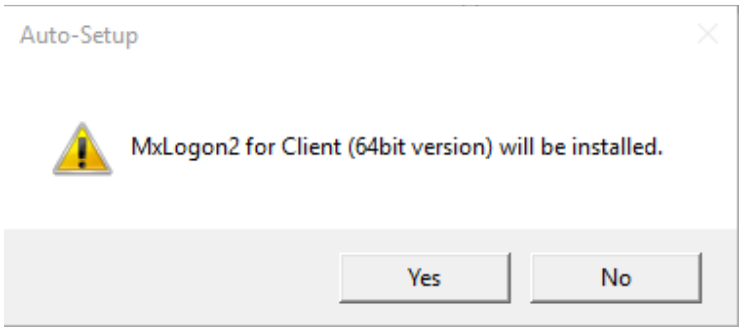
Client

X64

X86

Auto-setup.exe

Its root folder has 1 or 2 folders, one holding the client version and the other the server version. There you find 2 folders, [x64] for 64bit version and [x86] for 32bit version. Run "auto-setup.exe" in the root folder; it will detect the version of Windows the computer is running on and load the correct setup program.



Pressing [Yes] will start the setup program.

Press [Install] button to install. It will complete within a few seconds. Once the setup is complete, sign out and then try to log in via MxLogon2.

Changes in Sign-in Screen:

When you sign out, you may find the sign-in screen different from before installing MxLogon2. This is because the installer configures the screen to make it more secure; usernames do not get displayed in the screen and you are asked to enter an existing username manually.

[HKEY_LOCAL_MACHINE¥software¥microsoft¥windows¥currentversion¥policies¥system]

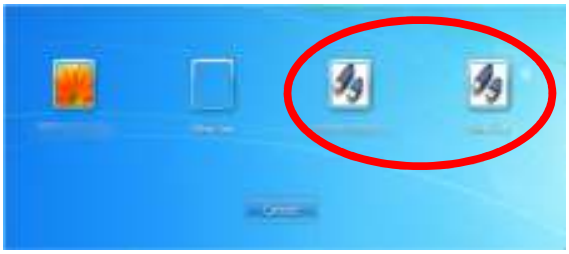
"DontDisplayLastUsername"=dword:00000001

"DontDisplayLockedUserId"=dword:00000003

If you want usernames displayed in the sign-in screen, set both registry values to 0(zero).

4. Signing in to Windows via MxLogon2

In the sign-in screen, you should be able to find MxLogon2 icon. On Windows 8/10, click on “Sign-in options” link. On Windows Vista/7, MxLogon2 icon is there on the screen.



4.1 PIN Authentication

Connect a valid USB key and select MxLogon2. It shows you the USB Key authentication screen with PIN entry field as shown above. MxLogon2 USB key has 4 (four) slots. Each slot has its own PIN assigned. You need to specify the slot by selecting one in the combo-box. The 4 slots' default PINs are **12345678**.

When multiple keys are connected, another combo box containing the key's serial numbers will be shown. This time, you need to select one USB key that you intend to use for login. The serial number is the default label of the key. You can change the key label to any arbitrary human readable string and the combo-box will show the string that is more helpful to identify a key.

Enter the correct PIN of the selected slot and submit.

4.2 PIN Lock

Successive entries of false PIN will lock a USB key. The lock is triggered on the 7th successive false PIN entry. You can change the default lock count of 7 to another value. Once a key is locked, the credential data in the key will be erased and PINs are reset to the default value. Unlocking will not restore the data and PIN; unlocked keys must be re-configured.

4.3 Username/Password Authentication

After the connected key is verified, MxLogon2 shows the username/password authentication screen. This is the same as Windows' standard username/password authentication screen; enter username and password as you would in Windows login screen.

5. Session Lock

Once you are logged in with a key, removing the login key will lock the screen. Unlocking the screen with a USB key is the same as logging in with one.

6. Configuring USB Keys

6.1 Built-in safeguard and PIN Change

MxLogon2 you receive is specially built for you. It only discovers USB keys that come with your MxLogon2; it will not detect the other users' keys. This means that other users' MxLogon2 will not accept your USB keys. This built-in safeguard protects each user's MxLogon2 and keys.

But all USB keys are delivered with the same default PINs (user PIN and SO PIN). The default PINs are well-known (12345678); they cannot serve as protective PIN. You must ensure that PIN serves to verify the USB key holder by changing PIN before release.

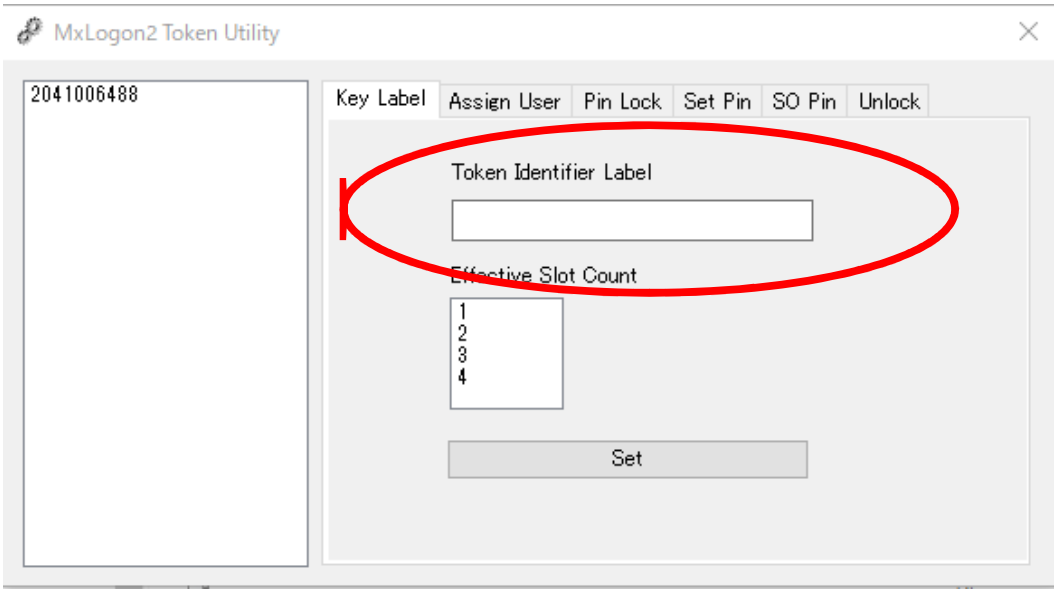
You can configure the USB keys using “cert.exe” in [Conf] folder in the distribution file. The files in [Conf] folder is not installed. The program is exclusively for use by the USB key administrator. The other users should not have any access to the program to protect the keys from unintended configuration changes.

6.2 Identifier String (Optional)

A key has a label for the identification purpose. The default label is the key’s serial number. You can assign an arbitrary human readable string as a label.

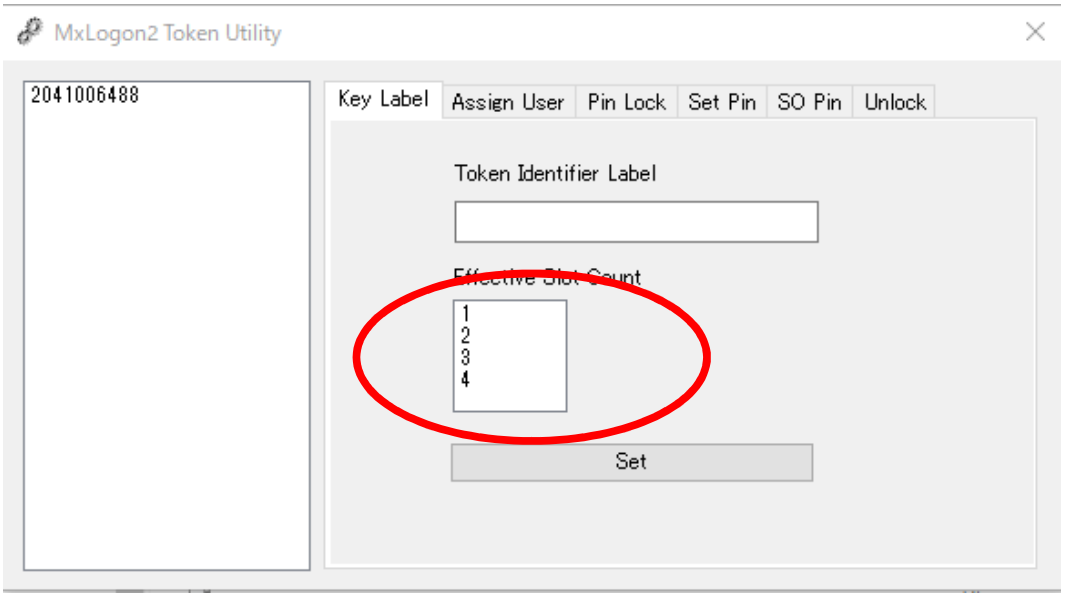
Labels are useful only when you connect multiple keys at the same time. Key naming helps distinguish among multiple keys .But if you connect one key at a time, you may not need to name a key.

