MyID PIV

Version 12.13

MyID Client for Mac

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: IMP2044-12.13.0-PIV

December 2024

Copyright

© 2001-2024 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

Apache log4net

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

Microsoft .NET

The MIT License (MIT)

Copyright © 2019 Microsoft

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Microsoft .NET MAUI

The MIT License (MIT)

Copyright © .NET Foundation and Contributors

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MauiIcons

MIT License

Copyright © 2022 AathifMahir

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

.NET MAUI Community Toolkit

The MIT License (MIT) Copyright © .NET Foundation and Contributors All Rights Reserved

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

.NET MAUI Markup Community Toolkit

The MIT License (MIT) Copyright © .NET Foundation and Contributors All Rights Reserved

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

.NET Community Toolkit

Copyright © .NET Foundation and Contributors

All rights reserved.

MIT License (MIT) Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED AS IS, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LocalizationResourceManager.Maui

MIT License

Copyright © 2023 Johan Svensson

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SkiaSharp

Copyright © 2015-2016 Xamarin, Inc. Copyright © 2017-2018 Microsoft Corporation.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SkiaSharp.Extended

MIT License

Copyright © 2015-2016 Xamarin, Inc. Copyright © 2017-2020 Microsoft Corporation.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

  For example:
  - Record a valid email address in **'From' email address**.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

  Warning: You must take a backup of your database before making any changes to it.

Contents

MyID Client for Mac **1**
Copyright **2**
Conventions used in this document **10**
Contents **11**
1 Introduction **13**
1.1 Architecture 13
1.2 Limitations 14
1.2.1 Changes since the beta version 14
1.3 Differences between the MyID Client for Mac and MyID Client for Windows 15
2 Installing and uninstalling the MyID Client for Mac **16**
2.1 System requirements 16
2.1.1 Supported client operating systems 16
2.1.2 Supported MyID versions 16
2.1.3 Supported devices 17
2.1.4 Supported smart card readers 17
2.2 Installing the MyID Client for Mac 18
2.3 Uninstalling the MyID Client for Mac 23
2.3.1 Uninstalling the MyID Client for Mac from the Applications folder 23
2.3.2 Uninstalling the MyID Client StatusBar Service 24
2.3.3 Uninstalling the MyID Client for Mac using the provided script 25
3 Configuring MyID CMS for the MyID Client for Mac **26**
3.1 Configuring access to actions 26
3.2 Setting up self-service device update 27
3.3 Configuring access to tasks 27
4 Launching the MyID Client for Mac **28**
4.1 Switching users 30
4.2 Launching the MyID Client for Mac from the MyID Client StatusBar Service 31
4.2.1 Launching the MyID Client for Mac from a notification 31
4.2.2 Checking for updates 32
4.2.3 Troubleshooting 32
4.3 Launching the MyID Client for Mac from a hyperlink 33
4.4 Keyboard shortcuts 34
5 Checking for device tasks **35**
5.1 Collecting a device 37
5.2 Activating a device 41
5.3 Collecting an update for a device 44
5.4 Collecting a replacement device 47
5.5 Collecting a certificate renewal 51
6 Carrying out self-service actions **54**
6.1 Changing your PIN 55
6.2 Changing your security phrases 57
6.3 Resetting your PIN 60
6.4 Updating your device 63

7 Configuring the MyID Client for Mac 66
7.1 Setting configuration options within the MyID Client for Mac 66
7.1.1 Administrator-configured options 66
7.1.2 Setting communication options 67
7.1.3 Setting authentication options 68
7.1.4 Setting logging options 69
7.1.5 Setting accessibility options 70
7.1.6 Setting advanced options 71
7.1.7 Accessing configuration options from the Terminal 73
7.2 Setting up an administrator configuration override file 74

1 Introduction

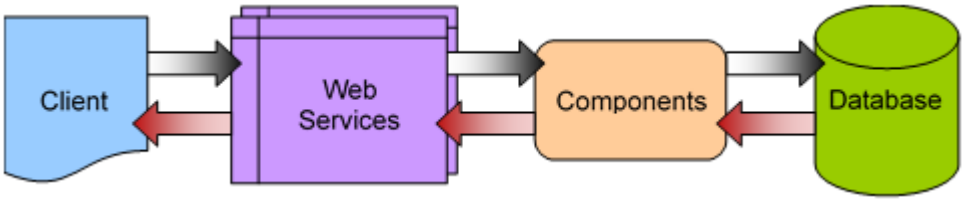
The MyID Client for Mac allows you to use your Apple Mac computer to carry out a wide variety of self-service operations.

You can:

- Change the PIN of your device.
- Change your security phrases.
- Reset your PIN.
- Update your device.
- Collect a device.
- Activate a device.
- Collect an update for your device.
- Collect a replacement device.
- Collect a certificate renewal.

You can also install an optional lightweight notifications application, the MyID StatusBar Client, which runs in the background and provides pop-up notifications when you have pending tasks.

1.1 Architecture



The MyID Client for Mac runs on your Apple Mac computer and passes requests through HTTP or HTTPS to the MyID Data Source and MyID Process Driver web services. The web services communicate using DCOM with the MyID components on the application server; these components provide the business logic and communicate with the MyID database. Responses are returned to the client through the MyID web services.

The web services, components, and database may be on separate servers, or on the same server; the MyID Client for Mac needs only to be able to communicate with the web services server, whether over the internet or on your organization's network.

1.2 Limitations

The MyID Client for Mac carries out many of the same functions as the Self-Service App does on Windows client PCs, but does have some limitations.

- The MyID Client for Mac supports a more limited range of smart cards and smart card readers.

  In particular, you cannot use devices that are specifically designed for Windows PCs; for example, VSCs, Windows Hello, or Windows minidriver-based smart cards. See section *2.1*, *System requirements* for details of the smart cards and readers the MyID Client for Mac supports.
- The MyID Client for Mac does not support Integrated Windows Logon.
- The MyID Client for Mac does not support fingerprint verification.
- The MyID Client for Mac does not support popup notification bubbles.
- The MyID Client for Mac does not support automation mode.
- **IKB-404 – The MyID Client for Mac fails to launch if reopened within five seconds of closing the application**

  If you attempt to launch the MyID Client for Mac within five seconds of closing the application, it fails to launch. If you wait five seconds after closing, the application opens as expected.

1.2.1 Changes since the beta version

If you previously installed the beta version of the MyID Client for Mac, be aware of the following:

- User preferences

  Any user preferences configured in the beta version are incompatible with the final release, and you must clear them before using the final version. You can clear existing preferences by running the following command in the macOS Terminal:

  ```
  defaults delete com.intercede.myidclient
  ```

  Alternatively, you can use the `Uninstall.sh` script provided in the disk image (`.dmg`) file to remove the beta, including any existing preferences; see section *2.3.3*, *Uninstalling the MyID Client for Mac using the provided script*.
- Reported platform ID

  MyID Client reports its platform ID to MyID, and in the beta it reported itself as the MyID Self-Service App to enable it to work with older versions of MyID. In version 2.0.0 of the MyID Client for Mac, it reports its ID correctly (meaning MyID Client for Mac appears in the audit); however, this new ID is recognized only by MyID 12.11 or later and is rejected by older systems. To use the client with versions earlier than 12.11, you must set the `UseLegacySsaPlatform` configuration to `true`; see section *7.1.6*, *Setting advanced options*.

1.3 Differences between the MyID Client for Mac and MyID Client for Windows

The MyID Clients for Windows and Mac have substantially the same functionality, with the following differences:

- The MyID Client for Mac supports a limited range of devices. The MyID Client for Windows supports additional devices, including minidriver-based smart cards, Microsoft Virtual Smart Cards, and Windows Hello for Business.

  See section *2.1.3*, *Supported devices*

- The MyID Client for Windows supports Integrated Windows Logon as an authentication method (for supported actions).
- By default, the MyID Client for Windows uses your current Windows user details rather than prompting for a username.

  In addition, if you manually provide a username that matches your user identifier, your SAM account name, or your UPN, the MyID Client for Windows provides all three identifiers to the server.
- You can use post-workflow triggered PowerShell scripts with the MyID Client for Windows; these are not available on the MyID Client for Mac.

  See the *Triggered scripts* section in the ***Administration Guide*** for details.

2 Installing and uninstalling the MyID Client for Mac

This section provides instructions for installing and uninstalling the MyID Client for Mac.

See:

- System requirements for the MyID Client for Mac.

  See section *2.1*, *System requirements*.
- Install the MyID Client for Mac.

  See section *2.2*, *Installing the MyID Client for Mac*.
- Uninstall the MyID Client for Mac.

  See section *2.3*, *Uninstalling the MyID Client for Mac*.

2.1 System requirements

This section contains information about the required operating systems, MyID versions, devices, and smart card readers.

2.1.1 Supported client operating systems

The MyID Client for Mac requires an Apple Mac computer with ARM-based M series Apple silicon running the one of the following operating system versions:

- Monterey – version 12.7.1 (21G920)
- Ventura – version 13.4
- Sonoma – version 14 to 14.4.1 (23E224)

2.1.2 Supported MyID versions

The MyID Client for Mac requires the following:

- MyID CMS 12.4.0 or later.

Note: If you are not using the most recent version of MyID CMS, you may need to change some configuration options:

- If you are using a version of MyID CMS earlier than 12.11, you must set the `UseLegacySsaPlatform` configuration option to `true` to allow the MyID Client for Mac to impersonate the Self-Service App and be recognized by the server.
- If you are using a version of MyID CMS earlier than 12.12, you must set the `UseLegacyPassphraseCollection` configuration option to `true` allow the MyID Client for Mac to use the old web-service endpoint; if you set this configuration option, support for authentication using external identity providers is disabled.

For information on setting configuration options, see section *7.1.6*, *Setting advanced options*.

2.1.3 Supported devices

The MyID Client for Mac currently supports the following devices:

- YubiKey 4 (PIV/smart card interface only)
- YubiKey 5 (PIV/smart card interface only)
- YubiKey FIPS (PIV/smart card interface only)
- YubiKey v57 (YubiKey 5 with firmware version 5.7.x)
- YubiKey v57 FIPS (YubiKey FIPS with firmware version 5.7.x)

  See the *Yubico smart cards* section in the ***Smart Card Integration Guide*** for information on configuring your system to work with YubiKey devices.
- IDEMIA ID-One PIV 2.4.2

  Note: IDEMIA ID-One PIV cards with Secure PIN Entry (SPE) are *not* supported.

  See the *IDEMIA smart cards* section in the ***Smart Card Integration Guide*** for information on configuring your system to work with IDEMIA devices.

Important: Your MyID server must support the device type; for example, YubiKey v57 and v57 FIPS devices are supported on MyID 12.10 (with HOTFIX-12.10.0.1) and 12.11, but not on earlier versions of MyID.

2.1.4 Supported smart card readers

The MyID Client for Mac has been tested with IDEMIA smart cards and the following smart card readers:

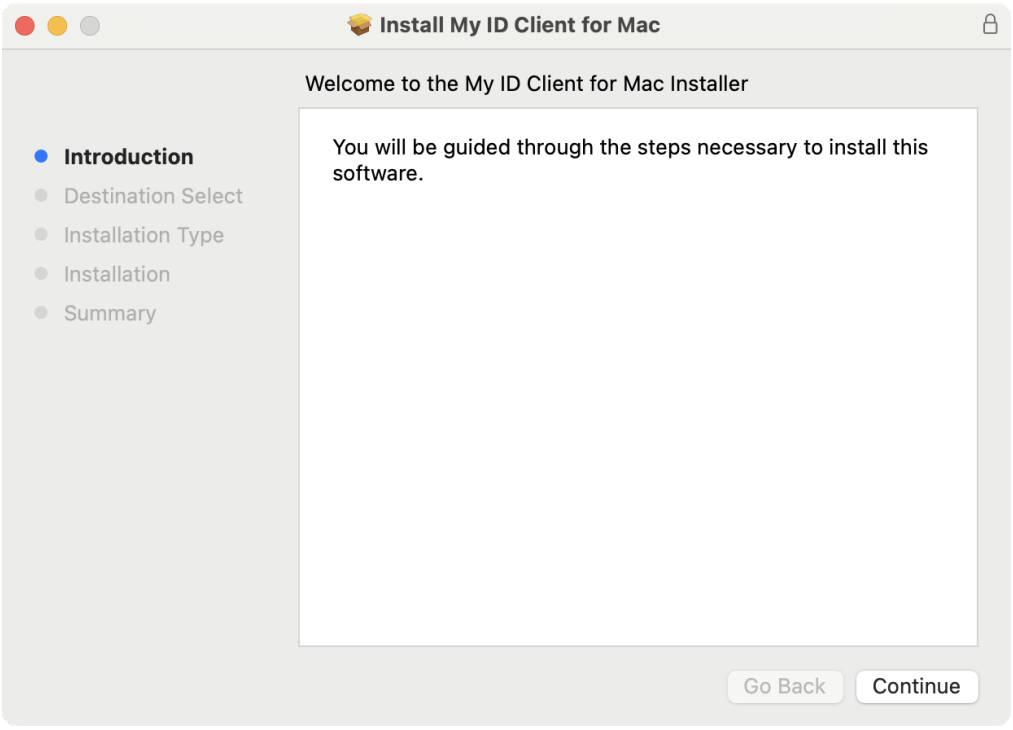
- Omnikey 3021
- Omnikey 3121

Note: Only recently-made readers are compatible with macOS and IDEMIA cards; for example, readers with copyright 2021 and Rev C on the back. Older smart card readers (for example, those with a date of 2013 or earlier) are not expected to work.

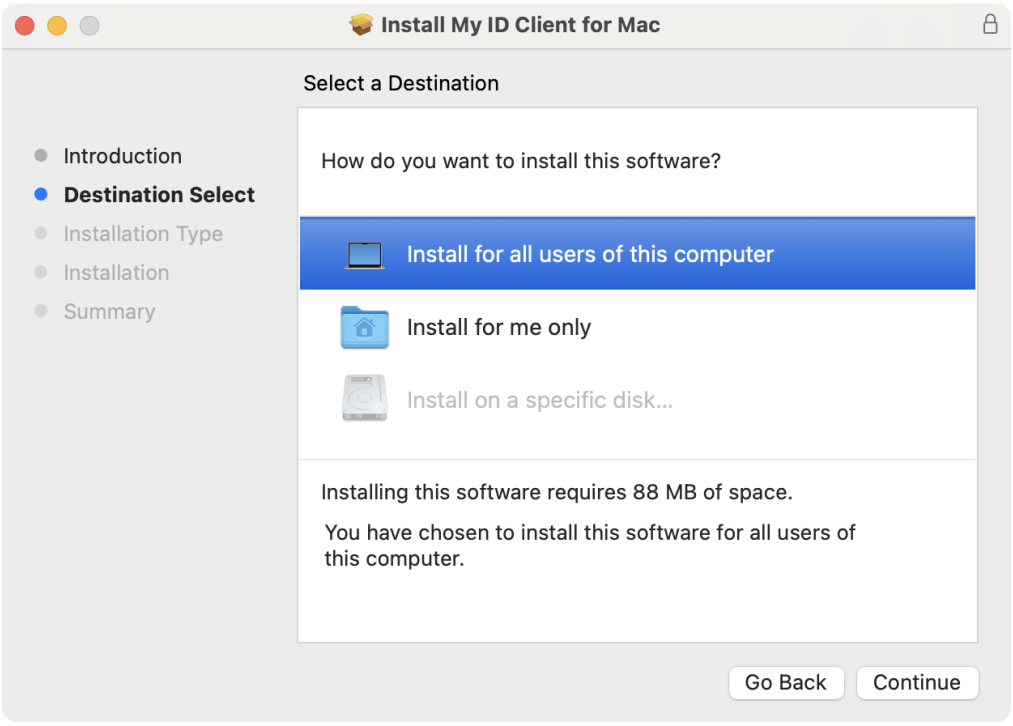
2.2 Installing the MyID Client for Mac

The MyID Client for Mac installation program is provided in a disk image (`.dmg`) file.

