privacyIDEA Credential Provider Documentation

Release 2.2

NetKnights GmbH

Mar 29, 2020

Contents

Contents:

Introduction

The privacyIDEA Credential Provider is a tool to improve the logon security of your Windows Desktops, Servers and Windows Terminal Servers. It is used to add a second factor for authentication, when logging into your Windows system.

The privacyIDEA Credential Provider does this by communicating with the privacyIDEA Authentication System[1]. The privacyIDEA Authentication System can manage many different kind of second factors for the domain users. Ranging from classical OTP tokens, one time codes via SMS, Smartphone Apps to the Yubikey.

Users need to authenticate with their windows password and additionally with their token as second factor.

---

[1] https://privacyidea.org

Installation

2.1 Prerequisites

To use the privacyIDEA Credential Provider you need to have a privacyIDEA Authentication System. The installation and setup of this backend is covered in another documentation[1].

Ask the company NetKnights to get an evaluation version of the privacyIDEA Credential Provider[2].

2.2 MSI package

The privacyIDEA Credential Provider comes as a 32bit and 64bit MSI package. You can install it manually or use your software distribution tool.

2.2.1 Start installation

In the first step you can decide, if you want to make the privacyIDEA Credential Provider the default provider. This means, that no other credential provider is active on this machine. The user can not login with only his Windows password anymore.
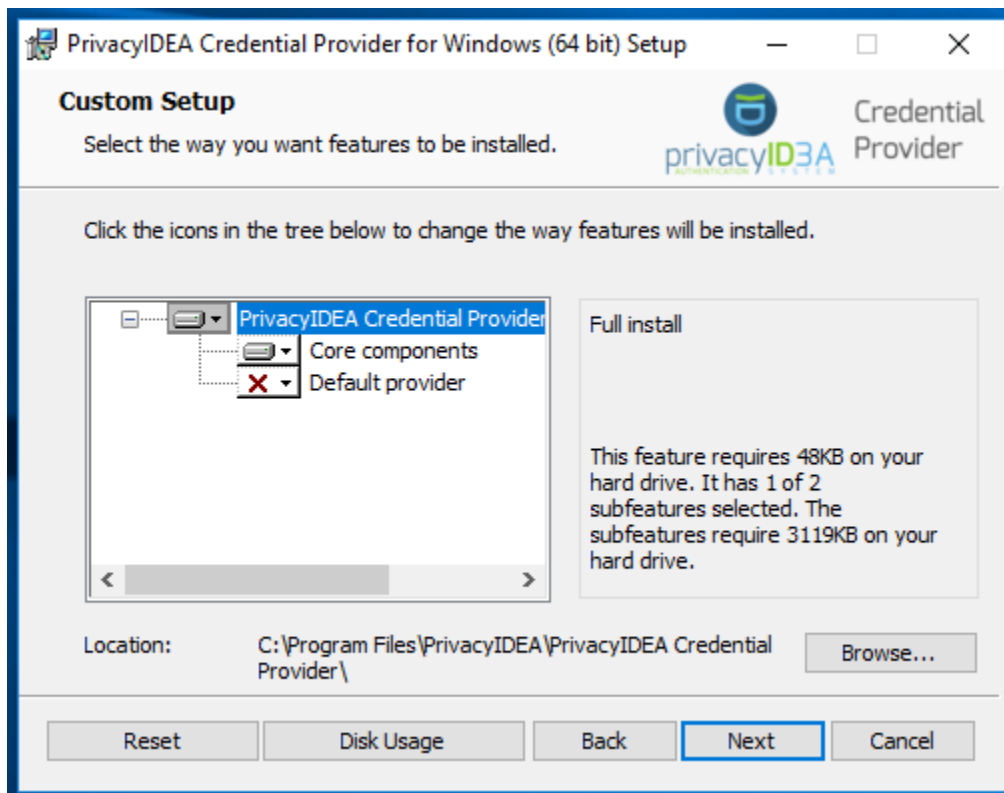
Note: We recommend not activating this setting during installation. First you should configure the privacyIDEA Credential Provider and check, if it works right. After this, you can change the installation and change this configuration.

2.2.2 Configure the privacyIDEA Authentication Server

In the next step, you can configure the communication to the privacyIDEA Authentication Server. The credential provider and the server communicate via the REST API `POST /validate/check`.