To set the label, select a USB key in the left list box and enter an identifier string in the edit box. Pressing [Set] button will save it to the key.



6.3 Effective Slot Count

Each key has 4 authentication slots. By default, all 4 slots are enabled, but you can set the number of slots to enable by select the count in the list box.



When you select one and enable just one slot, the combo box for the slot selection in the login screen will not be displayed.

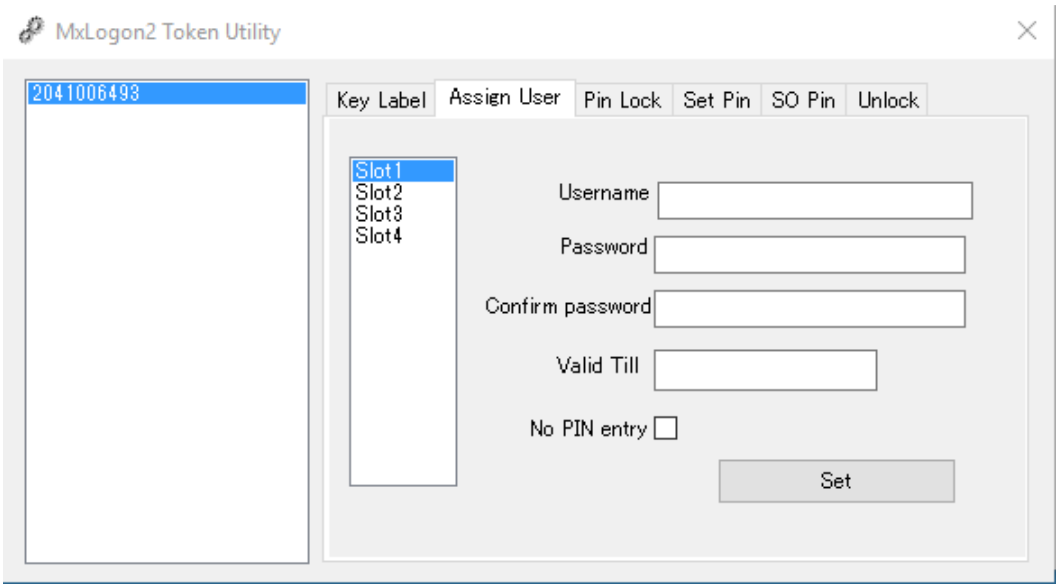
A key with one effective slot connected

6.4 PIN Bypass and Username/Password Auto-Fill

MxLogon2 allows you to bypass PIN entry. It can auto-fill the username field in the second step. It can also auto-fill both username and password field, logging you in automatically in the second step.

To set up, select [Assign User] tab and a slot

- PIN bypass - check “No PIN entry”.
- Username auto-fill - set a username. do not set a password
- Username/Password auto-fill – set a username and a password.



Username Field

Enter username as you would enter in the login screen. It can be in the form of down-level (Domain\Username) or UPN. You can specify “.”(dot) to denote the local domain. This is useful because “.”(dot) is expanded to a different local domain (computer name), depending on computers you connect a key to.

Password

Enter a correct Windows password for the username

ValidTill

Enter a date in the format of “yyyy/mm/dd” till the select slot’s credential remains valid. Keep the field empty if you do not want to set the expiry date.

No Pin Entry

When “No Pin Entry” is enabled, MxLogon2 will bypass the first PIN authentication and shows the username/password authentication screen.
Note that when this is enabled for slot1, MxLogon2 will always use Slot1 for login. You do no have chance to select another slot. When you also set Username/ Password auto-fill, MxLogon2 will log you in automatically upon slot selection.
When a key is plugged in, slot1 is selected.

6.4.1 Deleting the auto-fill

Leave the username field empty and press [Set] button

6.4.2 Password Change

When the username/password auto-fill is enabled, the key holder does not enter username nor password. We assume that the key holder is not expected to know the password. What if the password is expired and must be changed? The key holder cannot change the account password? No worry; the account password can be changed without knowing the old password.

When the username/password auto-fill is enabled, MxLogon2 will auto-fill the old password field, generate a new password and change passwords automatically. This happens when,

- while logged on, you press CTRL+ALT+DEL and select “Change a password”
- when trying to log in, the password is expired and Windows forces you to change passwords

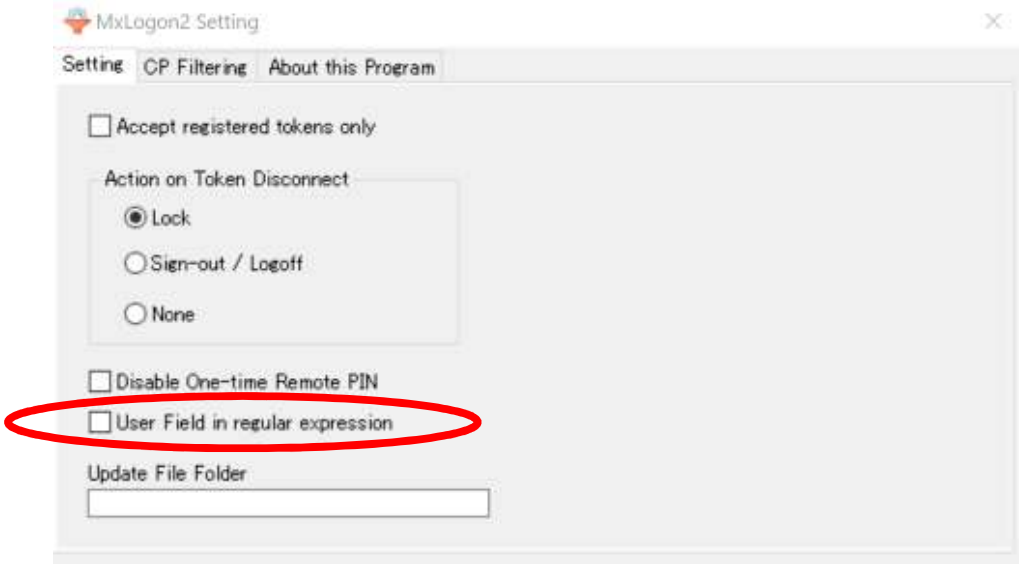
The auto-generation of a new password may be disabled; keep pressing CTRL+SHIFT as before the password change is executed.

- As when you submit PIN
- As when you change a password (PIN bypass enabled)

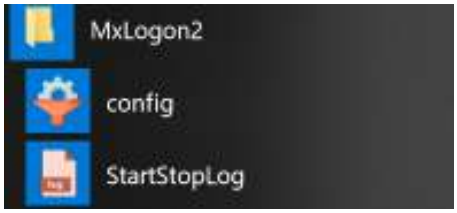
The password change screen will be shown with the old password auto-filled. You can manually set a new password.

6.4.3 "User Field in regular expression" Option

Instead of a plain username text, you can set a regular expression as the username.



Run "config" in [StartMenu]-[MxLogon2] or "config.exe" in MxLogon2 installation folder %%ProgramFiles%%\RiBiG\MxLogon2.



When this option is enabled, MxLogon2 will not auto-fill the username field in the second authentication screen. It will use the regular expression to test whether the username entered in the screen will match it or not. Only matched usernames are accepted for login. When the username is a regular expression, do not set a password.

Escaping the regular expression

When the first character is " (double-quote) , MxLogon2 will interpret the remaining characters as a plain text and use the text for the username auto-fill.

Note on how to set a regular expression

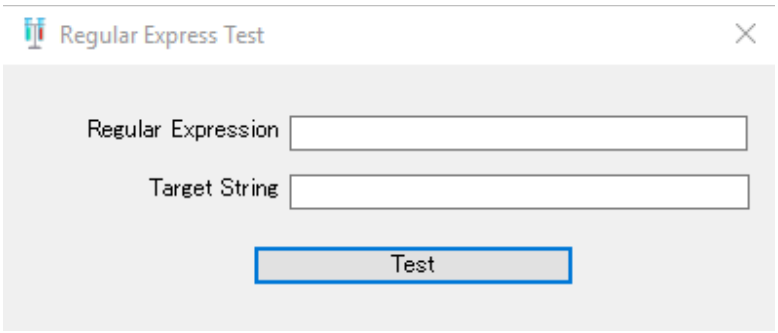
"."(dot) is a special character in the regular expression and cannot be used to denote the local domain. Use the string "LDMN" instead for the local domain.

e.g.

(LDMN|mydomain|mydomain1)\\.*

This expression will allow users in the specified 3 domains

A tool, Regex_test.exe, is available under "Conf" folder in the distribution file to test a regular expression.