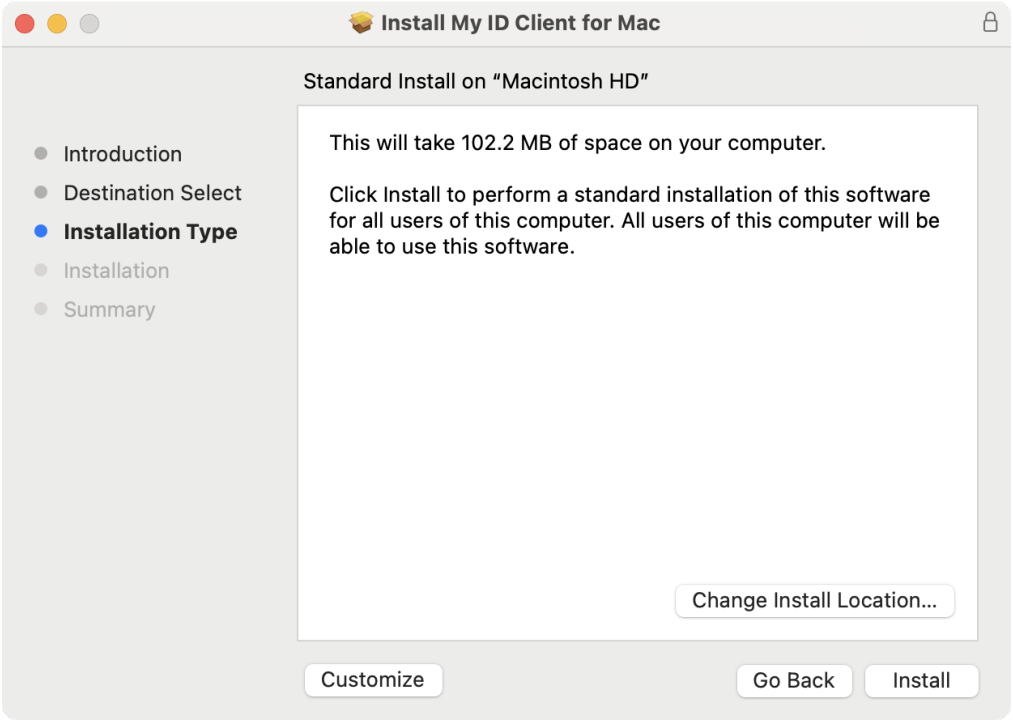
1. Open the disk image file, then double-click the package (`.pkg`) file to begin the installation.



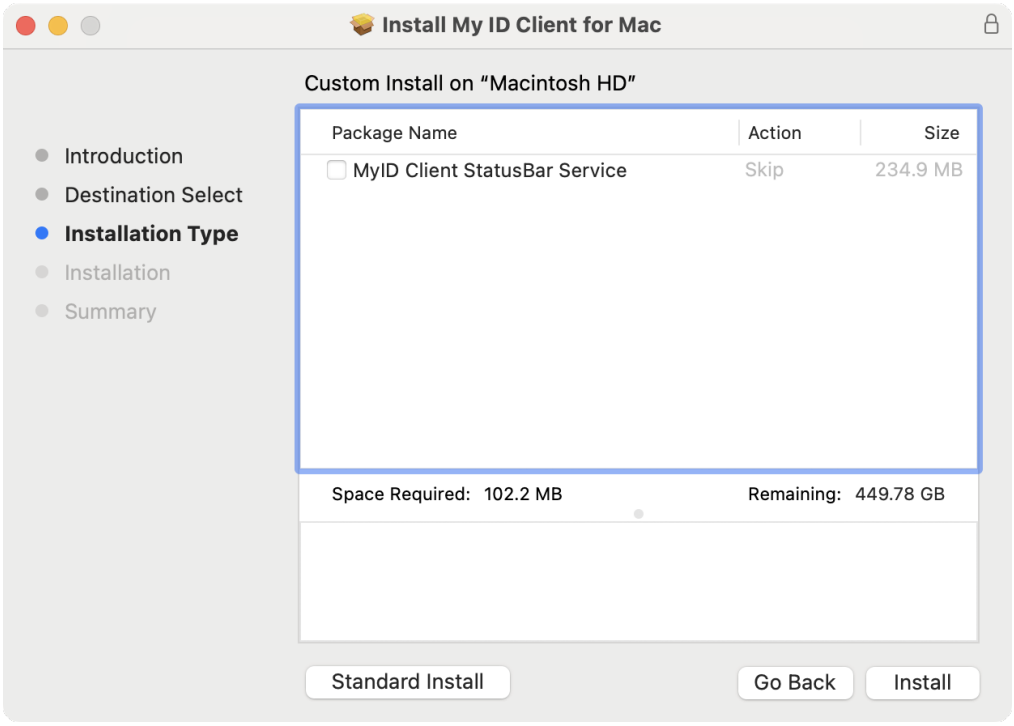
2. Click **Continue**.



3. Select one of the following options:
   - **Install for all users of this computer** – the MyID Client for Mac is available for all users of this computer.
   - **Install for me only** – the MyID Client for Mac is available for only the current user of this computer.
4. Click **Continue**.



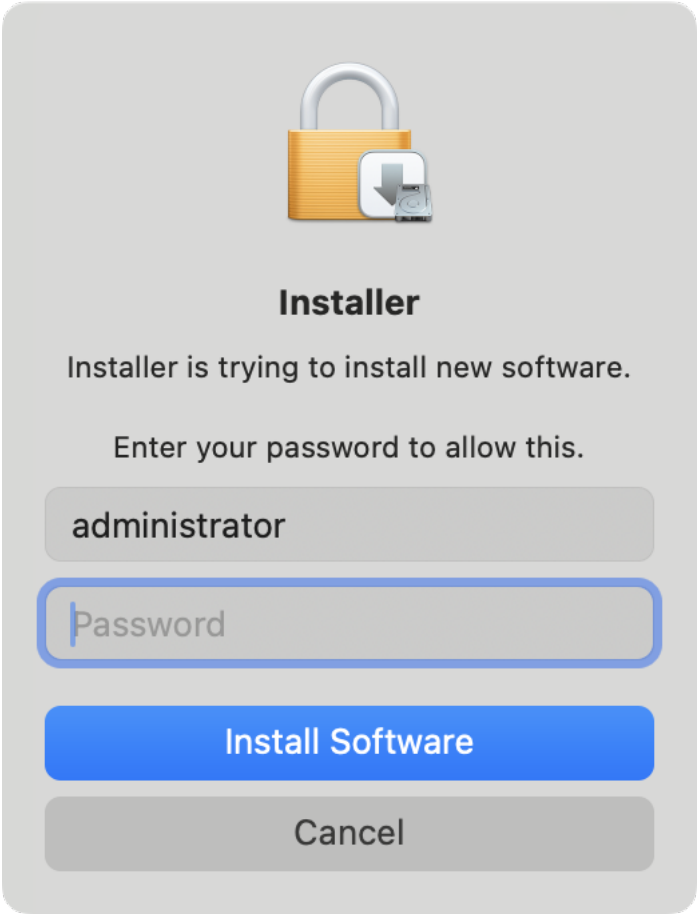
5. If you want to install the MyID Client StatusBar Service:
   a. Click **Customize**.



   b. Select **MyID Client StatusBar Service**.

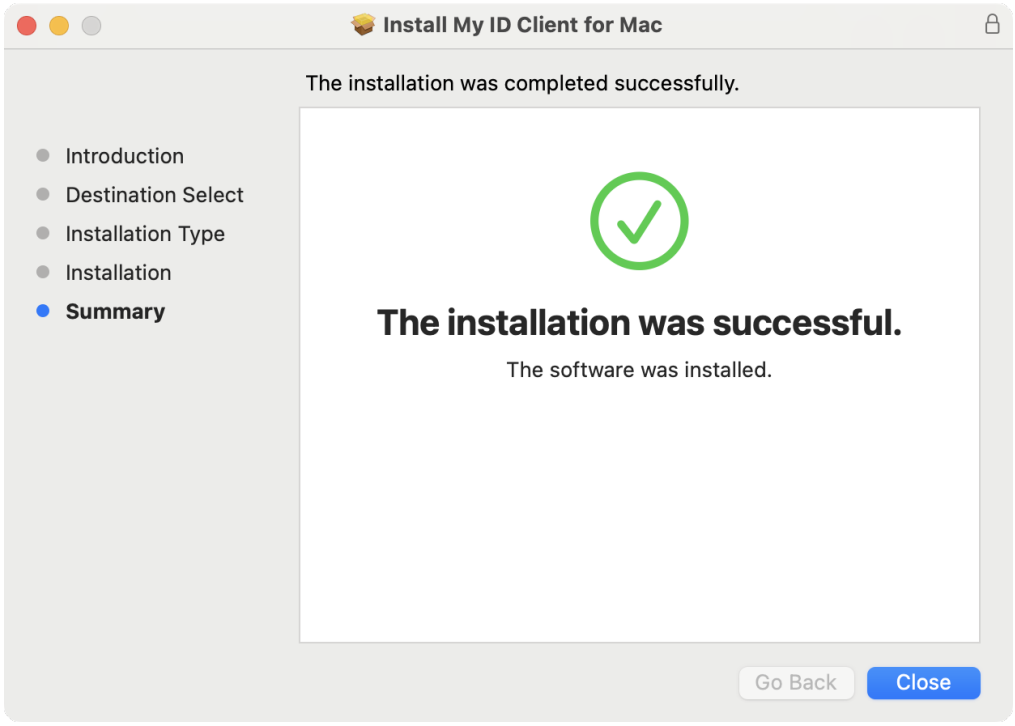
6. Click **Install**.

   If you are installing for all users, the installation program prompts you for your administrator password.



7. Type your password, then click **Install Software**.

   The installation program installs the MyID Client for Mac.



8. Click **Close**.
9. If you have installed the MyID Client StatusBar Service, a notification appears in the top right of the screen that the MyID Client StatusBar Service may provide notifications. Click the **Options** button on the notification, and select **Allow**.

2.3 Uninstalling the MyID Client for Mac

You can uninstall the MyID Client for Mac from the Applications folder, or you can uninstall using the provided script.

2.3.1 Uninstalling the MyID Client for Mac from the Applications folder

To uninstall the MyID Client for Mac from the Applications folder:

1. In the Finder, click **Applications**.

   Note: There are two `Applications` folders:

   - `/Applications` – the location for apps shared between all users.
   - `/User/<username>/Applications` – the location for apps installed for the current user only.

   Make sure you choose the appropriate folder.
2. Select the **MyID Client for Mac** option, then from the **File** menu select **Move to Trash**.
3. If you are uninstalling for all users, provide your administrator password.

   The MyID Client for Mac is uninstalled.

   Note: The uninstallation process does not remove the settings for the app. If you want to remove the settings for the current user, type the following in the Terminal:

   ```
   defaults delete com.intercede.myidclient
   ```

   You must do this for each user.

2.3.2 Uninstalling the MyID Client StatusBar Service

To uninstall the MyID Client StatusBar Service, you must first stop it from running:

1. In the Finder, open **Applications > Utilities > Activity Monitor**.
2. Locate the MyID Client StatusBar Service.
3. Click the Stop button .
4. Click **Force Quit**.

You can then uninstall the MyID Client StatusBar Service from the Applications folder:

1. In the Finder, click **Applications**.

   Note: There are two `Applications` folders:

   - `/Applications` – the location for apps shared between all users.
   - `/User/<username>/Applications` – the location for apps installed for the current user only.

   Make sure you choose the appropriate folder.
2. Select the **MyID Client StatusBar Service** option, then from the **File** menu select **Move to Trash**.
3. If you are uninstalling for all users, provide your administrator password.

   The MyID Client StatusBar Service is uninstalled.

   Note: The MyID Client StatusBar Service uses the configuration settings of the MyID Client for Mac, so uninstalling the MyID Client StatusBar Service does not affect the MyID Client for Mac settings.

2.3.3 Uninstalling the MyID Client for Mac using the provided script

The MyID Client for Mac disk image provides an uninstallation script you can use for either interactive or headless uninstallation.

The syntax is:

```
Uninstall.sh (--preserve-preferences | --dont-unregister | --headless | --reveal | --dry | --list | --log | --help)
```

where:

Parameter	Description
`--preserve-preferences`	Optionally prevent deletion of the user's settings and preferences. These are stored within the macOS user defaults database. This does not affect an administrator configuration override file.
`--dont-unregister`	Does not unregister the application from the macOS Launch Services. Files are still deleted from disk.
`--headless`	Suppresses prompting the user before uninstalling an instance. Instances of MyID Client for Mac are deleted without prompt.
`--reveal`	Reveals all instances of MyID Client for Mac in Finder, then quits. Not headless. No changes are made.
`--dry`	Performs a dry run of the uninstaller. No changes are made.
`--list`	Lists all instances of MyID Client for Mac, then quits. Headless. No changes are made.
`--log`	Specifies a log file path into which the output of the script will be written.
`--help`	Displays a list of the available parameters.

3 Configuring MyID CMS for the MyID Client for Mac

You control access to the actions and tasks available in the MyID Client for Mac by setting up your roles in MyID.

Note: This uses the same configuration as the Self-Service App uses for Windows clients. If you have already set up your MyID server for the Self-Service App, no additional configuration is required.

You can:

- Control access to self-service actions .

  See section *3.1*, *Configuring access to actions*.
- Set up access for self-service device updates.

  See section *3.2*, *Setting up self-service device update*.
- Control access to update tasks.

  See section *3.3*, *Configuring access to tasks*.

3.1 Configuring access to actions

Each person who wants to use the MyID Client for Mac must be assigned a role that provides the appropriate workflow that corresponds to the action; in addition, you must configure the built-in system role **Default SSA User** with the same permissions. This is because the MyID Client for Mac displays the list of actions before the person has authenticated themselves to the MyID server.

- **Change My PIN** – requires access to the **Change PIN** workflow in **Edit Roles**.
- **Change My Security Phrases** – requires access to the **Change My Security Phrases** workflow in **Edit Roles**.
- **Reset My PIN** – requires access to the **Unlock My Card** workflow in **Edit Roles**.

  Note: See the *Configuring self-unlock* section in the ***Web Service Architecture*** guide for details of editing the `AllowSelfUnlockForPIV` setting.
- **Update My Device** – requires access to the **Update My Device** (for both the Default SSA User role and the person's role) and **Collect My Updates** (for the person's role only) workflows in **Edit Roles**.

  Note: Self-service device update requires additional configuration, as it may not be suitable for all organizations. This configuration also determines what sort of device update is available; you may be able to update your device to the latest credential profile, or you may be able to reprovision your device completely. See section *3.2*, *Setting up self-service device update* for details.

