

THALES

SafeNet MiniDriver

USER GUIDE



Document Information

Document Information

Product Version	10.9 R1 (GA)
Document Number	007-001799-002
Release Date	October 2024

Revision History

Revision	Date	Reason
Rev. C	October 2024	Updated for 10.9 R1 (GA) release

Trademarks, Copyrights, and Third-Party Software

2024 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and affiliates, and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and any of its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any information of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”).

This document can be used for informational, non-commercial, internal, and personal use only provided that:

- > The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Thales Group.

CONTENTS

Document Information	2
Preface: About this Document	5
Audience	5
Document Conventions	5
Command Syntax and Typeface Conventions	5
Notifications and Alerts	6
Support Contacts	7
Chapter 1: Introduction	1
Chapter 2: Token Management	2
Prerequisite	2
Changing the Token Password	2
Unlocking a Token by the Challenge-Response Method	4

PREFACE: About this Document

This document describes the operational and administrative tasks you can perform to maintain the functionality and efficiency of your SafeNet MiniDriver.

This section also identifies the audience, explains how to best use the written material, and discusses the documentation conventions used. They are:

- > ["Audience" below](#)
- > ["Document Conventions" below](#)
- > ["Support Contacts" on page 7](#)

For information regarding the document status and revision history, refer to ["Document Information" on page 2](#).

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

It is assumed that the users of this document are proficient with security concepts.

Document Conventions

This section describes the conventions used in this document.

Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Format	Convention
bold	The bold attribute is used to indicate the following: > Command-line commands and options that you enter verbatim (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Dialog box titles (On the Protect Document dialog box, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italics</i>	In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Represent optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{a b c} {<a> <c>}	Represent required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[a b c] [<a> <c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

Tips

Tips are used to highlight information that helps to complete a task more efficiently.

TIP This is some information that will allow you to complete your task more efficiently.

Notes

Notes are used to highlight important or helpful information.

NOTE Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

CAUTION! Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

****WARNING**** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#).

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone

The support portal also lists telephone numbers for voice contact ([Contact Us](#)).

CHAPTER 1: Introduction

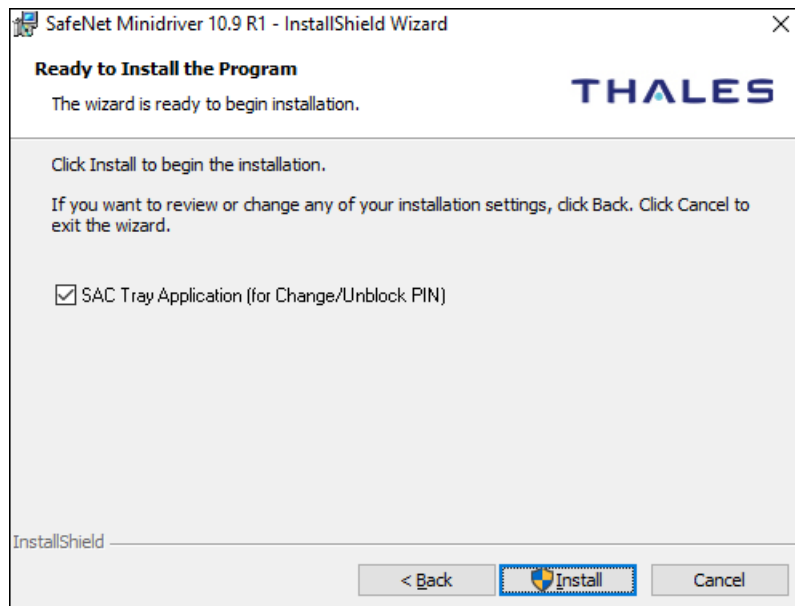
SafeNet MiniDriver is a simple alternative to developing a legacy cryptographic service provider (CSP) by encapsulating the complex cryptographic operations from the card MiniDriver vendor.

SafeNet Minidriver presents a consistent interface between Thales PKI authenticators and Microsoft's Smart Card Base Cryptographic Service Provider (CSP) or Crypto Next Generation (CNG) Key Storage Provider (KSP) and to the Smart Card Management Interface.

CHAPTER 2: Token Management

Prerequisite

To get the token management options, during SafeNet MiniDriver installation, select the **SAC Tray Application (for change/unblock PIN)** check box.



Changing the Token Password

NOTE The term *Token Password* may be replaced by another term (for example, *Token PIN*), depending on your configuration.

SafeNet eTokens are supplied with an initial default token password. In most organizations, the initial token password is **1234567890**.

IDPrime cards are supplied with an initial default token password: **0000**.

To ensure strong, two-factor security, it is important for the user to change the initial default token password to a private password as soon as the new token is received.

When a token password is changed, the new password is used for all token applications. It is the user's responsibility to remember the token password. Without it, the token cannot be used.