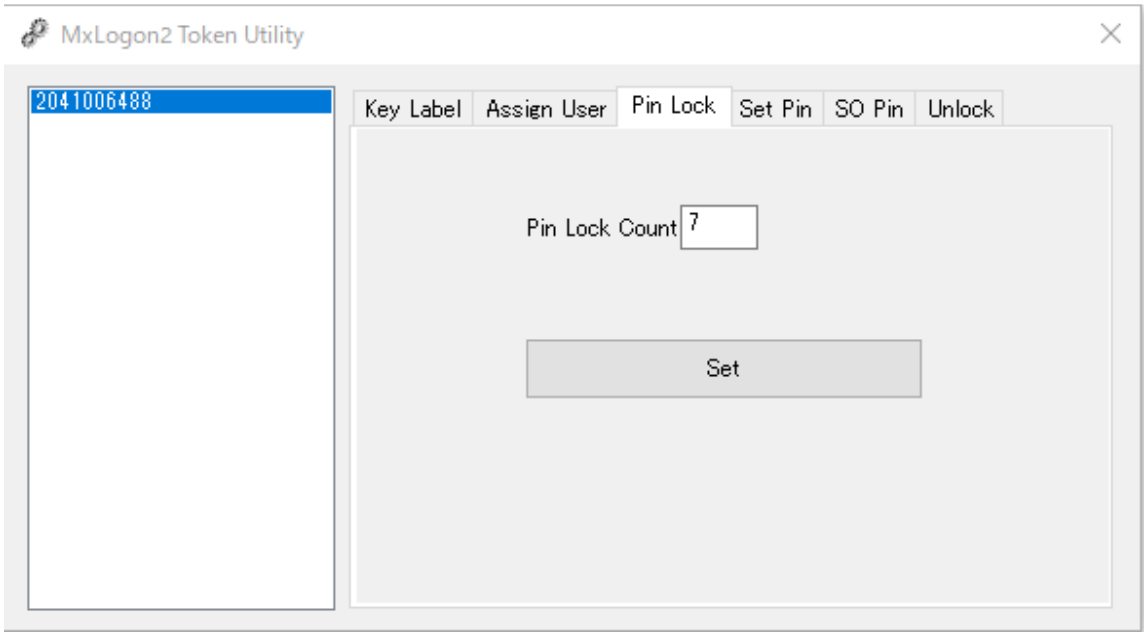


6.5 PIN Lock Count

PIN Lock count is the maximum number of successive PIN errors that you permit for PIN entry. The default is 7. When a user enters wrong PIN for this number of times straight, the USB key is locked and will not be detected as a valid key. PIN Lock is disabled when you set 0 to PIN Lock Count.

PIN errors are counted not on each Slot but across Slots. The error count on Slots accumulates. PIN error on any Slot will increment PIN error count to 1. The next PIN error on

any slot will advance the count to 2. A successful PIN entry on any Slot resets the error count to 0.



PIN is required to gain access to user credential data within a USB key. If you lose PIN, you will also lose access to the user credential of the slot. When Pin Lock is triggered, MxLogon2 will erase all the user credentials within the USB key and reset User PINs of 4 slots to their defaults. A locked key can be unlocked but unlocking will not restore the user credential nor PINs. You must re-configure the unlocked key.

6.6 User PIN and SO (Security Officer) PIN

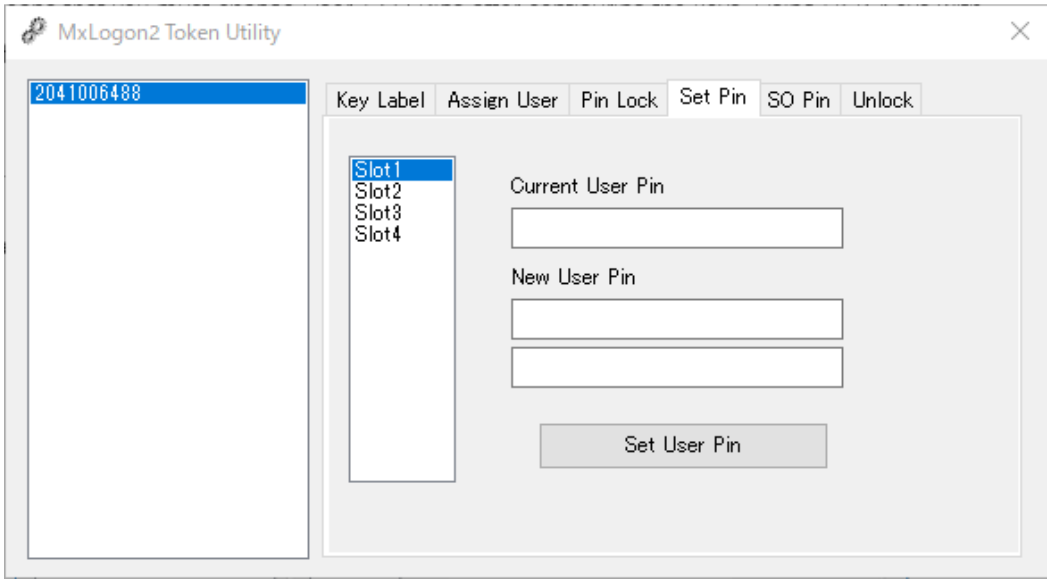
Till now, you can configure a key without entering its PIN. This is because “cert.exe” assumes that the slots are assigned the default user and the key SO PIN. If you try to configure a key with non-default PINs, you get a login error. To configure a key once released to the users, be sure to re-set the key PINs to their defaults.

Default Values

User PIN	12345678
SO PIN	admin123

6.6.1 Changing User PINs

You can set User PIN to each Slot.

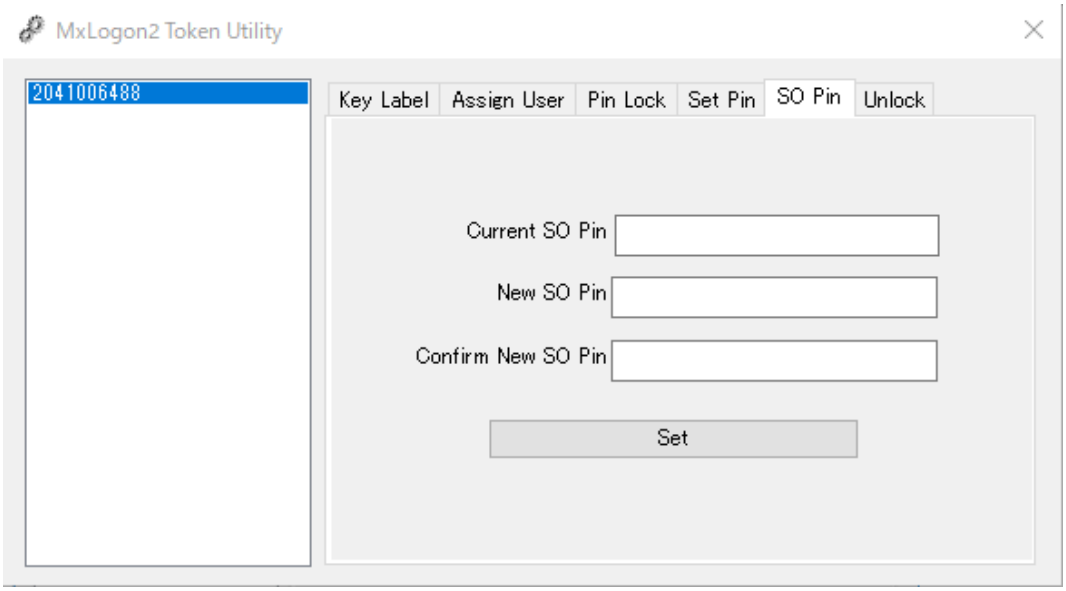


Select “User PIN” tab and change User PINs.

You can change User Pin in the login screen. In the USB key authentication screen, select a slot, enter the correct PIN and press “Change PINs” link. It will pop up a PIN change window.

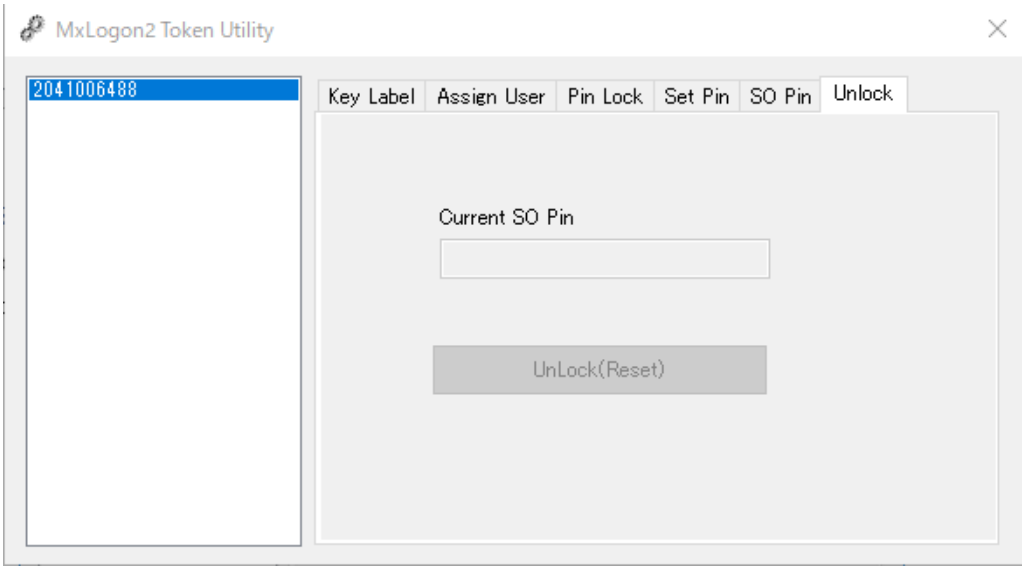
6.6.2 Changing SO PINs

Each USB key has one SO Pin. SO PIN is required to unlock / reset a key.