3.2 Setting up self-service device update

For self-service device update, in addition to the role configuration (see section *3.1*, *Configuring access to actions*), you must also configure MyID with a mapping file that details how the self-service device update is carried out.

To configure the external system for the self-service device update feature:

1. In MyID Desktop, from the **Configuration** category, select **External Systems**.
2. Click **New**.
3. From the **Listener Type** drop-down list, select **UserSync**.

   The configuration details for the self-service device update feature appear.
4. Type a **Name** and **Description** for the external system.
5. From the **Mapping File** drop-down list, select one of the following:
   - **UserSync_UpdateCardToLatest** – all self-service updates through the **Update My Device** option in the MyID Client for Mac carry out an update of the device to the latest version of the credential profile.
   - **UserSync_ReprovisionCard** – all self-service updates through the **Update My Device** option in the MyID Client for Mac carry out a full reprovision of the device.

   The mapping file contents are displayed in the Contents pane.
6. Click **Save**.

3.3 Configuring access to tasks

When you have a task available, it appears in your **Tasks** list. When you select the task and authenticate to the MyID server, the MyID Client for Mac checks that you have access to the appropriate workflow.

- Collecting a device – requires access to the **Collect My Card** workflow in **Edit Roles**.
- Activating a device – requires access to the **Activate Card** workflow in **Edit Roles**.
- Collecting an update for a device – requires access to the **Collect My Updates** workflow in **Edit Roles**.

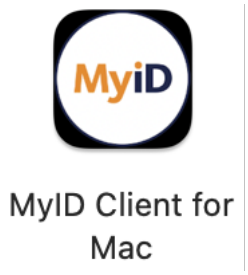
  Note: This task requires a card that has been issued with MyID Logon capabilities; you must also be permitted to log on with a smart card.
- Collecting a replacement device – requires access to the **Collect My Card** workflow in **Edit Roles**.
- Collecting a certificate renewal – requires access to the **Collect My Certificates** workflow in **Edit Roles**.

  Note: This task requires a card that has been issued with MyID Logon capabilities; you must also be permitted to log on with a smart card.

4 Launching the MyID Client for Mac

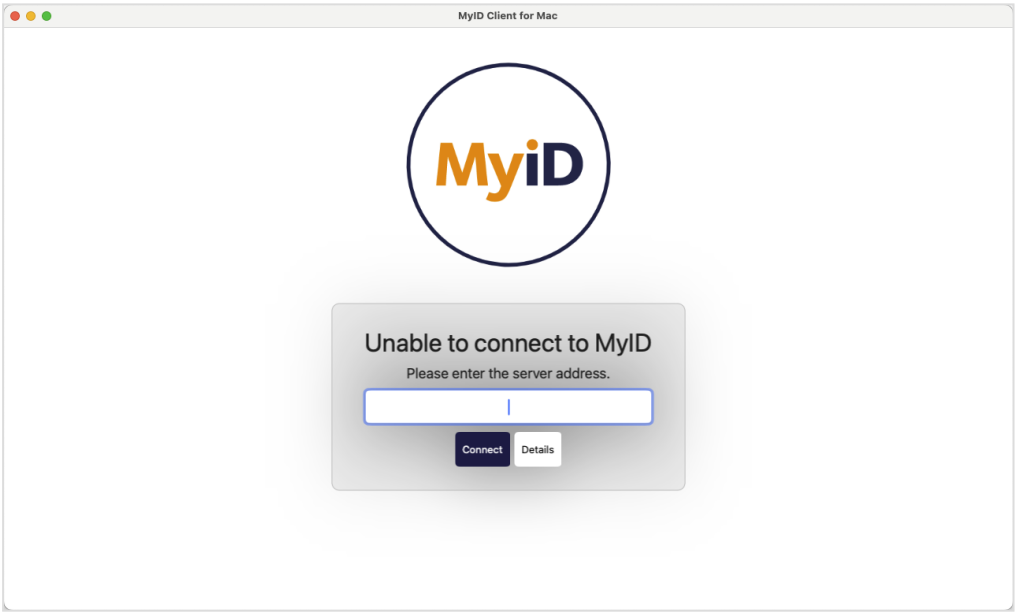
To launch the MyID Client for Mac:

1. Open the Launchpad, or in the Finder select **Applications**.
2. Double-click the MyID Client for Mac icon:

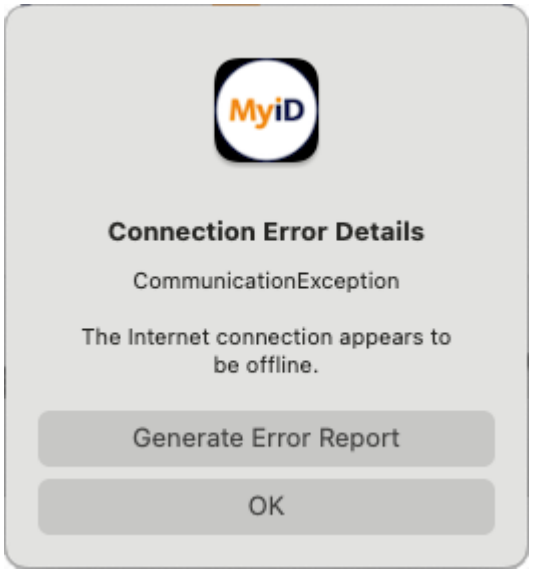


3. The MyID Client for Mac opens.

   The first time you launch the MyID Client for Mac, it is unable to connect to the MyID CMS server, as you have not yet provided its location.



   If you have already provided the location of the MyID CMS server, but the MyID Client for Mac cannot connect, you can click the **Details** button to provide further information, and optionally generate an error report to help diagnose the issue:



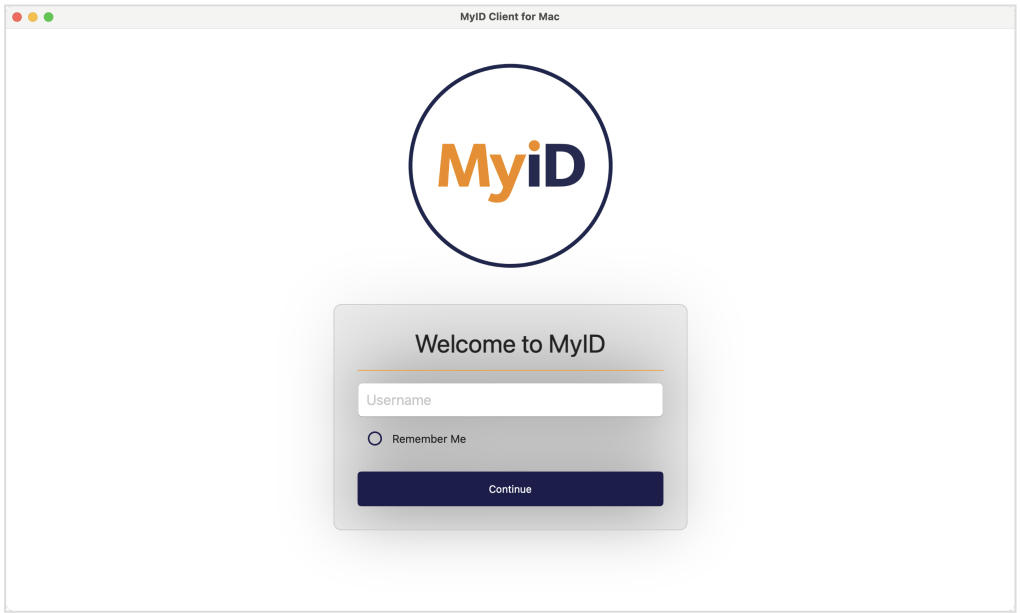
4. Type the URL of the MyID CMS server; for example:

   `https://myid.example.com/`

   Note: You must start the server address with `https://`.

5. Click **Connect**.

   The MyID Client for Mac connects to the server, and requests your username.

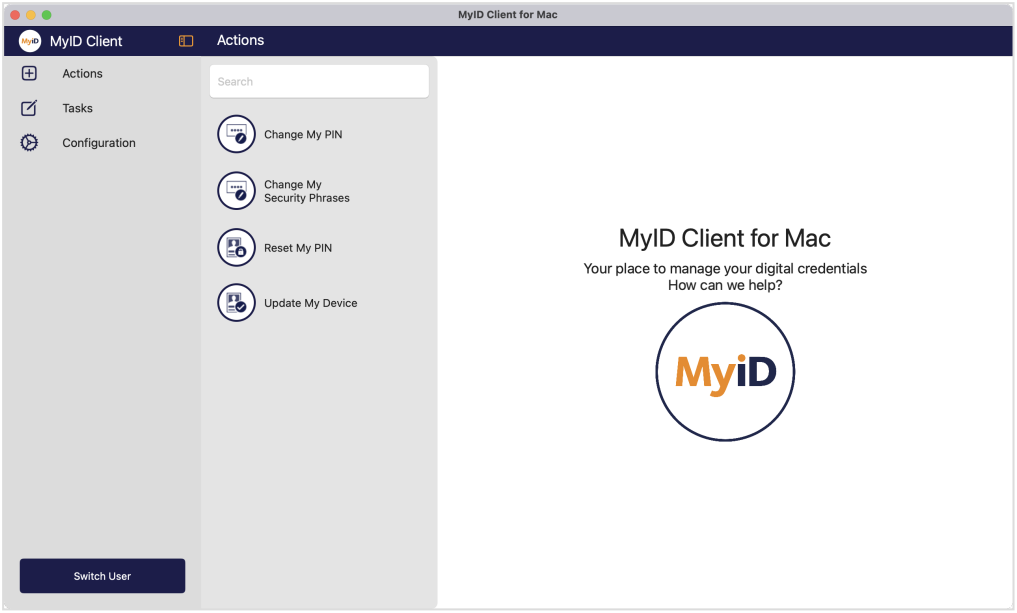


6. Type your username.
7. Optionally, select the **Remember Me** option to remember your username so you do not have to type it again when you launch the MyID Client for Mac.

   Note: If you subsequently want to change this option, you can do so in the **Configuration** screen.

8. Click **Continue**.

The MyID Client for Mac opens.



You can launch the MyID Client for Mac from the MyID Client StatusBar Service if you have outstanding tasks; see section *4.2*, *Launching the MyID Client for Mac from the MyID Client StatusBar Service*.

You can also launch the MyID Client for Mac from a hyperlink; for example, from an email notification, from an Intranet web page, or from the Self-Service Request Portal. For information about configuring hyperlinks, see section *4.3*, *Launching the MyID Client for Mac from a hyperlink*.

- **IKB-404 – The MyID Client for Mac fails to launch if reopened within five seconds of closing the application**

  If you attempt to launch the MyID Client for Mac within five seconds of closing the application, it fails to launch. If you wait five seconds after closing, the application opens as expected.

4.1 Switching users

You can switch to a different user account.

Note: If your administrator has configured your MyID Client for Mac with a username and specified that the user cannot override this value, you cannot switch user accounts.

To switch to a different user account:

1. Click **Switch User**.
2. On the Welcome to MyID screen, type your username.
3. Optionally, select the **Remember Me** option to remember your username so you do not have to type it again when you launch the MyID Client for Mac.

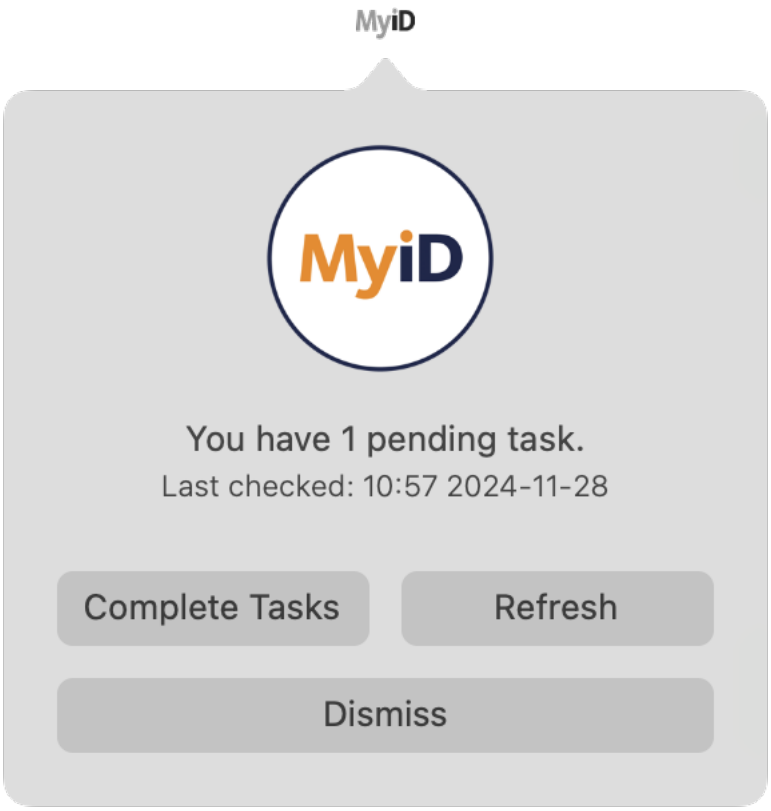
4.2 Launching the MyID Client for Mac from the MyID Client StatusBar Service

When you install the MyID Client StatusBar Service, it starts automatically whenever you log on to your Mac and runs in the background to check periodically for new tasks on the MyID server.

Note: The MyID Client StatusBar Service requires MyID 12.12 or later, and will not operate if you set the `UseLegacySsaPlatform` configuration option.

4.2.1 Launching the MyID Client for Mac from a notification

When a task is available for you, the MyID Client StatusBar Service pops up a notification from the menu bar. You can also click on the MyID Client StatusBar Service icon in the menu bar to check for tasks.

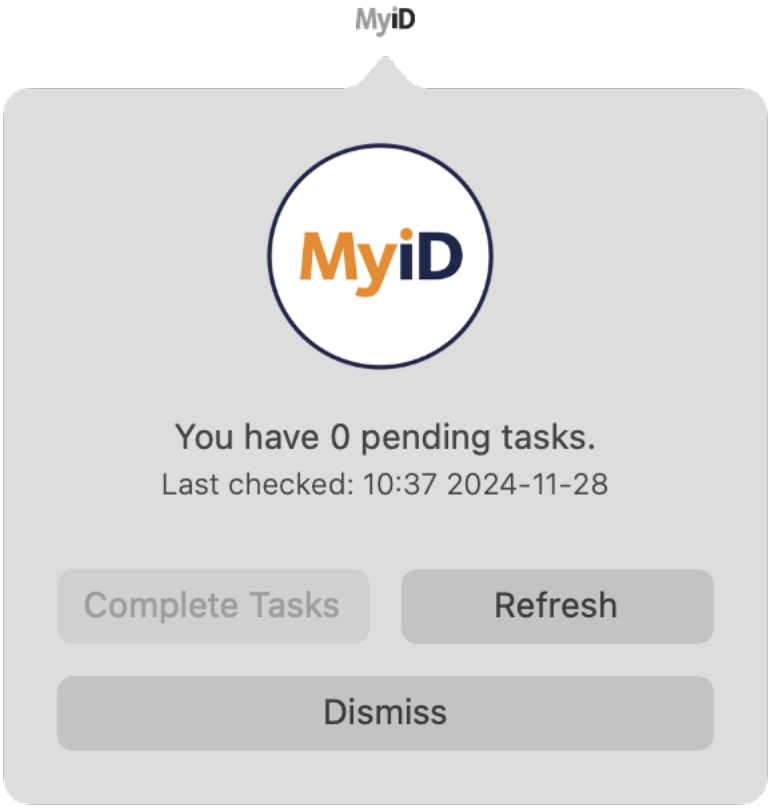


Click **Complete Tasks** to launch the MyID Client for Mac and start the first available task.