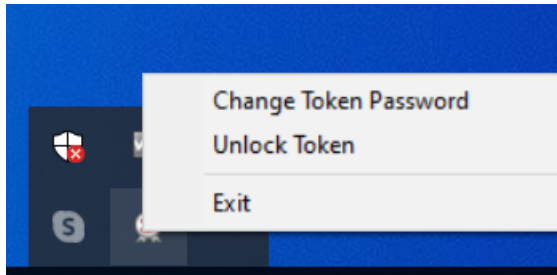
TIP The token password is an important security measure in safeguarding your company's private information. The best passwords are at least eight characters and include upper-case and lower-case letters, special characters such as punctuation marks, and numbers appearing in random order.

It is recommended not to use easily discovered passwords, such as names or birth dates of family members.

Perform the following steps to change a token's password:

1. Do the following to change the token password using the tray menu:

- a. Right-click the **SafeNet Authentication Client** tray icon.



- b. If more than one token is connected, hover over the following icon and select the appropriate token



- c. Select **Change Token Password**.
- d. Continue with step 4.

The **Change Password** window is displayed.

Change Password: My Token

SafeNet Authentication Client THALES

Current Token Password:

New Token Password:

Confirm Password:

The new password must comply with the quality settings defined on the token.

A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

Current Language: EN

Enter your current password.

OK Cancel

2. Enter the current token password in the **Current Token Password** field.

NOTE If an incorrect password is entered more than a pre-defined number of times, the token becomes locked.

3. Enter a new token password in the **New Token Password** and **Confirm Password** fields.

NOTE As you type a new password, the password quality indicator on the right displays a percentage score of how well the new password matches the password quality requirements.

4. Click **OK**.

A message confirms that the token password is changed successfully.

5. Click **OK**.

Unlocking a Token by the Challenge-Response Method

NOTE This feature is disabled for IDPrime SIS 840, IDPrime 940 SIS, and IDClassic 410 cards.

If an incorrect token password is entered more than a pre-defined number of times, the token becomes locked.

Tokens can be unlocked if, and only if, an Administrator Password was set during initialization.

NOTE

The unlock feature is supported by eToken and IDPrime devices.
For Common Criteria devices, the new user password is used for both the token password and Digital Signature PIN when unblocking a device.

When the administrator has access to the user's token, the administrator can unlock the token using the *Set Token Password* feature.

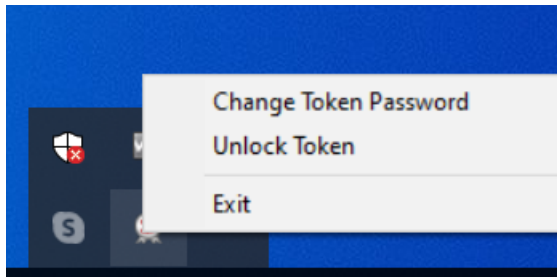
Another way to unlock the token and set a new token password is to use the Challenge – Response authentication method. The user sends the administrator the Challenge Code supplied by SAC Tray, and then enters the Response Code provided by the administrator. The token becomes unlocked, and the new token password set by the user replaces the previous password.

NOTE Unlocking the User PIN via the Challenge-Response method is not supported on Common Criteria cards when the User PIN is protected by the PUK.

Perform the following steps to unlock a token using the Challenge-Response method:

1. Do the following to change the token password using the tray menu:

- a. Right-click the **SafeNet Authentication Client** tray icon.



- b. If more than one token is connected, hover over the following icon and select the appropriate token.



- c. Select **Unlock Token**.
 - d. Continue with step 4.
2. The **Unlock Token** window is displayed, displaying a value in the **Challenge Code** field.

The *Challenge Code* is 16 characters or, if the token was initialized as Common Criteria, 13 characters.

Unlock Token: My Token

SafeNet Authentication Client THALES

Challenge Code: 1C 7A 8B EF EB E0 77 72

Response Code:

☐ Token Password must be changed on first logon

New Password:

Confirm Password:

The new password must comply with the quality settings defined on the token.
A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

Current Language: EN

Enter the Response Code provided by your administrator.

OK Cancel

3. Contact your administrator, and provide the administrator with the Challenge Code value displayed.

NOTE To copy the Challenge Code to the clipboard, click the **Copy to Clipboard** icon.

CAUTION!

- After providing the Challenge Code to the administrator, do not undertake any activities that use the token until you receive the Response Code and complete the unlocking procedure.
- If any other token activity occurs during this process, it affects the context of the Challenge – Response process and invalidate the procedure.
- For IDPrime devices only: - During the unlock operation, any application that attempts to connect to the device is suspended until the unlock operation is completed or canceled.

4. Enter the **Response Code** provided by the administrator.

The Response Code is 16 characters or, if the token is initialized as Common Criteria, 39 characters.

NOTE Response Code creation depends on the back-end application being used by the organization. Administrators should refer to the relevant documentation for information on how to generate the Response Code.

5. Enter a new token password in the **New Password** and **Confirm Password** fields.
6. If the new password is known to others and must be changed, select **Token Password must be changed on first logon**.

7. Click **OK**.

A message confirms that the token is unlocked successfully.

8. Click **OK**.