6.7 Unlock

To unlock a locked USB key, connect it, select “Unlock” tab and press [Unlock] button. If no locked USB key is connected, “Unlock” tab is grayed out.

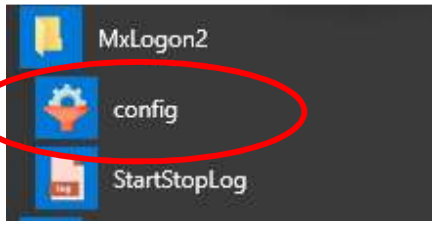


Once a key is unlocked, re-configure the key.

7. Configuring MxLogon2

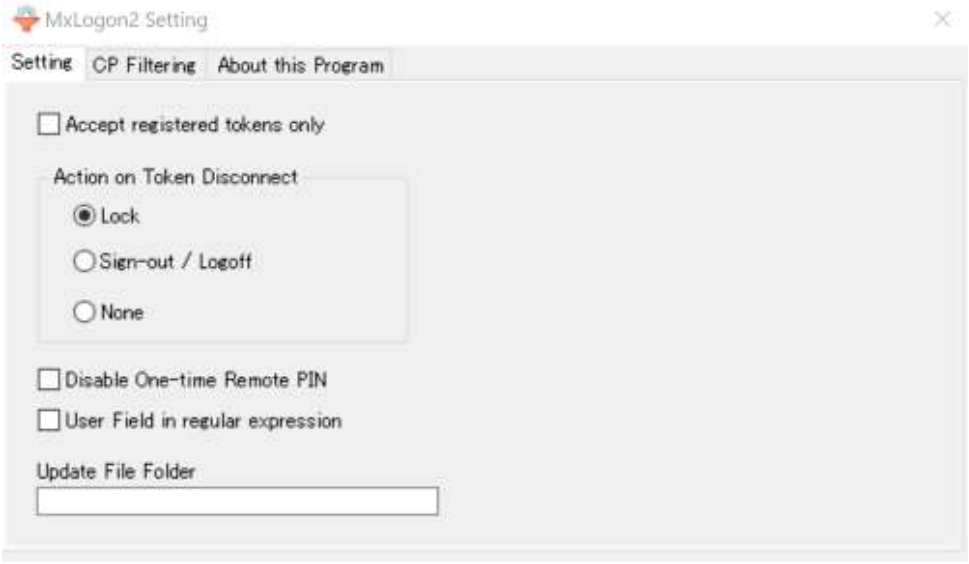
MxLogon2 installed on a computer may be configured using

- “conf” in [Start Menu]-[MxLogon2]



or

- “config.exe” in MxLogon2 installation folder; %%Program Files%%\RiBiG\MxLogon2.



7.1 Setting Tab

7.1.1 Action on USB Disconnect

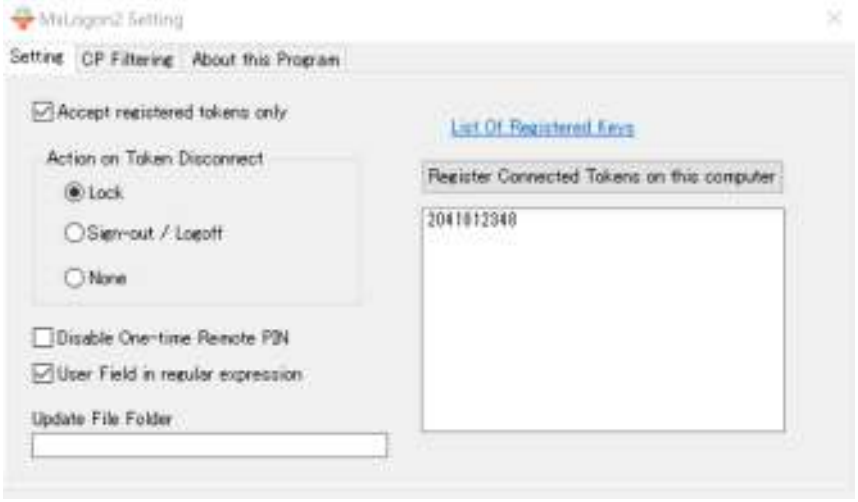
By default, MxLogon2 will lock the screen when the login USB key is unplugged. Instead of locking, it can sign out the login session or do nothing.

When sign-out is enabled, MxLogon2 will sign you out forcibly; you will lose any unsaved data upon plugging off the login key.

7.1.2 Registered Keys Only

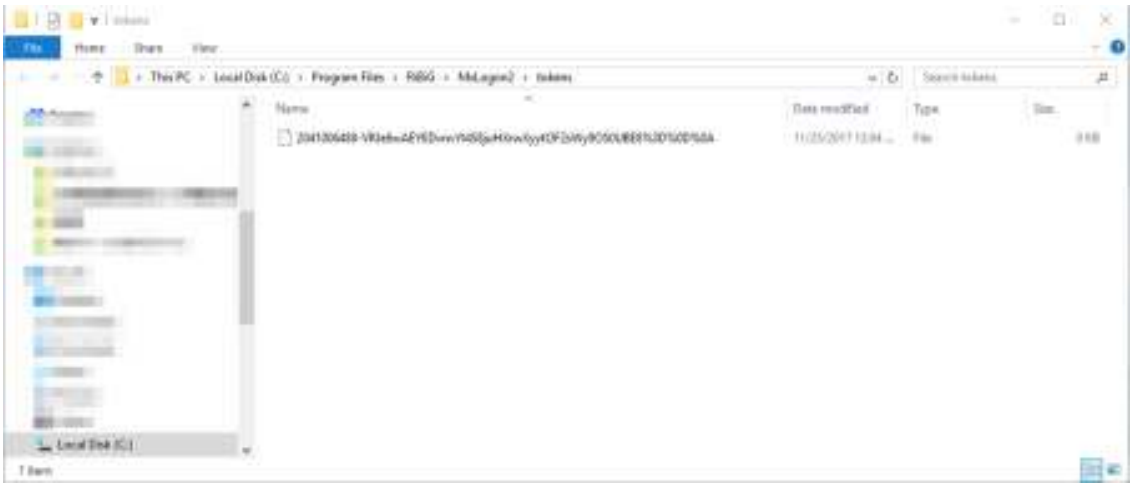
When enabled, MxLogon2 will detect only those USB keys registered on the computer; it does not show PIN entry screen when you connect a non-registered USB key.

Enabling the option will make a link, a button and a list box visible.



7.1.3 "List of Registered Keys"

When you register a key on a computer, MxLogon2 creates a file for the key under [tokens] folder in MxLogon2 installation folder. The file name begins with the key's identifier string. This link opens the folder in Explorer. Deleting a file de-register the key corresponding to the file.



7.1.4 [Register Connected Tokens on this Computer]

This button will register the detected keys in the list box on this computer.

7.1.5 How key registration works

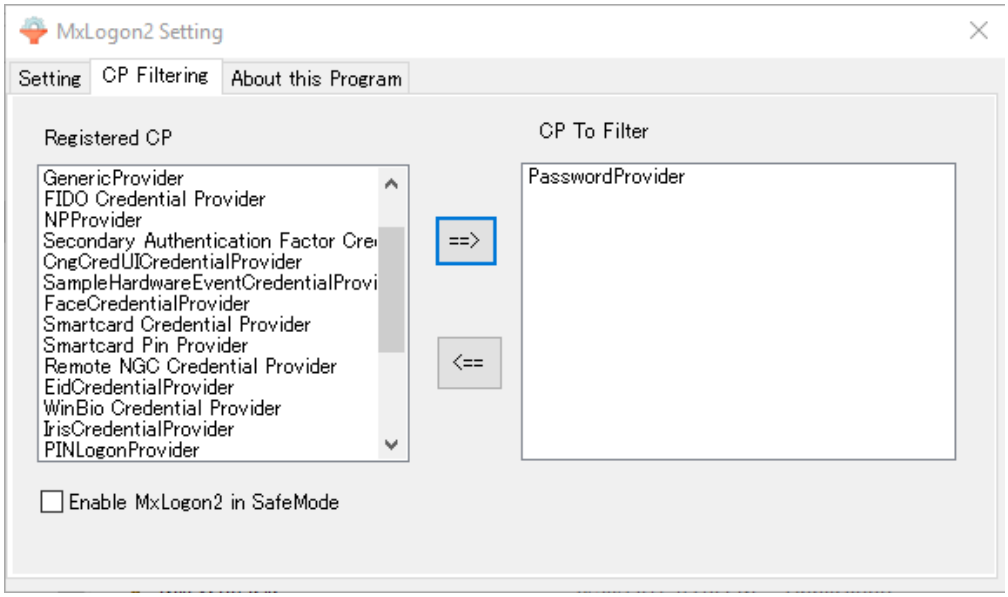
Even when “Accepted registered Tokens only” is enabled, MxLogon2 will internally disable the option when no key is registered. The option is effective only when at least one key is registered.