4.2.2 Checking for updates

The MyID Client for Mac automatically checks for available tasks periodically. You can force the MyID Client for Mac to check immediately in one of the following ways:

- Click on the MyID Client StatusBar Service icon in the menu. This opens the notification and forces a check for tasks.



- On your open MyID Client StatusBar Service notification, click **Refresh**.

4.2.3 Troubleshooting

The MyID Client StatusBar Service uses the server details and other configuration settings from the MyID Client for Mac. If the MyID Client StatusBar Service cannot connect to the server, use the MyID Client for Mac to set the server details and then restart the MyID Client StatusBar Service.

To restart the MyID Client StatusBar Service:

1. In the Finder, open **Applications > Utilities > Activity Monitor**.
2. Locate the MyID Client StatusBar Service.
3. Click the Stop button .
4. Click **Force Quit**.
5. Open the MyID Client StatusBar Service from the Launcher.

4.3 Launching the MyID Client for Mac from a hyperlink

When you install the MyID Client for Mac, it registers the `myidssa:` protocol – this means that you can click on hyperlinks on web pages and email messages to launch the MyID Client for Mac. This allows you to create tailored email notifications from within MyID; for example, to send to a user when there is a new security device to collect.

You can use the following parameters:

- `/un:username`

  Allows you to specify the username for the person.

  For example:

  ```
  <a href="myidssa:///un:susan.smith">
  ```

- `/jobid:task`

  Allows you to specify the ID of the task you want to collect. You can use the `%jobid%` substitution code in the email template to provide the appropriate ID.

  For example:

  ```
  <a href="myidssa:///un:susan.smith+/jobid:%jobid">
  ```

- `/opid:action`

  Allows you to specify an action to carry out. You can use the following codes:

  - `110` – **Change My Security Phrases**
  - `255` – **Reset My PIN**
  - `202` – **Change My PIN**
  - `5013` – **Update My Device**

  For example:

  ```
  <p><a href="myidssa:///un:susan.smith+/opid:110">Change My Security Phrases</a></p>
  <p><a href="myidssa:///un:susan.smith+/opid:255">Reset My PIN</a></p>
  <p><a href="myidssa:///opid:202+/un:susan.smith">Change My PIN</a></p>
  <p><a href="myidssa:///opid:5013+/un:susan.smith">Update My Device</a></p>
  ```

- `/w`

  Closes the MyID Client for Mac at the end of the operation.

  For example:

  ```
  <a href="myidssa:///w+/un:susan.smith+/opid:110">Change My Security Phrases</a>
  ```

  This opens the MyID Client for Mac for the user Susan Smith, prompts them to change their security phrases and, once they have completed that operation, closes the client.

  If you specify the `/w` parameter, but do not specify an `opid` for an action or a `jobid` for a task, the MyID Client for Mac opens, carries out the first available task for the specified user, then, once they have completed that task, closes the client. If the user has no tasks available, the MyID Client for Mac allows them to select an action to carry out, then, once they have completed that action, closes the client.

Note: You *must* include the username in hyperlinks to launch the MyID Client for Mac.

You can use the parameters in any order.

To make sure that usernames with spaces are dealt with correctly, you must replace the spaces with + signs. For URLs created from email templates, MyID can do this automatically if you use the correct syntax.

For example, if your email template includes the following:

```
Click <a href="myidssa:///jobid:%jobid+/un:{%logonName:URI}">Collect</a>.
```

when the email message is created, it becomes HTML similar to:

```
Click <a href="myidssa:///jobid:256+/un:Jane+Smith">Collect</a>.
```

4.4 Keyboard shortcuts

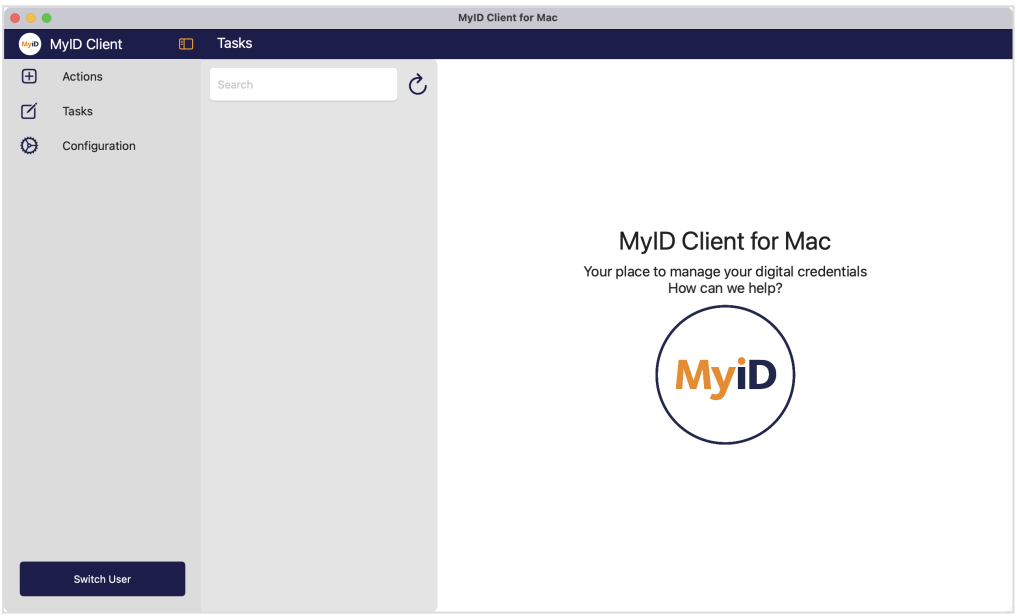
You can use the following keyboard shortcuts when working with the MyID Client for Mac:

Key	Context	Action
Enter	While in a PIN or security phrase field.	Submits the form.
⌘ + R	On the Tasks page.	Refreshes the available tasks.
⌘ + Enter	On any page with a **Continue** or **Apply Changes** button.	Submits the form.
⌘ + [	On any page with a **Back** button.	Goes back to the previous screen.
⌘ + Esc	On any page with a **Cancel** button.	Cancels the operation.

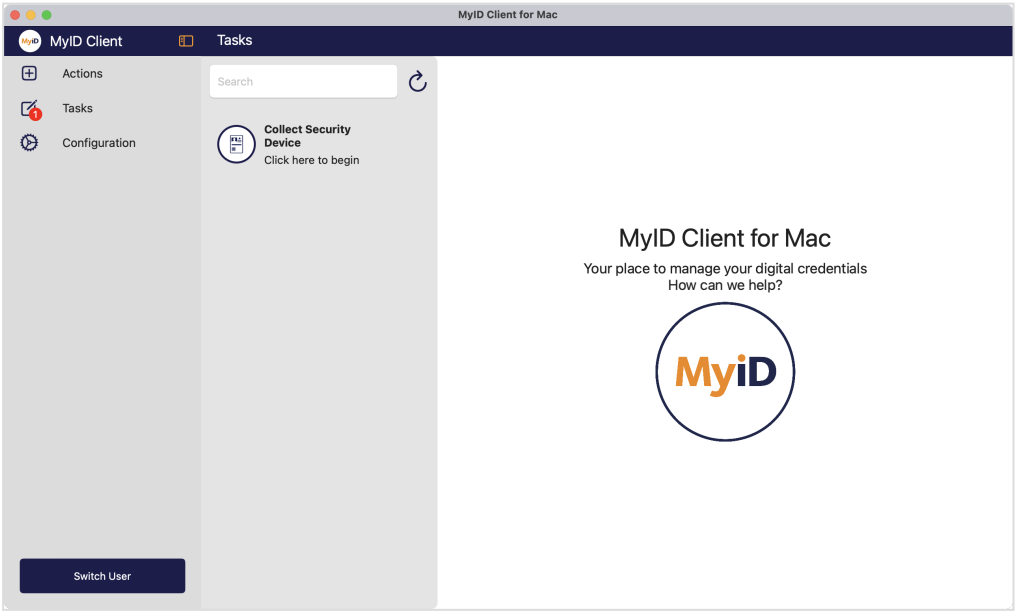
5 Checking for device tasks

The MyID Client for Mac allows you to carry out a variety of device tasks. Unlike Actions, where you instigate the procedure yourself, Tasks are made available for you by operators; for example, an operator may request a device for you, and a Task appears in your list informing you that you can collect it. Some tasks may be automatic; for example, if your certificates are nearing their expiry date, the MyID system may generate a certificate renewal task for you.

Click the **Tasks** option, and the list of available tasks appears. The list of tasks is refreshed periodically; click the refresh icon to check the MyID server immediately for any available tasks.



If there are available tasks, a badge appears on the **Tasks** link showing the number of tasks.



You can use the **Search** box to search for a particular task.

You can carry out the following types of task:

- Device collection.

  See section *5.1*, *Collecting a device*.
- Device activation.

  See section *5.2*, *Activating a device*.
- Device update.

  See section *5.3*, *Collecting an update for a device*.
- Device replacement.

  See section *5.4*, *Collecting a replacement device*.
- Certificate renewal.

  See section *5.5*, *Collecting a certificate renewal*.

5.1 Collecting a device

You can use the MyID Client for Mac to collect a device that has been requested for you.

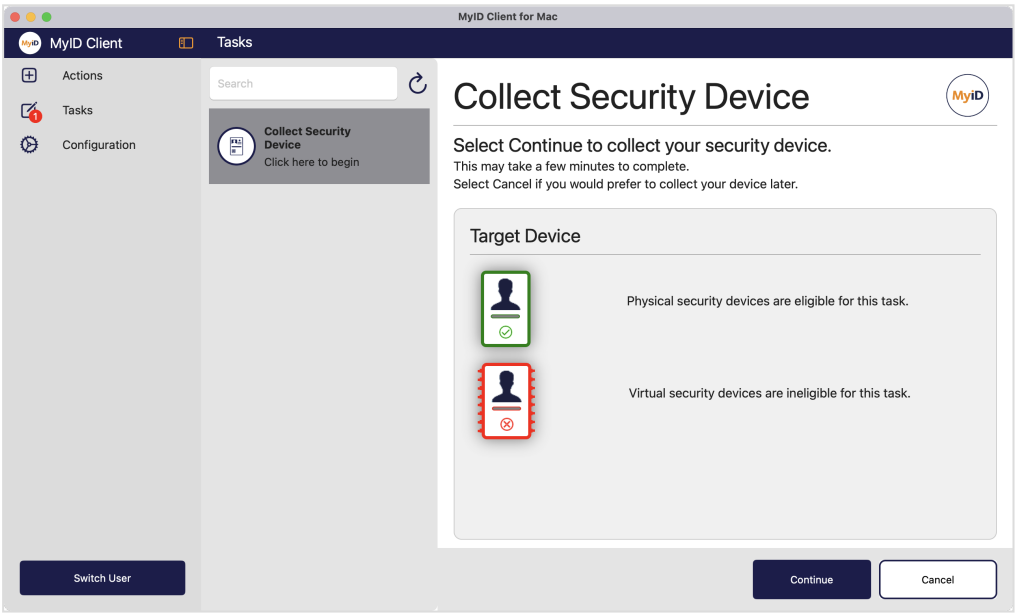
Using this task requires access to the **Collect My Card** workflow in **Edit Roles**.

To collect a device:

1. Click the **Tasks** option.
2. Click the **Collect Security Device** task in the list.

   The MyID Client for Mac displays information about the target device that is required for this task.

   For example, you may have to use a specific device, or you may be able to use any physical device (smart card or USB token) that is supported.



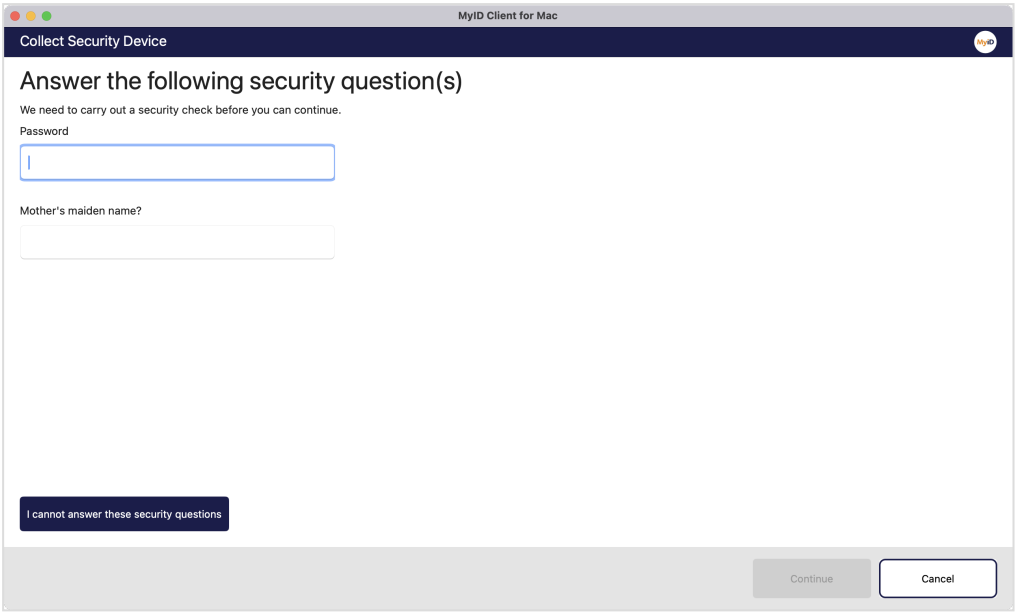
3. Click **Continue**.

   You must now provide your authentication details to the MyID Client for Mac.

   You must have permission to authenticate using security phrases or an external identity provider.

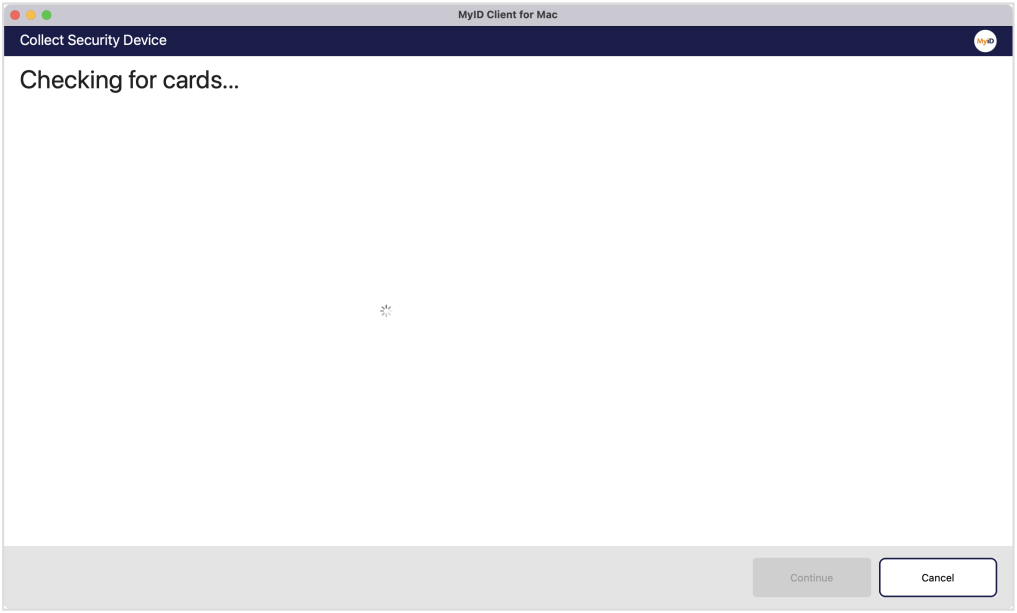
   Note: The order of these authentication methods is determined by the **Logon Priority** tab in the **Security Settings** workflow in MyID Desktop. **Windows Logon** is not available as an option in the MyID Client for Mac; also, you cannot use an external identity provider if the credential profile for the device being collected requires activation.