---

[1] http://privacyidea.readthedocs.io/en/latest/installation/index.html
[2] https://netknights.it/en/unternehmen/kontakt/

Note: You only need to specify the hostname of the authentication server. In most cases you only need to enter the hostname like *yourserver.example.com*. Additionally the path can be specified if there is. Something like */path/to/pi*.

You can specify a custom **login text**, which will be displayed underneath the provider.

You can also specify if certain SSL errors shall be ignored.

Warning: We recommend NOT to ignore any SSL errors in productive use. Otherwise you will be vulnerable to man-in-the-middle attacks. An attacker who intercepts the communication could modify the authentication response and thus make the second factor useless.

You may specify the path to a custom login image.

Note: The image must be a BMP version 3 file.

After these two steps the privacyIDEA Credential Provider is installed on your system and can be chosen for login.
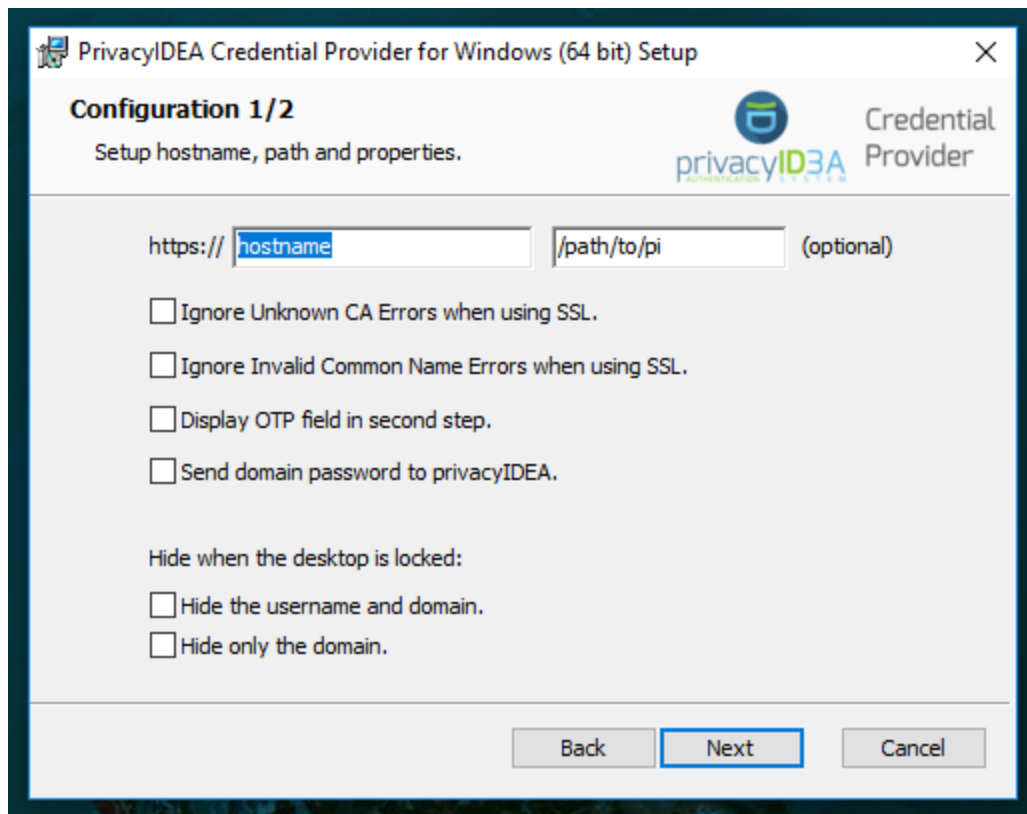
Configuration

During installation of the privacyIDEA Credential Provider you already configured all necessary settings, but it can be interesting to change settings later. Like changing the available credential providers or changing the verification of the authentication server certificate.

3.1 Registry Settings

If you want to change the configuration after the installation, you can only do this by editing the registry keys. You can use administrative templates to deploy the credential provider on many desktops in your network.

The configuration is located at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\NetKnights GmbH\PrivacyIDEA-CP\`.