A key with an identifier string ending with “-master” does not have to be registered. MxLogon2 will treat such a key as “Master”.

7.2 [CP Filtering] Tab

Windows comes with a variety of credential providers. When appropriately set up, those credential providers become available in the login screen. You choose one of them to log in to Windows.

You can require users to sign in via MxLogon2 by filtering other providers. When you filter a provider, it does not appear in the login screen.



In “CP Filtering” tab, the list box on the left shows the credential providers available on the system. Select a credential provider to filter on the left list box and press [➔] button. This will move the selected item to the right list box. The CPs on the right list box will be filtered out.

To enforce USB key login on standard Windows 8/10, filter out the following CPs.

PasswordProvider

PinLogonProvider

PicturePasswordProvider

WLIDCredentialProvider

On Azure AD joined computer, filter “NGC Credential Provider” to make PIN provider hidden in the login screen.

On Windows Vista/7, filter out just PasswordProvider.

7.2.1 “Enable MxLogon2 in Safe Mode”

When you boot Windows to Safe Mode, all third-party CPs will be disabled by default and only those CPs bundled with Windows are enabled. MxLogon2 is also disabled and CP filtering is not effective. In Safe Mode, you log in by entering username/password.

Safe Mode exists for the maintenance purpose. With third-party software enabled, Windows may fail to boot. But a computer must always boot to Safe Mode successfully. Disabling third party software in Safe Mode is one of many ways to guarantee the successful boot in Safe Mode

But allowing non-USB key login in Safe Mode could become a loophole in a secure Window authentication scheme. You must make a trade-off between security and maintenance. If you opt for security, check this option to enable third-party CPs in Safe Mode. Note that this option enables not only MxLogon2 but all third-party CPS in Safe Mode.

Before turning this option for the first time, be sure that PasswordProvider is enabled in Safe Mode so that you can log in using username/password, should other providers fail to log you in. After thoroughly testing that you can sign in through MxLogon2, filter out PasswordProvider.

7.2.2 Turning On/Off “Enable MxLogon2 in Safe Mode” using USB Key

A dedicated key is available that toggles “Enable MxLogon2 in Safe Mode” option. In the login screen, select MxLogon2 and connect this key. On each connection, “Enable MxLogon2 in Safe Mode“ option will toggle; if the option is enabled, it will be turned off and vice versa.

Sound Alert

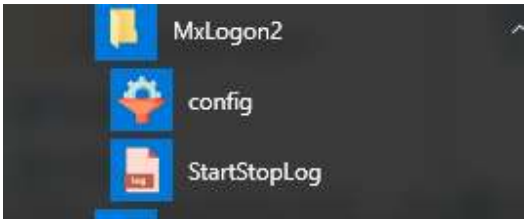
The option state changes made by the dedicated key are not visible. In order to give feed-back to the operator, MxLogon2 plays the sound file named set.wav, when the option is turned on and unset.wav when turned off. You can replace the sound files with other sound files of your choice.

%Program Files%¥RiBiG¥MxLogon2¥set.wav

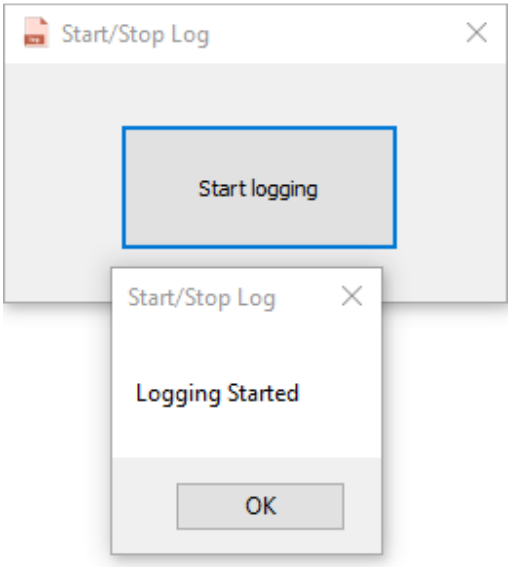
%Program Files%¥RiBiG¥MxLogon2¥unset.wav

8. Log

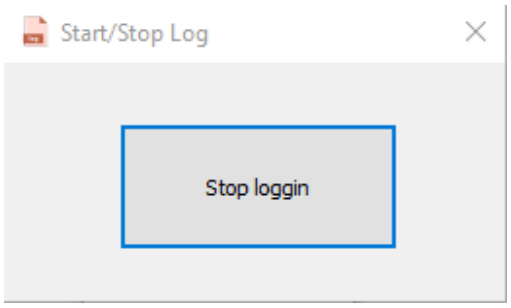
MxLogon2 does not record any log by default. To enable logging, select “StartStopLog” in Start Menu or run %Program Files%¥RiBiG¥MxLogon2¥instEvtProvider.exe. If the event viewer program is open, close it first.



Press [Start Logging] button to enable logging.



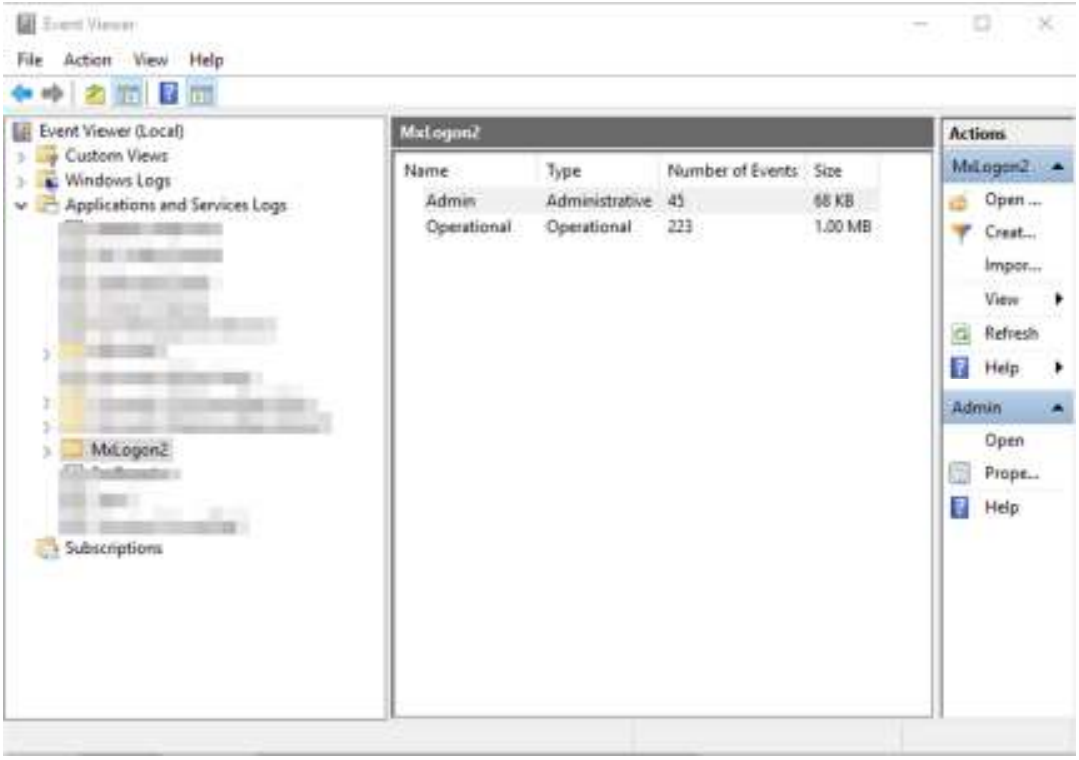
If logging is already enabled, the text on the button will be “Stop logging”. Press the button to disable logging.



8.1 Viewing Log

Open EventViewer. When logging is enabled, you will find “MxLogon2” under “Application and Service Logs” pane on the left. Select MxLogon2 and the center pane will show 2 types of logs; Admin and Operational. The operational log is the record of USB key login, logout and lock. The admin log contains warnings and errors.

Once you disable logging, MxLogon2 will not be shown in EventViewer.



9. Uninstallation

You can uninstall MxLogon2 using

Windows 10: Setting - [Apps & Features]

Windows Vista/7/8 : ControlPanel-Programs-Uninstall a program

10.Remote Desktop : USB Login to a Remote Computer

10.1 Setup

When MxLogon2 is installed on a remote computer, you can log in to it with a USB key connected locally to the client computers, provided that

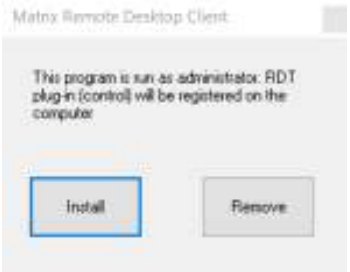
1. You use Remote Desktop client software from Microsoft
2. The plug-in software supplied with MxLogon2 is installed on the client side

> USB key login to a remote computer will not work where client computers are running 64 version of Windows Vista/7

Before setting up USB login to a remote computer, be sure that you can log in to the remote computer using username/password.