   For details of using external identity providers, see the *Setting up an external identity provider* section in the ***MyID Authentication Guide***.

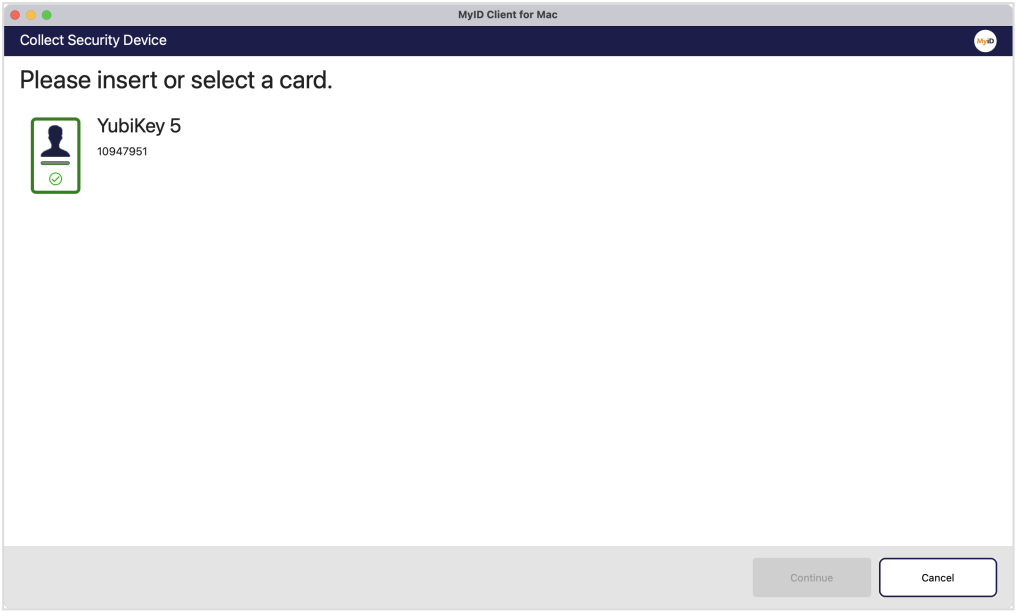


4. Provide your authentication details then click **Continue**.

   The MyID Client for Mac checks for attached devices.

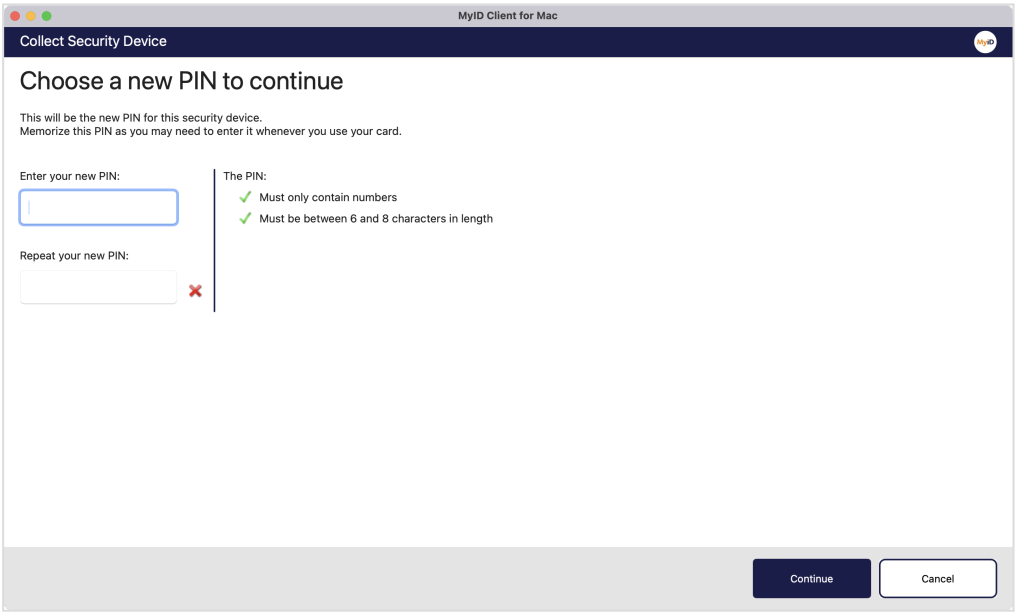


5. Insert your smart card into a card reader, or your USB token into the USB port.



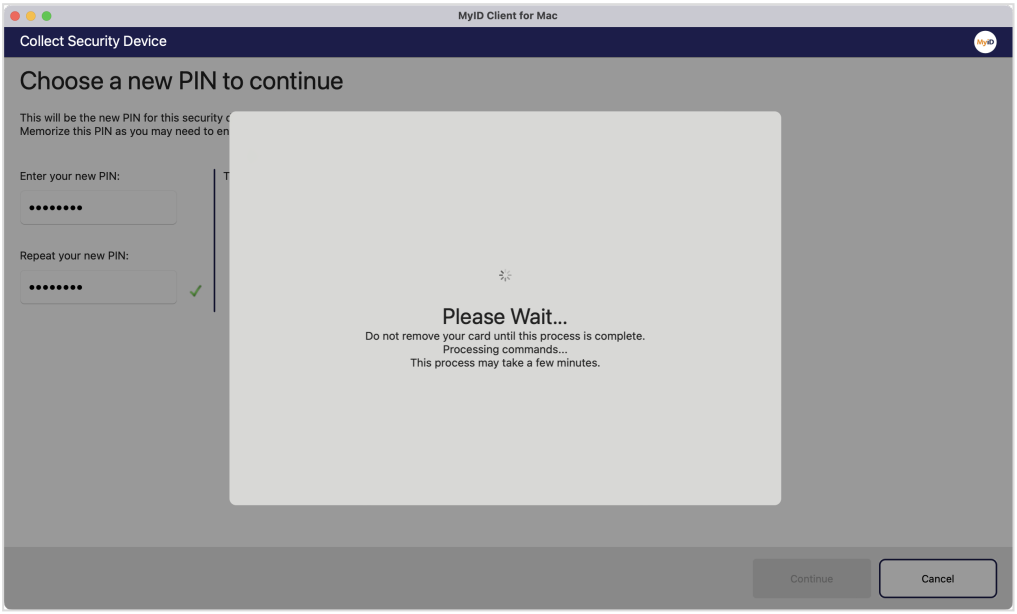
6. Select your device from the list and click **Continue**.

   You must now provide a PIN for your new device.



7. Type your new PIN and confirm it, then click **Continue**.

   The MyID Client for Mac collects your device.



8. When the collection has completed, you can remove your device from the reader.

5.2 Activating a device

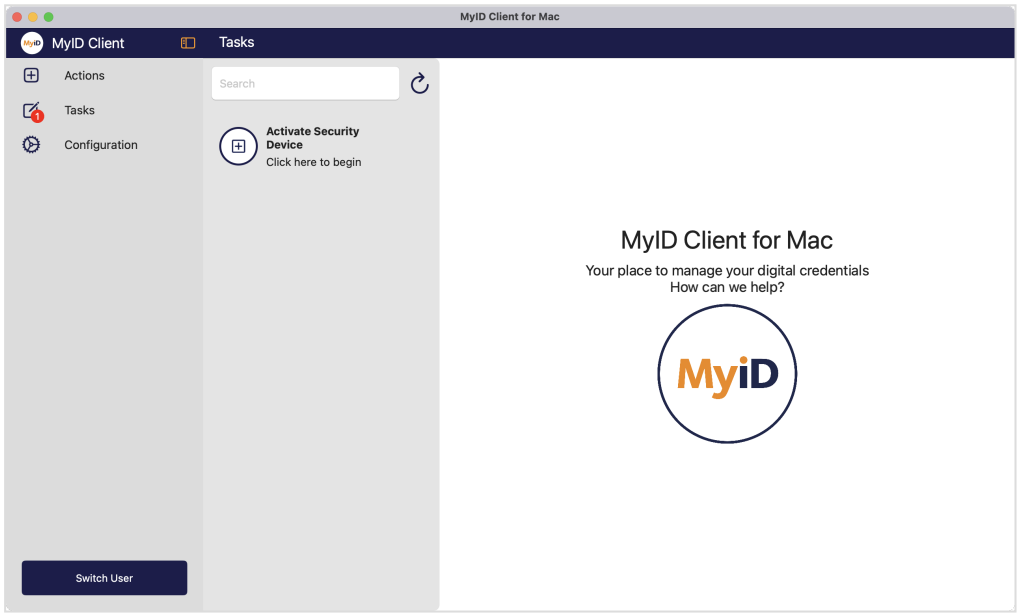
You can use the MyID Client for Mac to activate a device. For example, your organization may ship you a locked device; until you activate it using the MyID Client for Mac, no-one can use it.

Currently, the MyID Client for Mac supports the use of authentication codes for device activation.

Using this task requires access to the **Activate Card** workflow in **Edit Roles**.

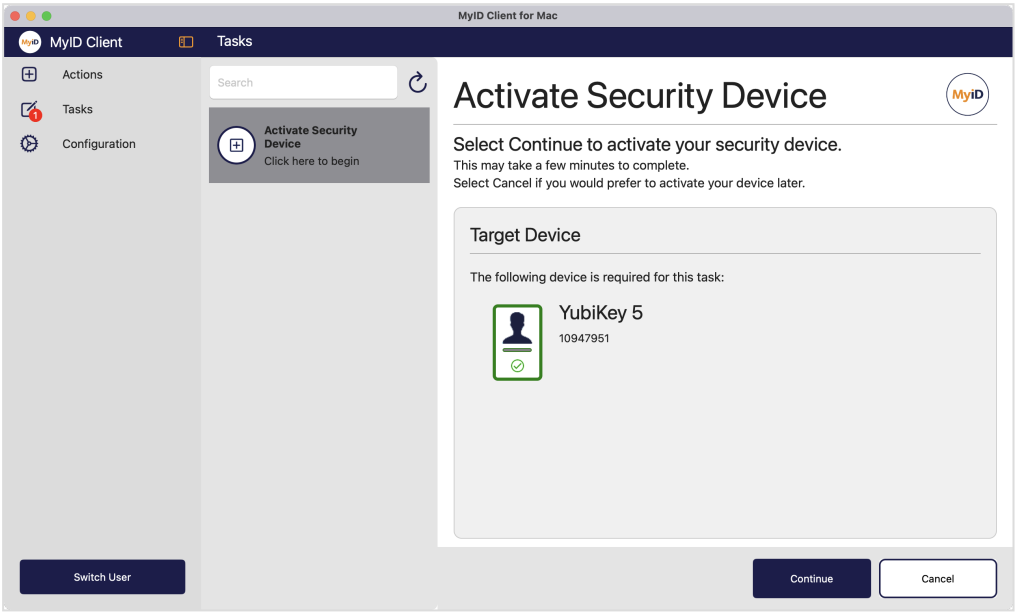
To activate a device:

1. Click the **Tasks** option.



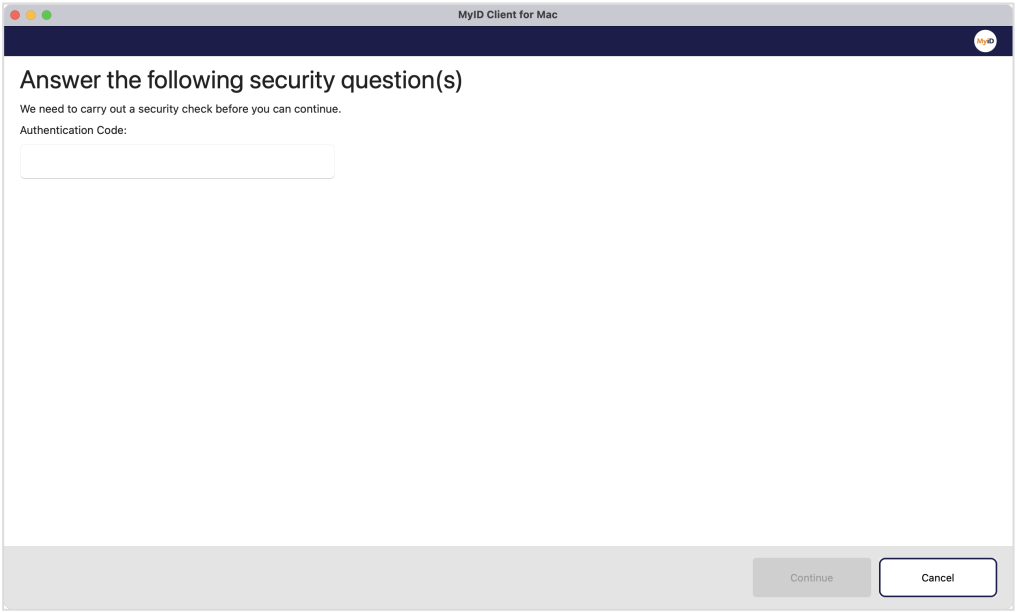
2. Click the **Activate Security Device** task in the list.

   The MyID Client for Mac displays information about the target device that is required for this task.



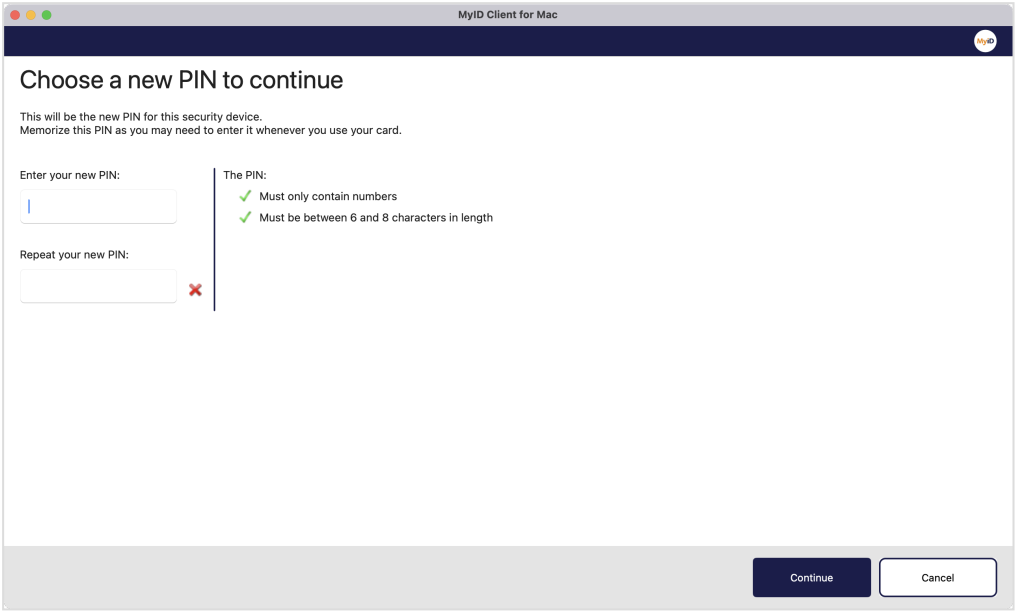
   For device activation, you must use a specific device; the MyID Client for Mac displays the device type and serial number of the device you need to activate.

