IDENTIV

Identiv's Windows Login

User Guide

Before installing Identiv's Windows Login software, make sure that you know your Windows username and password for the local account. You will need this after you have rebooted, otherwise you'll be locked out of your computer.

If you have set up your Windows PC using your Microsoft account, you will need to take some additional steps to switch to a local account so that you can set up your account to login with your uTrust FIDO2 NFC+ security keys. See details here.

It is highly recommended that you configure a primary and at least one backup key for each account that you register a uTrust FIDO2 NFC+ security key for.

About

Identiv's plugin for Windows Login adds the Challenge-Response capability of the uTrust FIDO2 NFC+ as a second factor for authenticating to local Windows accounts. Identiv's Windows login application is a full implementation of a Windows Authentication Package and a Credential Provider.

This guide provides instructions for:

- Configuring uTrust FIDO2 NFC+ security keys to work with Windows Login
- Best practices for implementing Identiv's Login for Windows, such as configuring a primary and a backup key for each account

Requirements

- For each user (both admins and end-users) at least one (preferably two) uTrust FIDO2 NFC+ security keys
- Systems that are running any of the following operating systems, fully updated and for as long as they are supported by Microsoft:
    - Windows 10
    - Windows 11
- You must disable all other Sign-in options other than Password (e.g. PIN, Face, Fingerprint)

Best Practices

- Have a plan in case end-users lose their security keys, to enable them to regain access to their accounts:
    - Configure at minimum a primary and a backup uTrust FIDO2 NFC+ security key for each end-user.
    - If a user loses both keys, a new key can be added by a local administrator account.
    - Without a local administrator account, if both keys are lost, the only way of recovering is to use a recovery code.
    - Configure a recovery code for each account.
    - Ensure that the username and password for each account are available and have been tested for validity before using Identiv's Windows Login app to configure those accounts.
- Also, be aware that the only way to remove the uTrust FIDO2 NFC+ security key with Identiv's Windows Login app is to remove it from the registry manually.

Before Installation

- Before installing Identiv's Windows Login app, make a note of your Windows username and password for the local account. The person who installs the software must have the Windows username and password for their account. Without these, nothing can be configured and the account is inaccessible.
- Windows' automatic login is not compatible with Identiv's Windows Login app. If a user whose account was set up for automatic login no longer remembers their original password when the Identiv's Windows Login configuration takes effect, the account can no longer be accessed. Address this issue preemptively by:
    - Having users set new passwords before disabling automatic login.
    - Have all users verify they can access their accounts with username and their new password before you use Identiv's Windows Login to configure their accounts.
- Once Identiv's Windows Login has been configured, there is:
    - No Windows Password Hint
    - No way to reset passwords
    - No Remember Previous User/Login function.
- You can use the same key on multiple accounts on the same system.
- You can use the same key on accounts on multiple different systems, for example, if you are the admin for a small company, you might want to register your uTrust FIDO2 NFC+ security key on all user accounts to be the backup option for every end-user.

Install

1. Download Identiv's Windows Login app from here.
2. Run the installer by double-clicking on the download.
3. In the installation wizard, specify the destination folder location or accept the default location and agree to the license terms and conditions.
4. Restart the machine on which the software has been installed. After the restart, the Identiv credential provider presents the login screen that prompts for the uTrust FIDO2 NFC+ security key.
5. The Identiv credential provider (Identiv's Windows Login) requires that you enter not only the password for your local Windows account, but also the username. If necessary, consult Microsoft's instructions for switching to the local account.
6. After you have logged in, search for the "uTrust Windows Login" folder in the quick start applications list. You will find the uTrust FIDO GUI here.

Configuring Windows Login

Only accounts that are supported can be configured for Identiv's Windows Login. If you launch the configuration wizard, and the account you are looking for is not displayed, it is not supported and therefore not available for configuration.

Primary and Backup Keys

Use a different uTrust FIDO2 NFC+ security key for each registration. If you are configuring backup keys, each user should have one uTrust FIDO2 NFC+ security key for the primary and a second one for the backup key.

Recovery Code

A recovery code is a last-resort mechanism to authenticate a user if all uTrust FIDO2 NFC+ security keys have been lost. Recovery codes can be assigned to the users you specify; however, the recovery code is only usable if the username and password for the account are also available. The option to generate a recovery code is presented during the configuration process. Please note that Identiv's Windows Login software asks for recovery key generation upon every token enrollment, but there is only one recovery key per user account. So, when a second token is enrolled and the user opts to generate a recovery key, the first key is overwritten.

Specify Configuration

The Login Manager lists the local accounts available for selection, from which you can select and deselect user accounts to enable, allowing you to register a key or keys for each account.