On the client side

1. Copy RDTPlugin.DLL / setupClient.exe in RDT folder in the distribution file to a folder on a fixed disk. Both files must be in the same folder. RDTPlugin.DLL will be loaded every time your run Microsoft remote desktop client. Copy to a folder that is always available, such as one on HD.
2. First, run SetupClient.exe in the elevated mode. [Register] button will make the component available. After registering the plugin, do not delete or move RDTPlgin.DLL.



3. Each user must run SetupClient.exe to enable the plugin. Users who does not run this program and register the plugin will not be able to use the local USB key for remote logins.

On the server side

4. Install MxLogon2

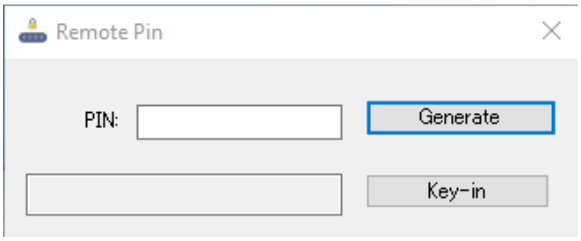
Run Microsoft remote desktop client on the client side and connect to the remote computer. When Network Level Authentication (NLA) pop up appears, enter the username and password for the remote computer.

There may be cases where the local USB keys are so configured to auto-fill the username and password and the key users are not expected to know either the username or the password. In those cases, how can they provide the remote computer credential for NLA? This will be discussed later. For now, we assume to log in using a slot without username / password auto-fill nor PIN bypass set.

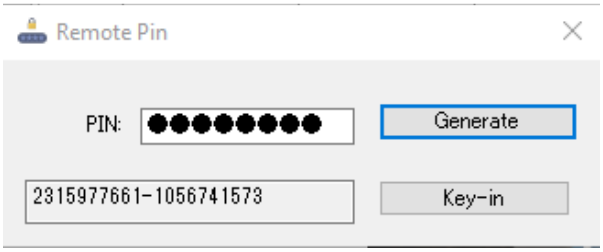
10.2 Remote Desktop PIN

The remote desktop client will display the login screen of the remote computer. If MxLogon2 is not selected, click on “Sign-in options” and select MxLogon2. If a key is connected, you can enter PIN for the key. Enter the correct PIN; you will get PIN error. In the remote mode, MxLogon2 will not accept the plain PIN. The keyboard entry in the remote desktop client screen is not considered secure. By default, MxLogon2 will accept one-time remote PIN.

You can generate a remote PIN by the tool, remotpin.exe, in [RDT] folder of the distribution file.



Enter the slot's PIN and press [Generate] button. One-time Remote Pin is generated and displayed in the gray box. You need to enter this PIN in the PIN field.

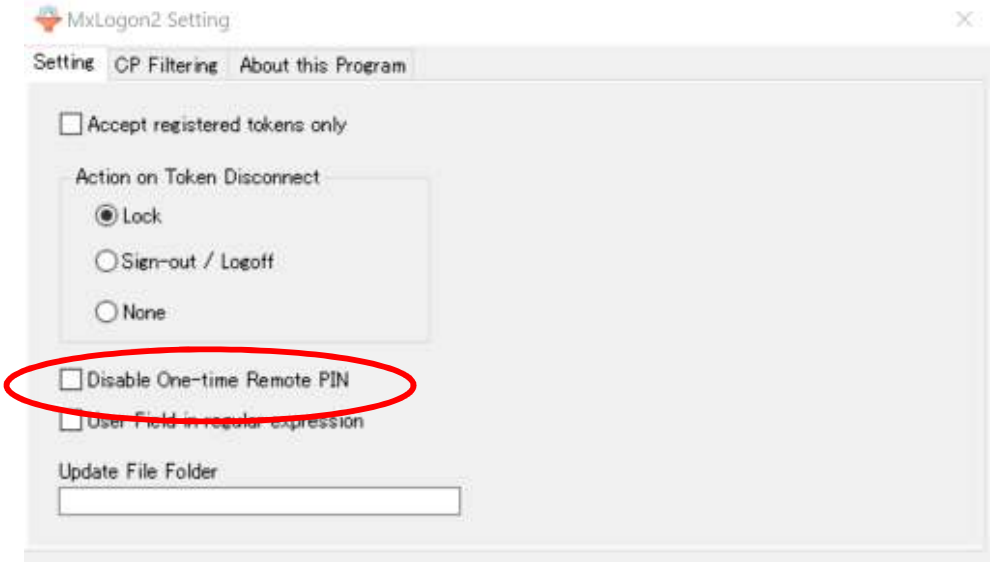


You do not have to key in this long one-time PIN manually. Pressing [Key-in] button will automatically key in the long PIN into a focused edit field. After pressing [Key-in] button, select PIN field of the remote desktop client to give it the input focus. In 5 seconds, the program will start keying in the long PIN automatically.

Once the PIN entry is completed, you will be logged in to the remote computer. MxLogon2 uses the credential you entered for NLA for the username/password authentication.

10.3 Disabling Remote Desktop PIN

You may disable one-time PIN in the remote desktop



10.4 Remote Desktop Plug-in for 32bit Windows Vista/7/2008

If the remote computer is running 32bit version of Windows Vista/7/2008, you need to install a different plugin named RDTLogon.DLL.

Server Side	Client Plugin
Windows 8/10/2012/2016 64bit Windows Vista/7	RDTPlugin.DLL / setupClient.exe
32bit Windows Vista/7	RDTLogon.DLL

*64bit Windows Vista/7 client not supported

Copy RDTLogon.DLL. (32bit or 64bit depending on the client Windows) to a folder on a fixed disk and run the following command in the command prompt.

> regsvr32 (path to RDTLogon.DLL)

This registers the plugin for the current user. Each user has to register the plugin. After registering the plug-in, do not delete or move the file.

10.5 Network Level Authentication (NLA) vs Classic Authentication

Review Appendix 1 for the difference between NLA and the classic authentication.

NLA requires you to enter the remote login credential locally. Unless you know them, you cannot connect to the remote computer. But when you have a token with the username/password auto-fill enabled, you may not know either the username or the password. In this case, you need to disable NLA and log in using the classic authentication. After connecting to the remote computer, you are asked to enter PIN unless PIN bypass is enabled. Enter a remote PIN. Once the key is authenticated, MxLogon2 will auto-fill the username/password and log you in automatically. The login credentials are sent the remote computer in the encrypted form. In this case, the class authentication is as secure as NLA.

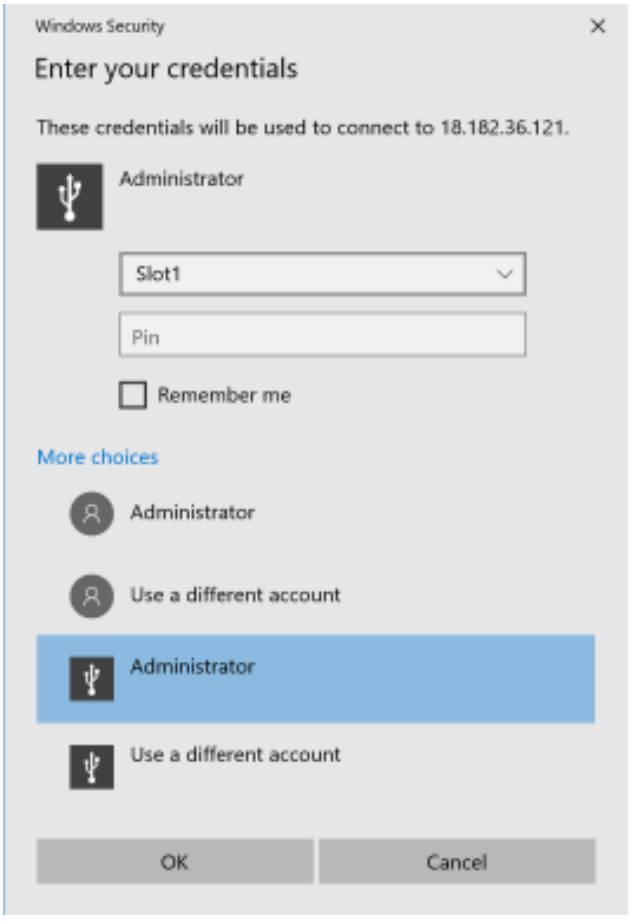
10.6 A Problem with Network Level Authentication (NLA)

After NLA is successful and you enter a remote PIN on the screen, MxLogon2 will log you in automatically using the NLA credential sent from the client. But MxLogon2 running on a version of Windows cannot receive the NLA credential from the client side. When this happens, MxLogon2 will show the username/password authentication screen after USB key verification. But you cannot key in your credential in the login screen; it is not safe. MxLogon2 provides a solution to overcome this problem and that solution is a one-for-all recipe to the remote authentication problem with MxLogon2 USB key

10.7 Installing MxLogon2 on the client for NLA

You can install MxLogon2 only for NLA purpose. For this, check “Install for Network Level Authentication only” in the setup window.

MxLogon2 will appear only in CredUI (Windows Security) window. It will not be available in the login or unlock screen.