   Note: Make sure you have an authentication code for device activation before you click **Continue**.



3. Type your authentication code, then click **Continue**.

4. If your credential profile is configured for the acceptance of terms and conditions, accept the terms and conditions and continue.



5. Type and confirm the new PIN for your device, then click **Continue**.

   The MyID Client for Mac activates your device.

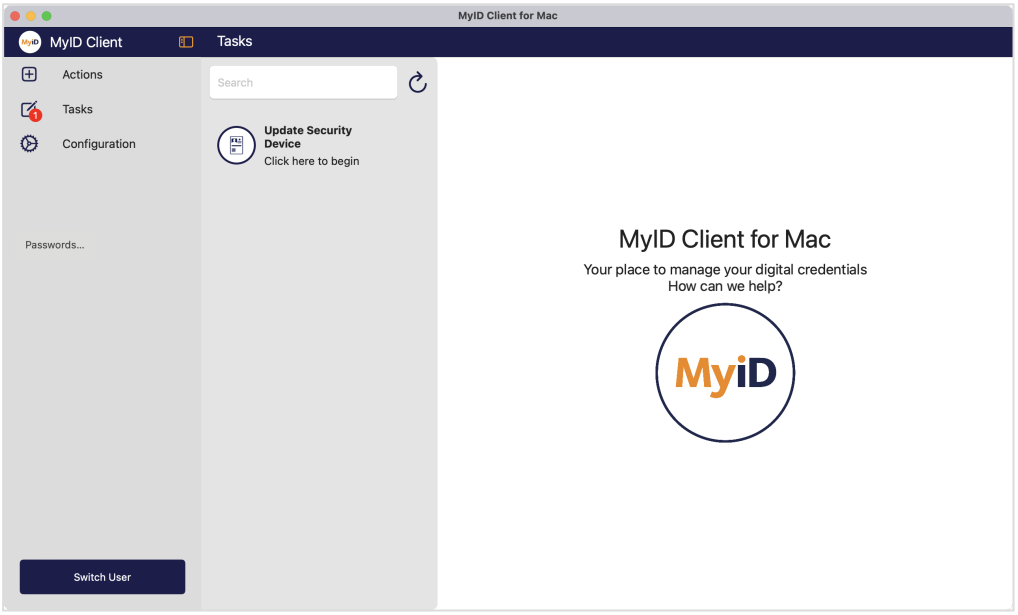
5.3 Collecting an update for a device

You can use the MyID Client for Mac to collect a pending update for your device. For example, your organization may have requested an update for your device to change the credential profile.

Using this task requires access to the **Collect My Updates** workflow in **Edit Roles**. In addition, this task requires a card that has been issued with MyID Logon capabilities; you must also be permitted to log on with a smart card.

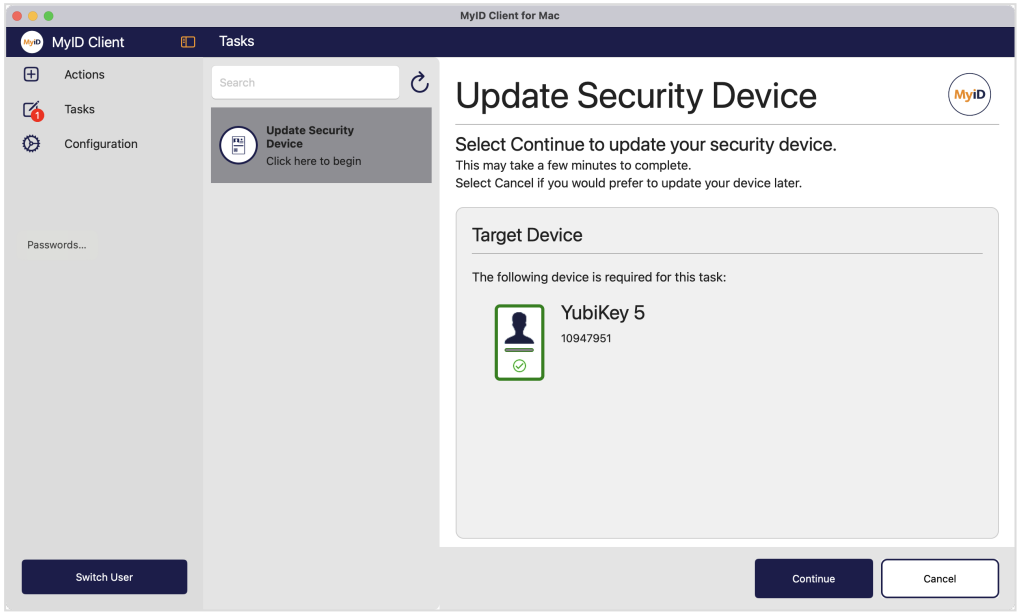
To collect an update:

1. Click the **Tasks** option.

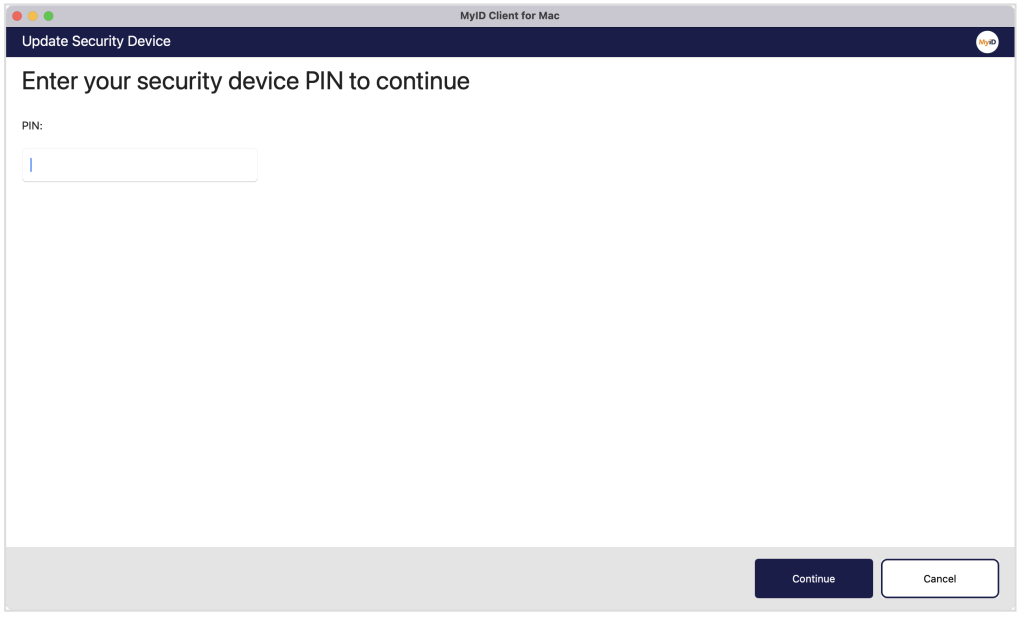


2. Click the **Update Security Device** or **Reprovision Security Device** task in the list.

   The MyID Client for Mac displays information about the target device that is required for this task.

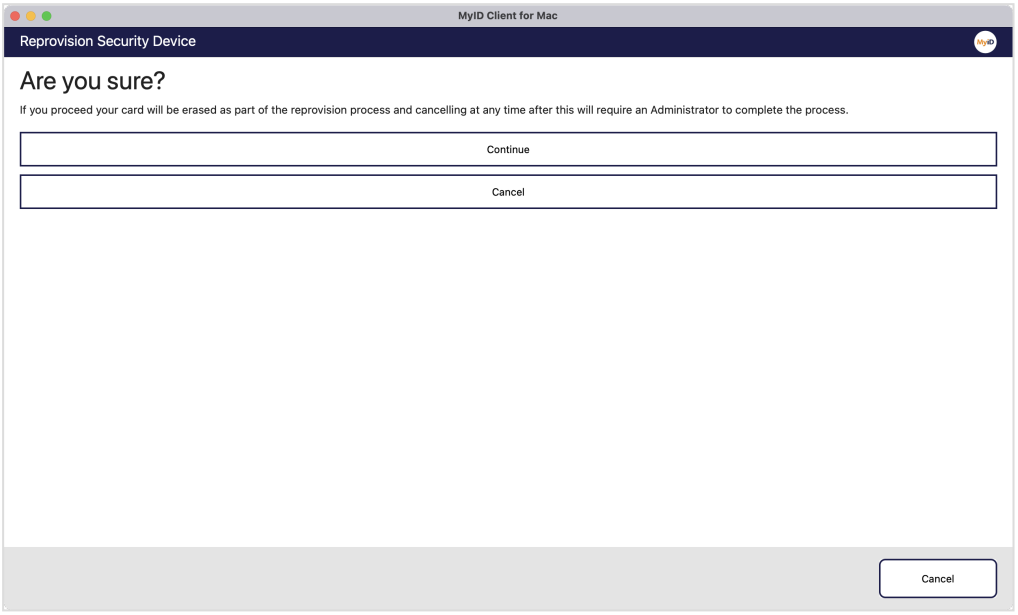


3. Insert the required device and click **Continue**.



4. Type your device PIN and click **Continue**.

   If the request has been configured to carry out a full reprovision, the MyID Client for Mac displays a confirmation screen.



   The MyID Client for Mac updates your device.

5.4 Collecting a replacement device

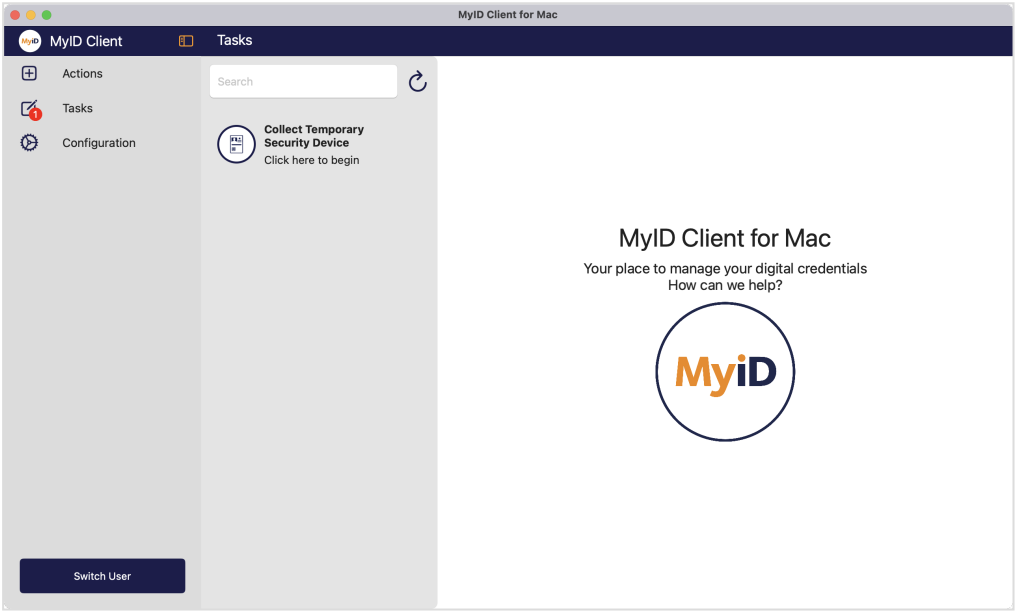
You can use the MyID Client for Mac to collect a temporary or permanent replacement device. For example, if you have forgotten your smart card, an operator can request a temporary smart card to allow you access to your systems.

Using this task requires access to the **Collect My Card** workflow in **Edit Roles**.

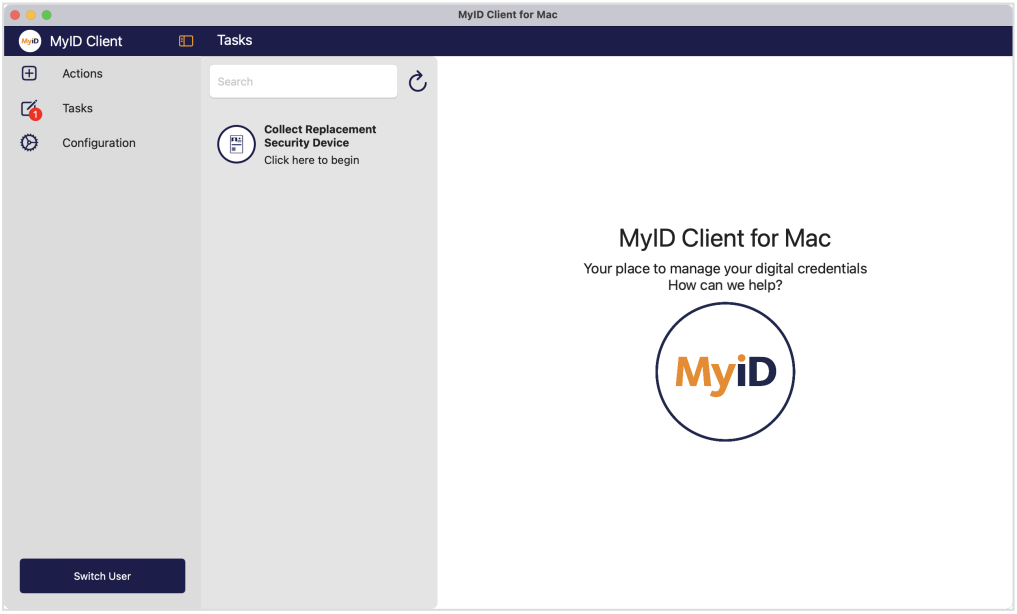
To collect a replacement device:

1. Click the **Tasks** option.

   The option presented depends on whether you have a temporary device waiting:

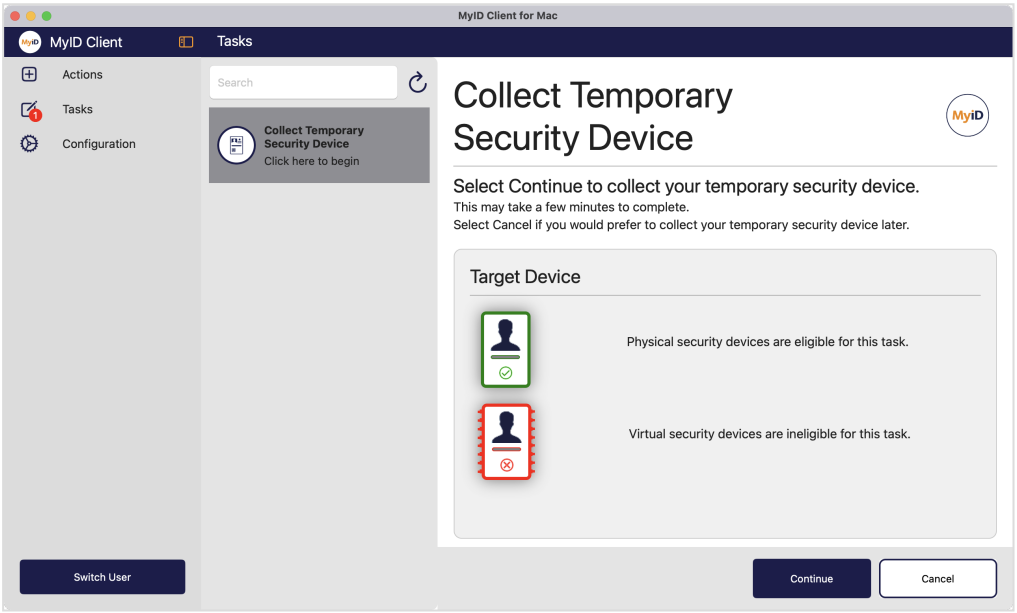


   Or a permanent replacement:



2. Click one of the following options:
   - **Collect Temporary Security Device** – collect a temporary device; for example, for a forgotten smart card.
   - **Collect Replacement Security Device** – collect a permanent replacement device; for example, for a damaged smart card.