3.1.1 Connection Settings

These settings define the connection to the privacyIDEA server. The connection is established via https by default, like indicated in the installer.

hostname

The hostname of the privacyIDEA Authentication Service. That usually is something like *yourserver.example.com* without any additional path information.

path

Optional. The path to the privacyIDEA Authentication Service if there is. E.g. */test/path/pi*

NOTE: The entry */path/to/pi* is a placeholder. If it is read by the Credential Provider, it is treated as an empty entry.

ssl_ignore_invalid_cn

Set to `1` if the privacyIDEA Credential Provider should ignore SSL errors originating from an invalid common name.

ssl_ignore_unknown_ca

Set to `1` if the privacyIDEA Credential Provider should ignore SSL errors originating from an unknown CA.

custom_port

This entry is not there by default. You can add it to declare a custom port. The value has to be of type *REG_SZ* with the name *custom_port*.

NOTE: By default the port is the default https port, which is 443.

3.1.2 Login behaviour

Using these settings you can specify the behaviour of the privacyIDEA Credential Provider. The credential provider can ask for the username, the password and the otp value in one step or in two steps.

two_step_hide_otp

Set to 1 if the privacyIDEA Credential Provider should ask for the user's OTP in a second step. In the first step the user will only be asked for the password.

two_step_send_password

Set to 1 if the privacyIDEA Credential Provider should send the user's password to the privacyIDEA Authentication Service.

two_step_send_empty_password

Set to 1 if the privacyIDEA Credential Provider should send an empty password to the privacyIDEA Authentication Service.

NOTE: If both **two_step_send_password** and **two_step_send_empty_password** are set to 1, the privacyIDEA Credential Provider will send an empty password to the privacyIDEA Authentication Service. NOTE: Sending the windows or an empty password can be used to trigger token types like SMS or Email.

3.1.3 Recommended setup for remote desktop scenarios

In scenarios where the privacyIDEA Credential Provider shall be used for RDP connections, it is recommended to install the privacyIDEA Credential Provider only on the RDP target together with the Filter. It is also recommended to use the *two_step_hide_otp* setting to skip entering the windows password a second time.

3.1.4 Customization of the Look and Feel

You can also change the look and feel of the privacyIDEA Credential Provider.

login_text

Specify the text, that is displayed underneath the credential provider logo.

otp_text

Speficy the text, that is displayed in the OTP input field. Usually this is "One-Time Password", but you can change it to any other value you like.

hide_domainname

Set to 1 if you want the privacyIDEA Credential Provider to hide only the domain name when the desktop is locked.

hide_fullname

Set to 1 if you want the privacyIDEA Credential Provider to hide the user and domain name when the desktop is locked. Instead only the contents of the *login_text* settings will be displayed.

v1_bitmap_path

The complete path and filename of a bitmap image. This is a customized login image. The image must be a version 3 Windows BMP file with a resolution of 128x128 pixels.

no_default

Add this registry entry and set it `1` to not have the privacyIDEA Credential Provider selected by default when logging in.

3.1.5 Log file

release_log

Set to `1` if you want the privacyIDEA Credential Provider to write a logfile in the release version. The log only contains errors and is located at C:\privacyIDEAReleaseLogFile.txt.

The log file of the debug version contains more detailed information and is located at C:\privacyIDEADebugLogFile.txt

log_sensitive

In some cases it can be useful to log sensitive data (e.g. passwords) to find the cause of a problem. By default sensitive data is not logged. To log sensitive data aswell, create a new registry key of type *REG_SZ* with the name *log_sensitive* and a value of *1*. This can be deleted after creating a logfile. NOTE: This only affects the *debug* versions of the privacyIDEA Credential Provider.

3.1.6 Other

sleep On some windows machines the credential provider freezes after the first step when using *only* the *two_step_hide_otp* configuration. Adding this key with a value of `1` solves this issue.

Development, Maintenance and Support

The privacyIDEA Credential Provider was first developed by Last Squirrel IT[1]. The company has a long experience in Microsoft Windows security tools. They developed many different credential providers and plugins for Active Directory Federation Services.

Since 2018 the development is continued by NetKnights. You will get maintenance and support via the company NetKnights[2]. NetKnights also maintains the privacyIDEA Authentication System and issues different service level agreements[3] for the privacyIDEA Credential Provider and the privacyIDEA Authentication System.

---

[1] http://www.lastsquirrel.com
[2] https://netknights.it
[3] https://netknights.it/en/produkte/privacyidea-credential-provider/

CHAPTER 5

Indices and tables

- genindex
- modindex
- search