In this window, MxLogon2 can authenticate both a USB key and a remote user before connecting to the remote host. You can safely type in PIN and user credential at the client

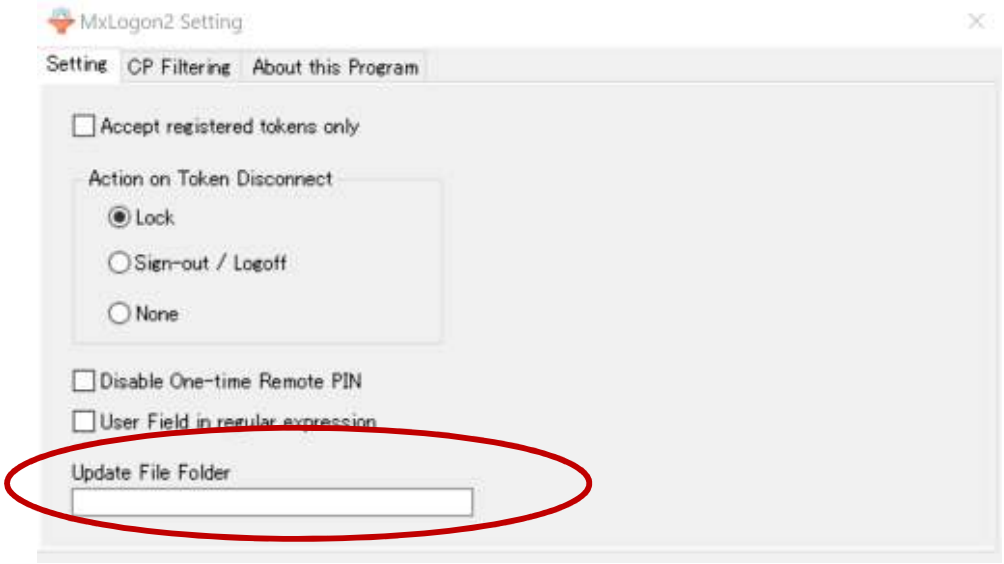
side. When the client connects to the remote host, MxLogon2 at the remote host will be able to collet the PIN and the user credential from the client in an encrypt format and securely log you in. You can use any valid USB keys, no matter how they are configured.

11. Updating MxLogon2

MxLogon2 has a built-in update feature. Just when you submit your username/password in the login screen, press [SHIFT] key. MxLogon2 looks for new files in the designated update folder. The folder can be on a local or a remote computer. When MxLogon2 finds any new files, it will install the new files replacing the installed ones. If you need to update MxLogon2 installations on multiple computers, this update feature could reduce your maintenance burden.

Setup:

1. Specify an folder where you store update files in “Setting” tab of config.exe. The folder can be on a remote computer.

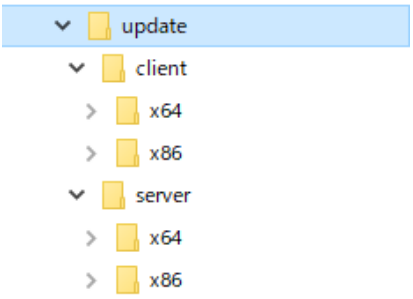


Example: Local Folder : **C:\mxlogon_update**

Remote Folder : **\\server\shared\update**

2. Place new MxLogon2 files in the update folder. It must have the following directory tree.

Example Update folder **\\server\shared\update**



This tree is the same as that contained in the distribution ZIP file. The files for 32bit client should be under [client] – [x86], 64bit client files under [client] – [x64]. Program files (EXE, DLL) as well as a setting file MxLogon2.ini and the sound files, set.wav / unset.wav, will be updated if they have more recent dates. You only place the files you want to update; no need to put the whole set of MxLogon2 files.

3. MxLogon2 tries to read the update folder with the privileges of the user who is attempting to log in in the login screen. Only those users who have the read access to the update folder can perform the update. Only the administrative users who copy new files to the update folder should have the write access.

In the login screen, when submitting username/password, press [SHIFT] key and then submit button.

MxLogon2 will read the update folder with the login user privileges. When it finds any new files, it will install them. After completing it, MxLogon2 will show the update success message and play the sound file, set.wav.

Pressing [Ok] will return you to the user authentication screen.

When MxLogon2 finds no update files, it does not show any message and logs you.

Update can only be started if a USB key is configured to have you enter username/password manually. If you have a USB key with auto-fill enabled, you cannot update MxLogon2.

12.Placing Files in the Update Folder

You can manually copy new files in the update directory tree. Only those files that have more recent date than the installed files will be updated. You must make sure that the files you copy is newer. Instead of manually copying files, you may utilize a tool included in MxLogon2. This tool is a Windows service program that periodically queries a ZIP file on our web server. When it finds a new ZIP file, it will download the file and extract its content to the update folder automatically.

12.1 ZIP File Format

It must contain the same directory tree as that of update folder. Include only those files you want to update in the ZIP file.

12.2 Upload URL

You can Upload the ZIP file in the following URL, using a valid username/password.

https://www.ribig.co.jp/mxlogon2/upload/

12.3 Installing the Windows Service, GetUpdateFile.exe

GetUpdateFile.exe can be run either as an application or as a Windows service

Run as application

Just run GetUpdate.exe

Run as Windows service

Register it as a Windows service and it will be run automatically.

>getupdatefile install

Remove it from Windows service

>getupdatefile remove

12.4 Configuration File for GetUpdateFile(GetUpdateFile.ini)

Before running GetUpdateFile, you must set the following options

1. The location of the update folder - UpdateFolder

2. Username / Password for downloading ZIP file - web_userpass

3 . If the location of the update folder is on another computer, Username/Password to access the remote computer' update folder - userpass

Optionally, you can set the time interval in minute at which GetUpdateFile queries the web server.

GetUpdateFile.ini

[options]

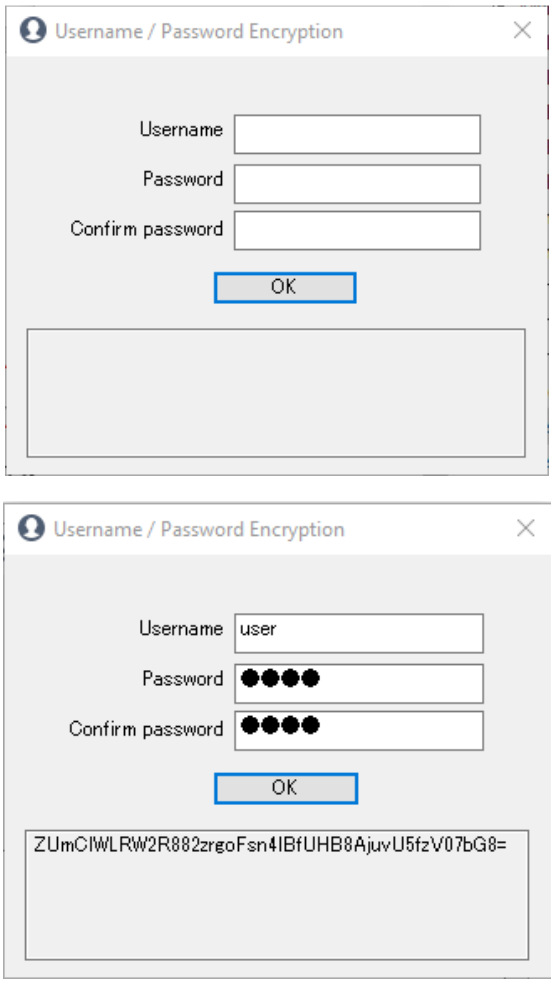
UpdateFolder=¥¥server¥shared¥update

web_userpass=lZSiZ5LgNtq5fu**********

UpdateIntervalInMin=30

userpass=QfccsvTVr**********

The values to be given to web_userpass and userpass must be encrypted strings generated by the tool, UserPass.exe.



Enter username / passwords and press [OK]. Copy the generated encrypted string in the gray box. The username for a remote computer can be down-level (domain\user) or UPN. The user must have the write permission on the update folder.

12.5 Downloaded ZIP File

After downloading the ZIP file containing update files, GetUpdateFile saves it in the same folder where it is located. Do not delete the downloaded ZIP file. GetUpdateFile compares the date of the downloaded ZIP file against the date of the ZIP on the web server to determine if the web server has a newer file.

12.6 Log file(GetUpdateFile.log)

GetUpdateFile outputs logs to the file named GetupdateFile.log in the same folder as itself.