   The MyID Client for Mac displays information about the target device that is required for this task.



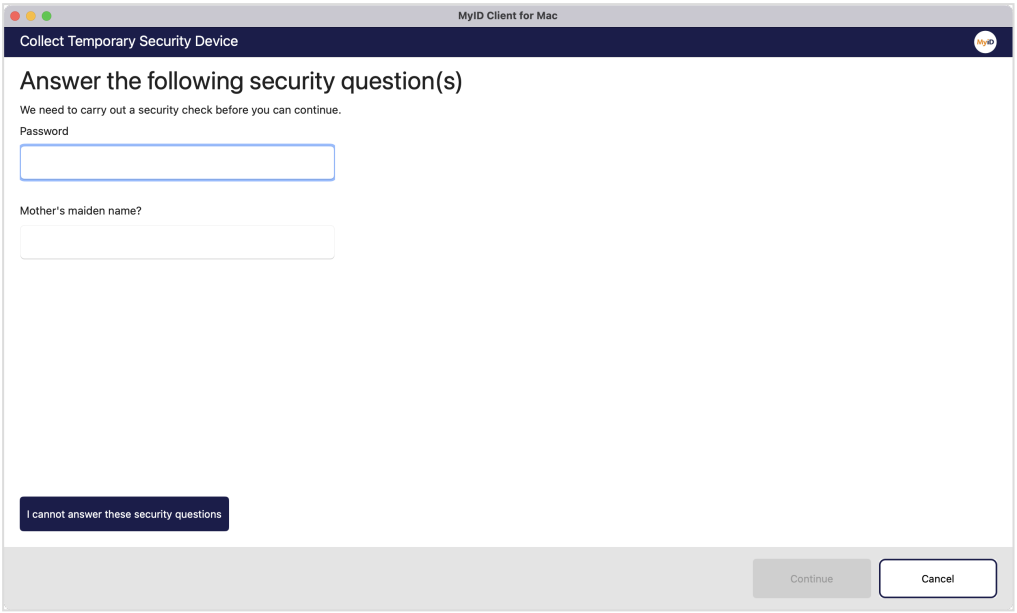
3. Click **Continue**.

   You must now authenticate to the MyID server.

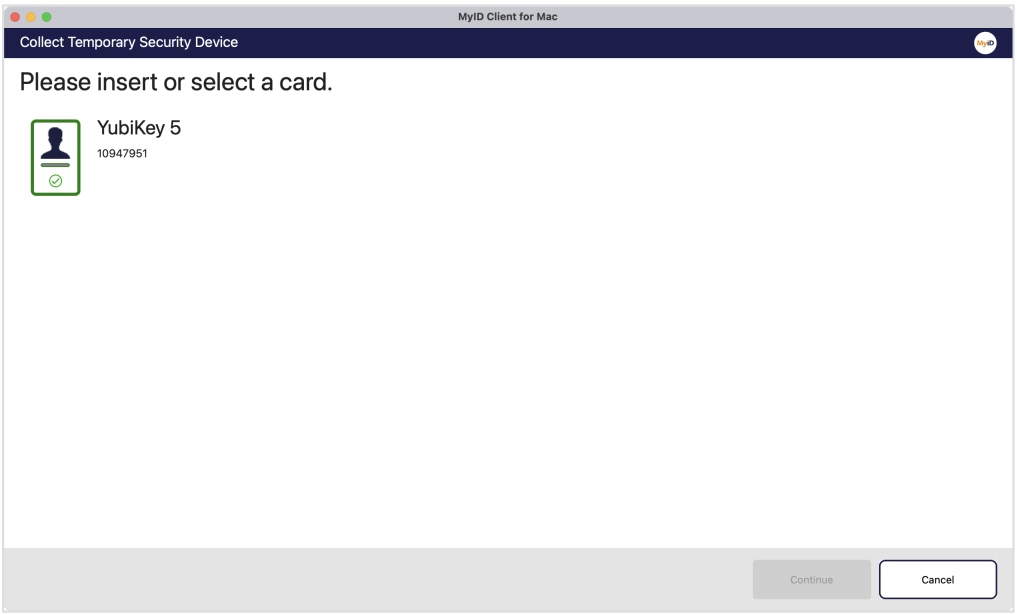
   You must have permission to authenticate using security phrases or an external identity provider.

   Note: The order of these authentication methods is determined by the **Logon Priority** tab in the **Security Settings** workflow in MyID Desktop. **Windows Logon** is not available as an option in the MyID Client for Mac; also, you cannot use an external identity provider if the credential profile for the device being collected requires activation.

   For details of using external identity providers, see the *Setting up an external identity provider* section in the ***MyID Authentication Guide***.

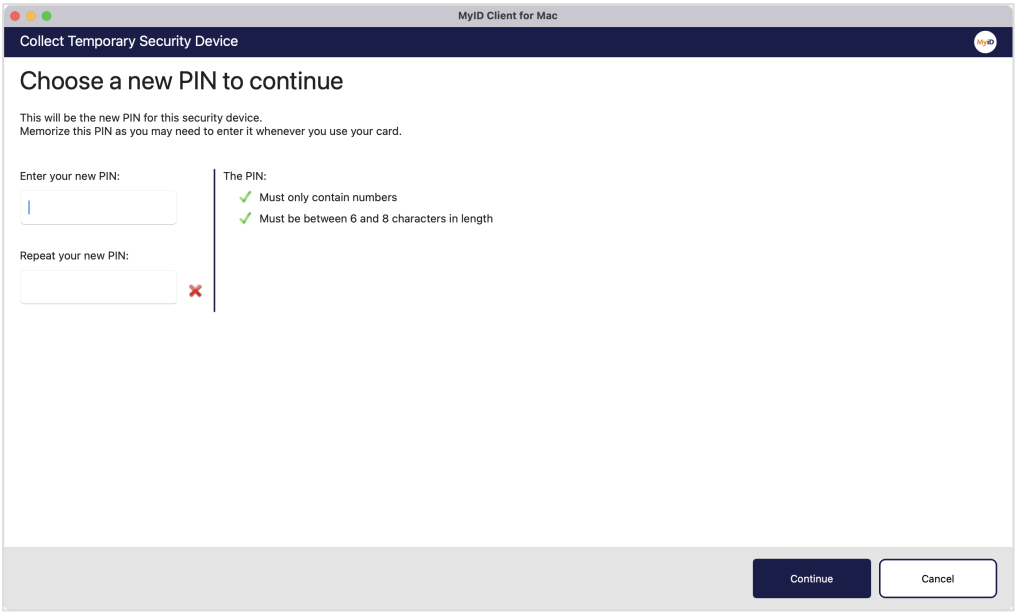


4. Provide your authentication details then click **Continue**.
5. Insert your smart card into a card reader, or your USB token into the USB port.



6. Select your device from the list and click **Continue**.

   You must now provide a PIN for your new device.



7. Type and confirm the new PIN for your device, then click **Continue**.

   The MyID Client for Mac issues your device.

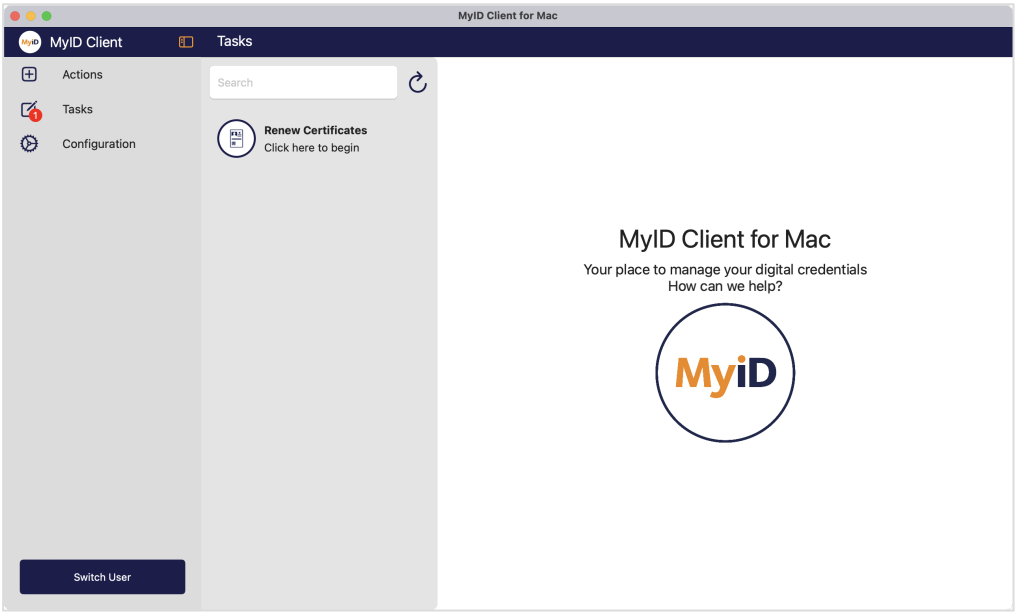
5.5 Collecting a certificate renewal

If you have been issued certificates that have been configured for automatic renewal, when the certificates are near expiry, MyID creates a task for you to collect an update for your device containing your renewed certificates.

Using this task requires access to the **Collect My Certificates** workflow in **Edit Roles**. In addition, this task requires a card that has been issued with MyID Logon capabilities; you must also be permitted to log on with a smart card.

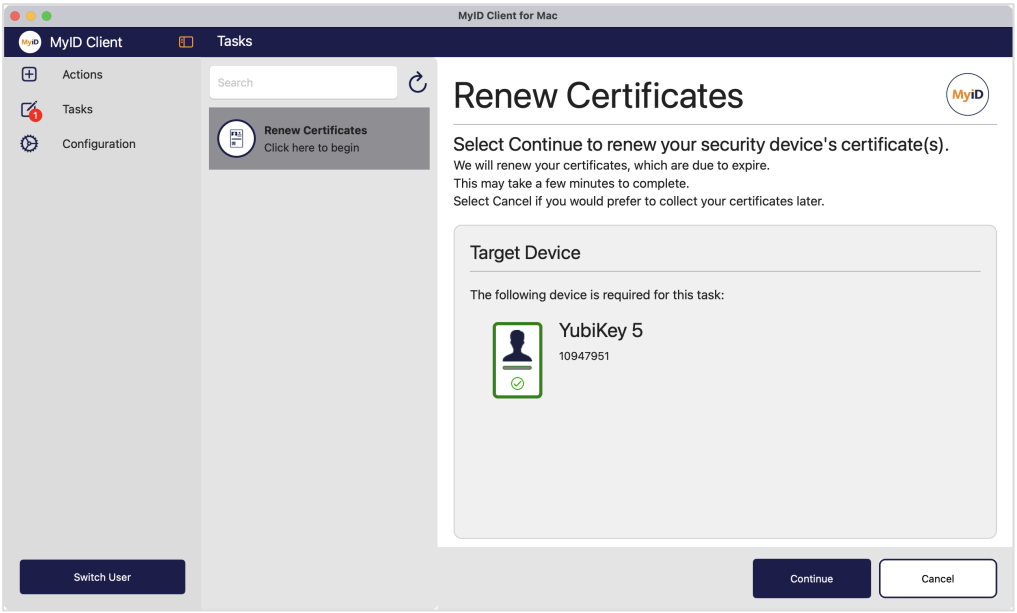
To collect a certificate renewal:

1. Click the **Tasks** option.



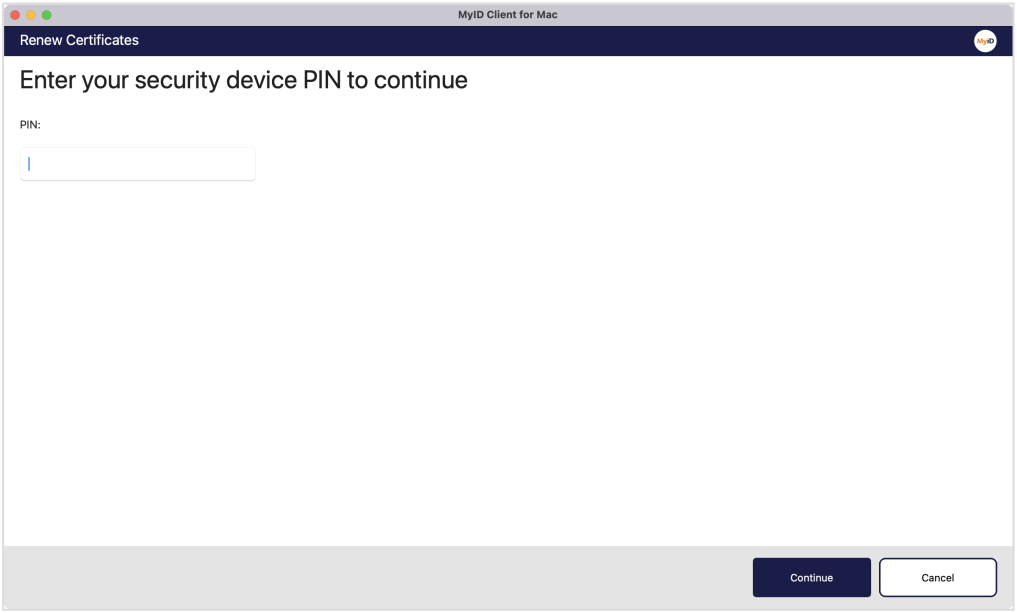
2. Click the **Renew Certificates** task in the list.

   The MyID Client for Mac displays information about the target device that is required for this task.



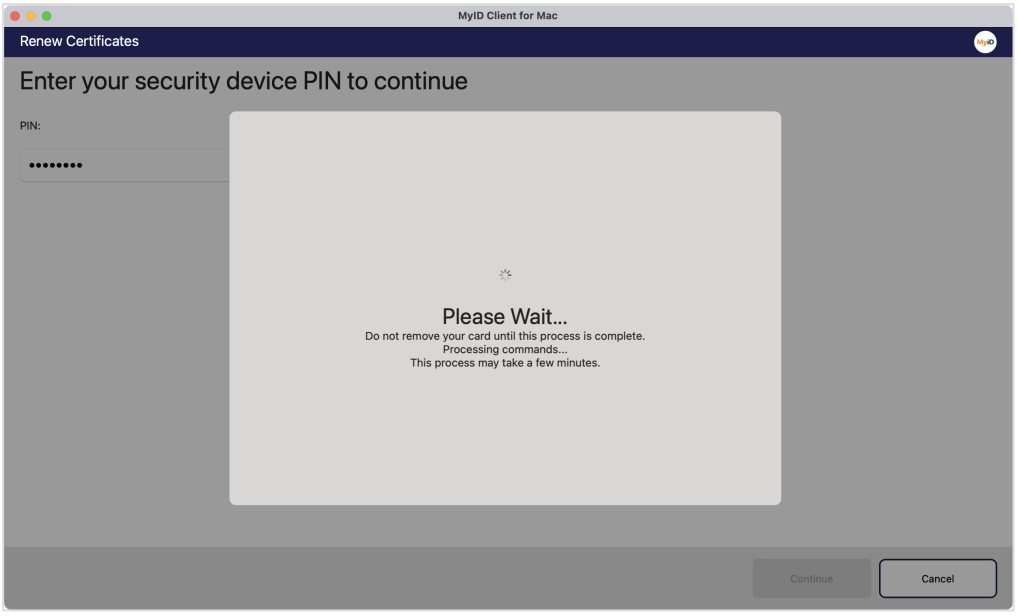
3. Insert your smart card into a card reader, or your USB token into the USB port, and click **Continue**.