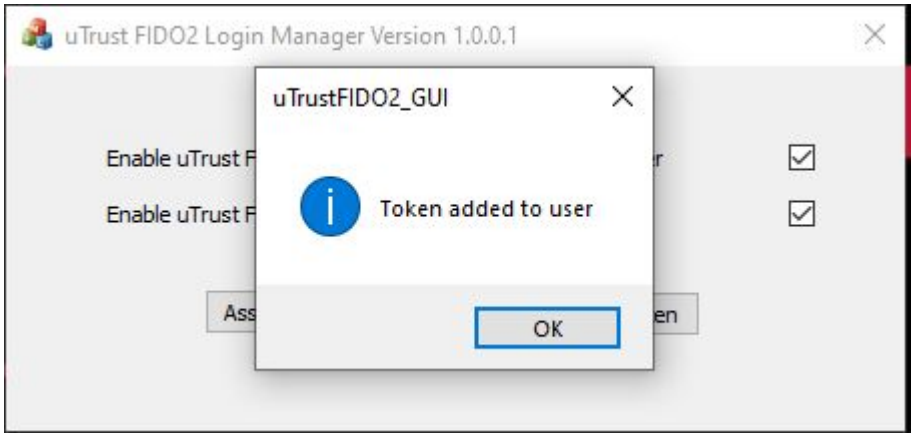
This tool can be run as often as necessary. You can also add additional uTrust FIDO2 NFC+ security keys for users already configured for Identiv' Windows Login.

You will need to insert a uTrust FIDO2 NFC+ security key for Identiv' Windows Login to proceed with configuration.

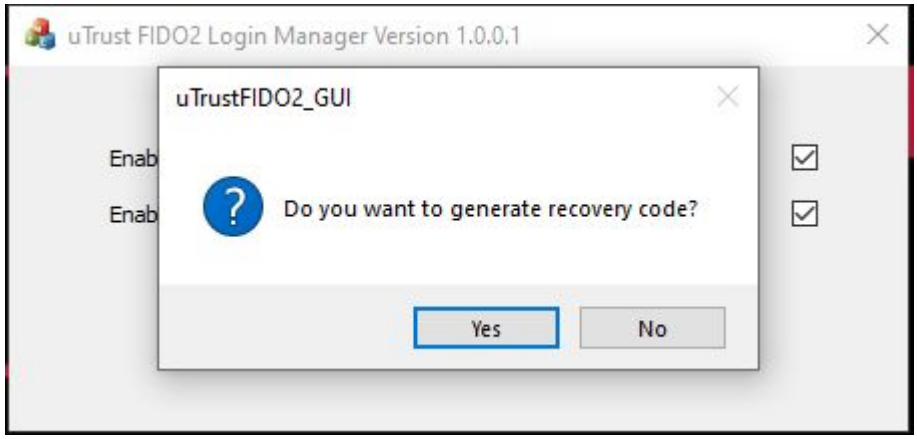
1. User Accounts appear, as shown in the screenshot below. If there are no local user accounts supported by Identiv' Windows Login, the list will be empty.

Note: You can add additional uTrust FIDO2 NFC+ security keys for users already configured by selecting the users here.

2. On the page shown above, select the user accounts to be associated with the security key during the current run of the Identiv' Windows Login by selecting the checkbox next to the username, and then click “Associate Token”. A “Token Added” alert will appear as shown below.



3. After the uTrust FIDO2 NFC+ security key for the specified user account has been enabled you will be prompted to Generate a Recovery Code as shown below.*



*Note: When a second token is enrolled and the user opts to generate a recovery key, the first key is overwritten.

4. It is recommended that you generate and save a recovery code in the event your security keys are lost. After clicking the "Yes" button, your code will be displayed. You should write down or save an image of this code and keep it in a secure location before proceeding.

Logging In

When the local user account has been configured to require a uTrust FIDO2 NFC+ security key, the user is authenticated by the Identiv Credential Provider instead of the default Windows Credential Provider. The user is prompted to insert their uTrust FIDO2 NFC+ security key. Then Identiv's Windows Login screen is presented. The user enters their username and password.

Note: It is not necessary to press the button on the uTrust FIDO2 NFC+ security key to log in. In some instances, pressing the button actually causes the login to fail.

Attempts to Log In Without uTrust FIDO2 NFC+ security key

When the end-user logs in, they must insert the correct uTrust FIDO2 NFC+ security key into a USB port on their system. If the end-user enters their username and password without inserting the correct uTrust FIDO2 NFC+ security key, authentication will fail and the user will be presented with an error message.

Login With Recovery Code

If an end-user's account is configured for Identiv' Windows Login, and if a recovery code was generated, and a user loses their uTrust FIDO2 NFC+ security key(s), they can use their recovery code to authenticate. The end-user unlocks their computer with their username, recovery code, and password.

Until a new uTrust FIDO2 NFC+ security key is configured, the end-user must enter the recovery code each time they log in.

Changing the Password

Changing the password works the same as with the default Windows Credential Provider.

Troubleshooting

uTrust FIDO2 NFC+ security key not detected

If Identiv' Windows Login does not detect that a uTrust FIDO2 NFC+ security key has been inserted, it is likely you are not inserting a uTrust FIDO2 NFC+ security key, but instead a Security Key, which is not compatible with this application.

Error Enabling a uTrust FIDO2 NFC+ security key

An error alert may appear when you select a user account. This typically indicates that another Windows sign-in option is enabled for the particular account. The key will still register with the account, but login using the uTrust FIDO2 NFC+ Security Key will not be enforced until all other sign-in options are disabled.

Able to log in using sign-in options other than Identiv's Windows Login after provisioning

Windows sign-in options beginning with Windows Hello (e.g. Windows Hello PIN), as well as the Picture Password sign-in option will allow a user to log in to Windows without their uTrust FIDO2 NFC+ security key, even if a requirement has been established with Identiv' Windows Login. It is recommended to disable Windows Hello/Picture Password sign-in options on accounts that are protected by Identiv' Windows Login.