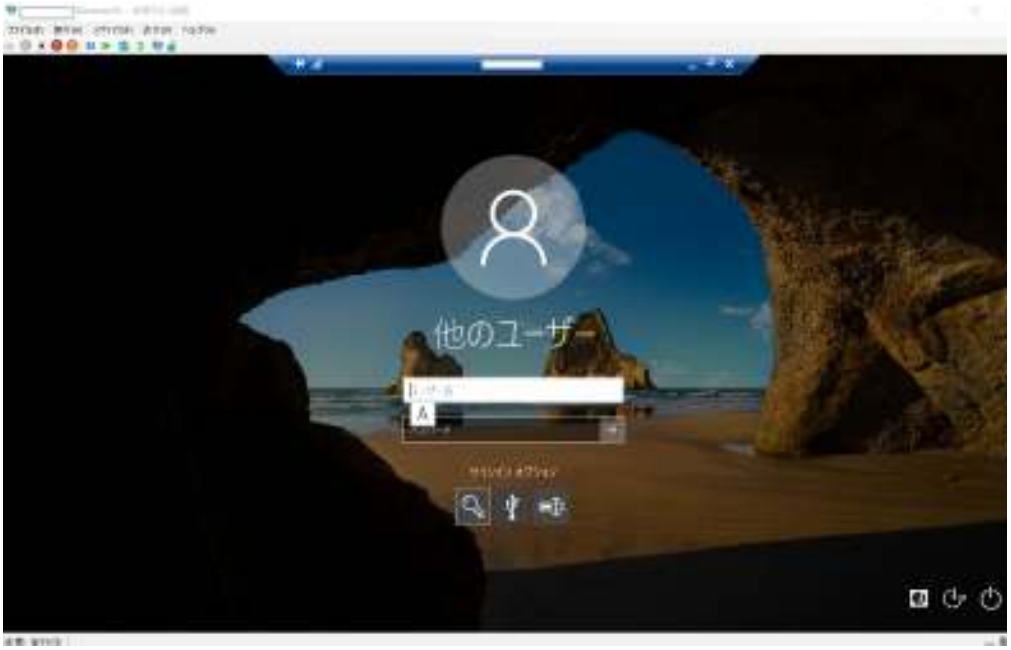
Please contact us for the details on this auto update feature.

Appendix 1. Network Level Authentication (NLA) and Classic Authentication

Classic Authentication

Run the remote desktop client and specify the remote computer.

The login screen of the remote computer will appear.

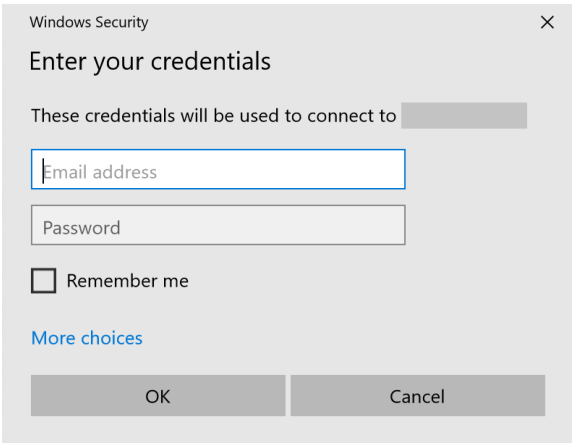


You enter your login credential in the screen.

Network Level Authentication (NLA)

Run the remote desktop client and specify the remote computer.

"Window Security" window pops up. You enter the remote computer's login credential.



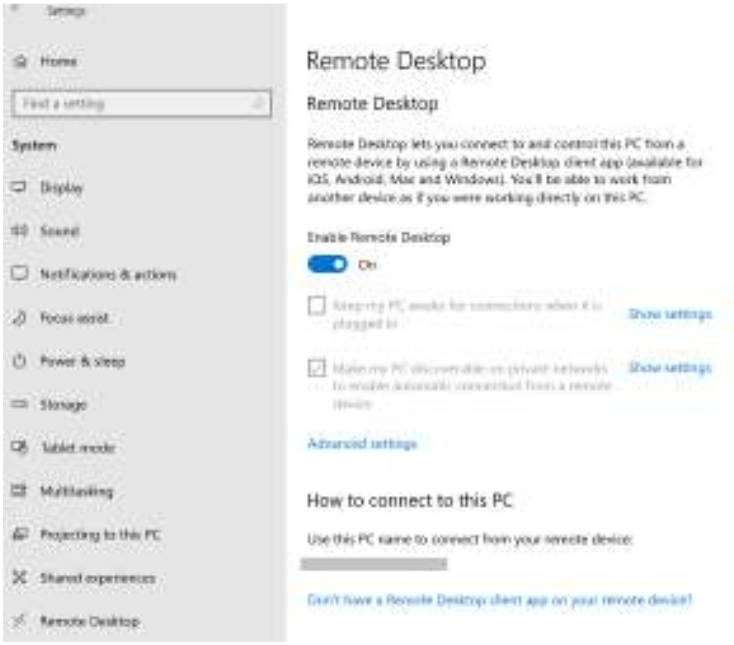
The remote computer receives the credential collected at the client side in an encrypted form and log you in automatically without showing the login screen.

NLA is safer than the classic authentication. The data you key in in the remote computer's logon screen may be visible to a third party unless the network connection is secured.

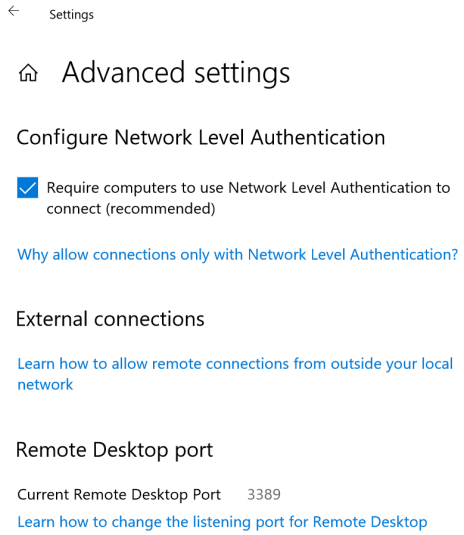
Setup to enable the remote access

Server side

Windows 10: Setting – System – Remote Desktop

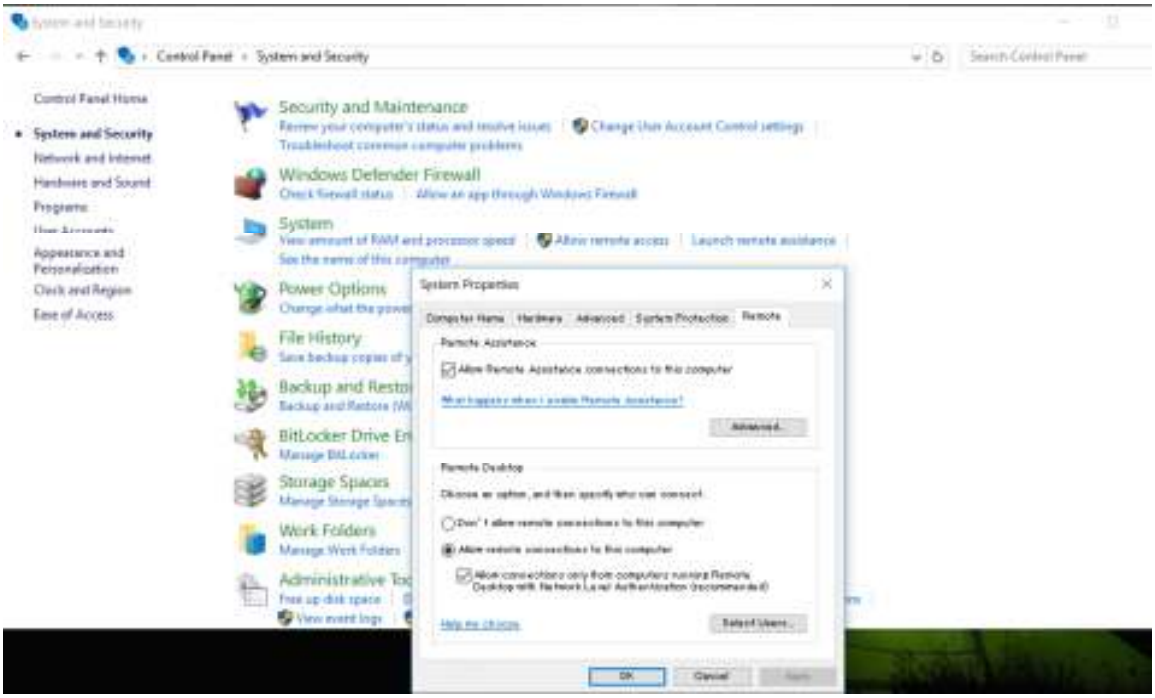


Turn on “Enable Remote Desktop”. Click on “Advanced settings”.



“Require computers to use Network Level Authentication to connect” is enabled by default. You disable this option to allow the classic authentication.

Pre-Windows 10: Control Panel – System – Allow remote access



Enable “Allow remote connections to this computer”. Uncheck “Allow connection only from computers running Remote Desktop with Network Level Authentication” to enable the classic authentication.

Client Side

The recent versions of the remote desktop client will connect to the remote computer with NLA enabled. To disable NLA connection to the server, locate the file “Default.rdp”, in your document folder. If you do not find the file or the file size is 0, run the remote desktop client and save the connection settings. For this, just click on [Save] button.

Add the following line to the bottom of the file.

```
enablecredsspsupport:i:0
```

The client will be detected as one without NLA by the remote computer. If it allows such a client, the login screen will be displayed.

When you try to allow non-NLA client at the server side, Windows shows you the warning message. If you log in through MxLogon2, you can securely log in even in the classic authentication.