   You must now provide the PIN for your device.



4. Type your PIN and click **Continue**.

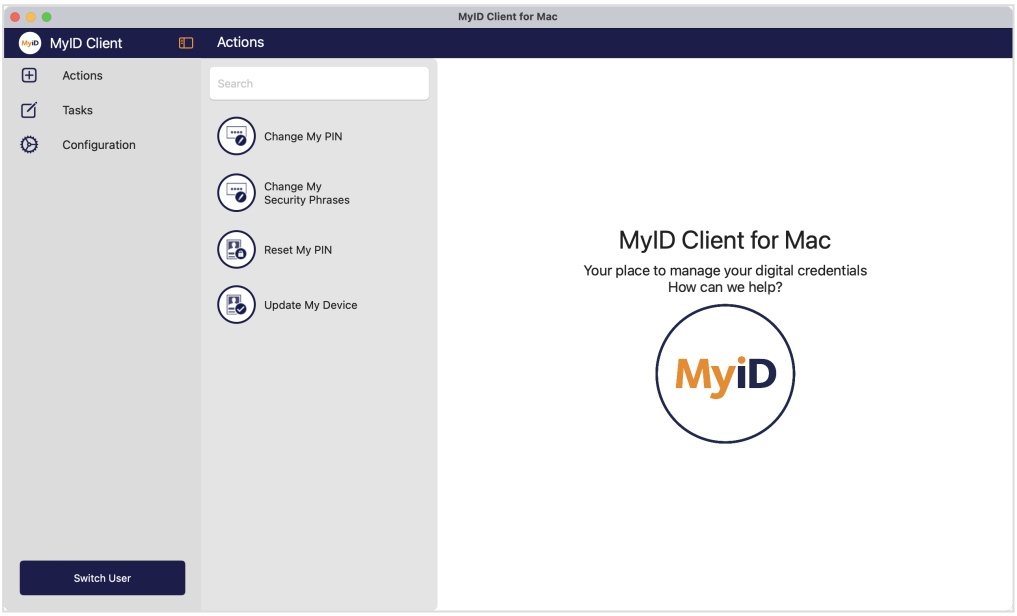
   The MyID Client for Mac updates your device with your renewed certificates.



6 Carrying out self-service actions

The MyID Client for Mac provides several features that you can use at any time, without asking for an operator to generate the task for you.

Click the **Actions** option, and the list of available actions appears. You can use the **Search** box to search for a particular action.



You can:

- Change the PIN of your device.

  See section *6.1*, *Changing your PIN*.
- Change your security phrases.

  See section *6.2*, *Changing your security phrases*.
- Reset your PIN if you do not know the current PIN.

  See section *6.3*, *Resetting your PIN*.
- Request and collect an update your device.

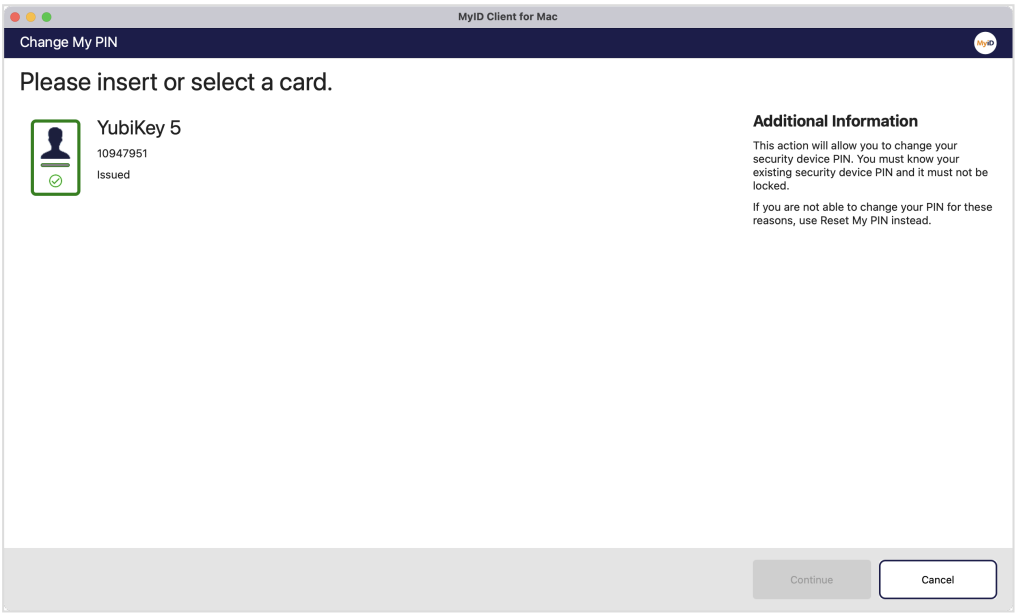
  See section *6.4*, *Updating your device*.

6.1 Changing your PIN

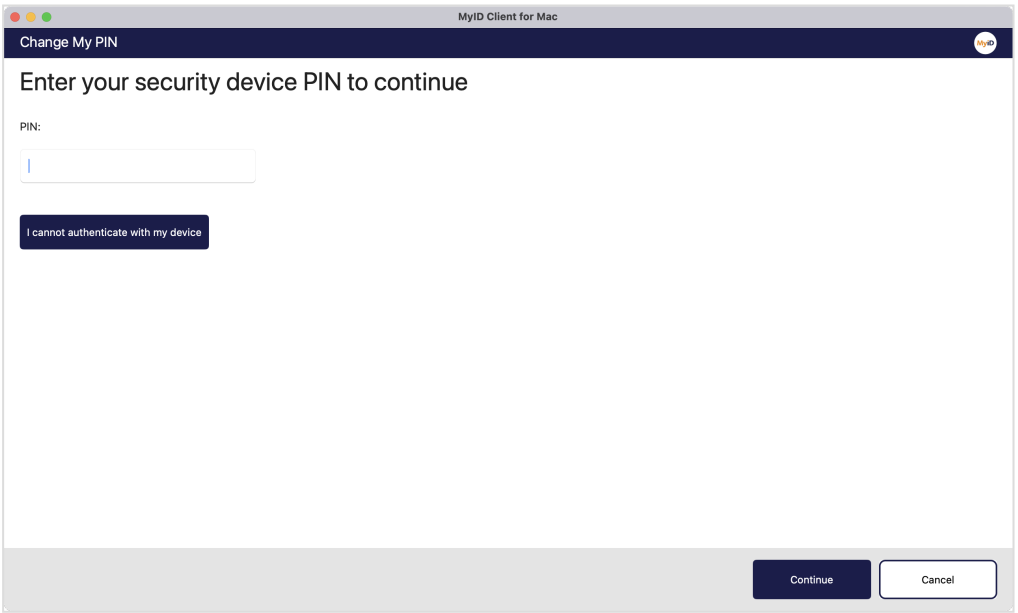
To change the PIN on your device, you must have a role that has access to the **Change PIN** workflow.

To change your PIN:

1. From the **Actions** list, click **Change My PIN**.

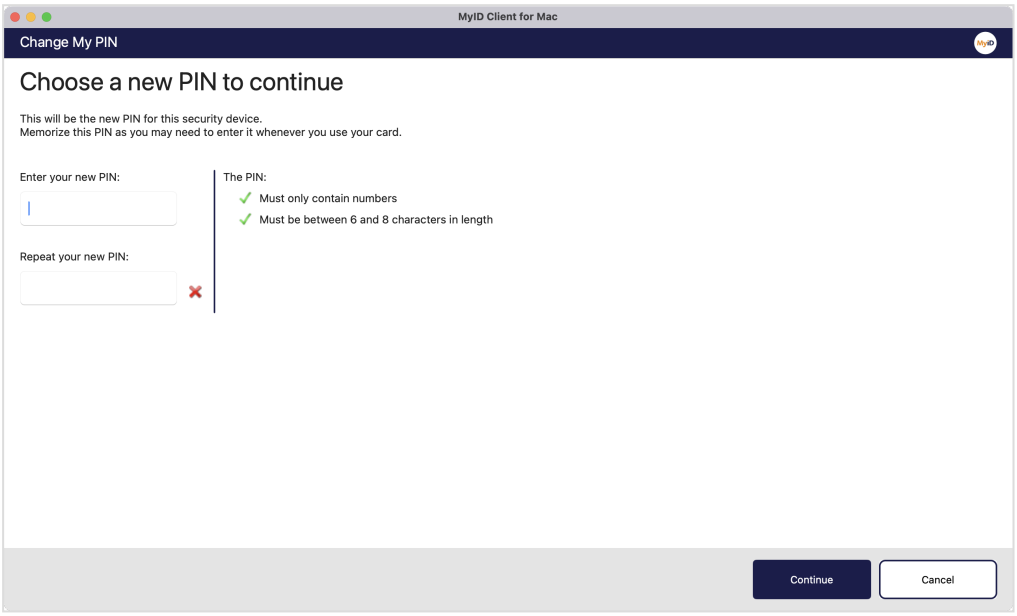


2. Insert your device into the card reader or USB slot, then select it from the list of displayed devices and click **Continue**.



3. Type the current **PIN** for your device, then click **Continue**.

   Note: If you do not know the PIN for your device, you may be able to use the **Reset My PIN** action to provide a new PIN. This feature requires additional configuration for your MyID system.



4. Type your new PIN and confirm it, then click **Continue**.

   The MyID Client for Mac updates your device with the new PIN.

6.2 Changing your security phrases

To change the PIN on your device, you must have a role that has access to the **Change My Security Phrases** workflow.

You must also have a way of authenticating yourself to the MyID Client for Mac – if you do not remember your existing security phrases, you must have an issued device. If you cannot remember your existing security phrases and do not have an issued device, you cannot use the MyID Client for Mac to change your security phrases, and must contact an operator who can change your security phrases for you.

To change your security phrases:

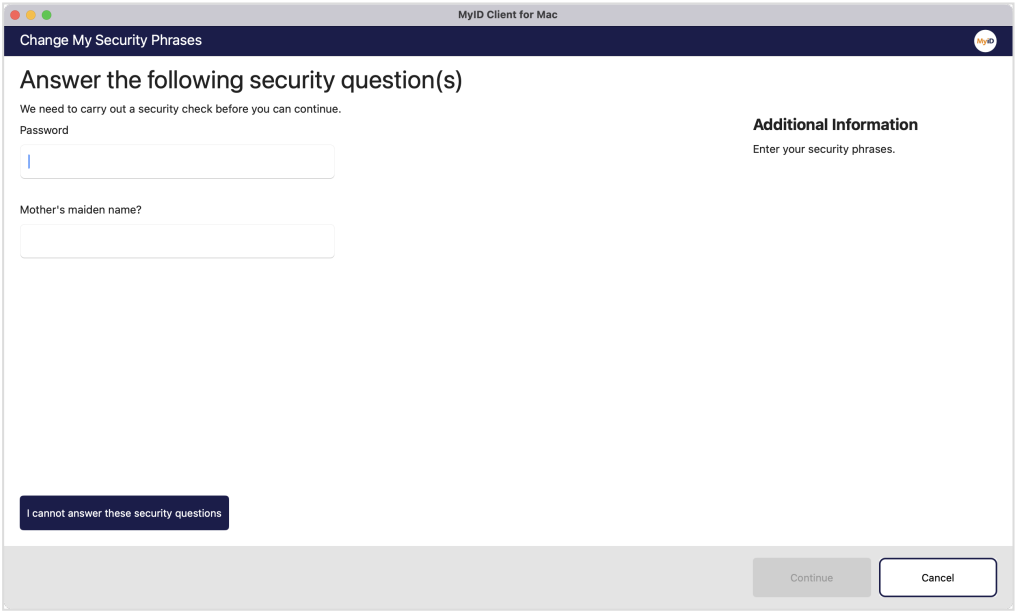
1. From the **Actions** list, click **Change My Security Phrases**.
2. Authenticate to the MyID Client for Mac.

   By default, the MyID Client for Mac checks first for an issued device. Insert the device and provide the PIN to continue.

   If you do not have an issued device, or do not have it available, the MyID Client for Mac checks for alternative methods of authentication.

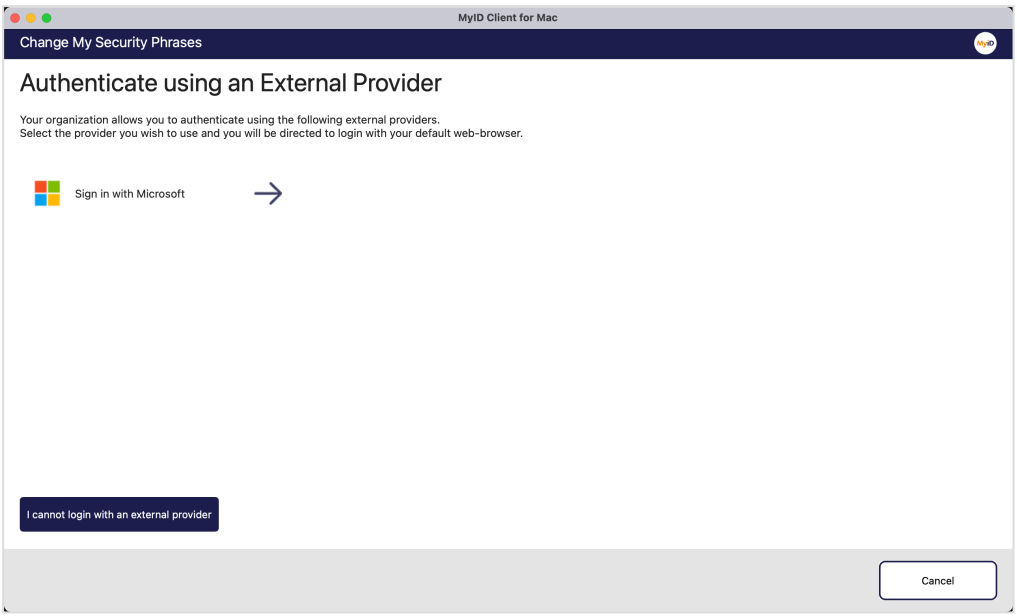
   Note: The order of these authentication methods is determined by the **Logon Priority** tab in the **Security Settings** workflow in MyID Desktop. **Windows Logon** is not available as an option in the MyID Client for Mac.

   To authenticate using security phrases, provide your existing security phrases to continue.



   To try an alternative method of authentication, click **I cannot answer these security questions**.

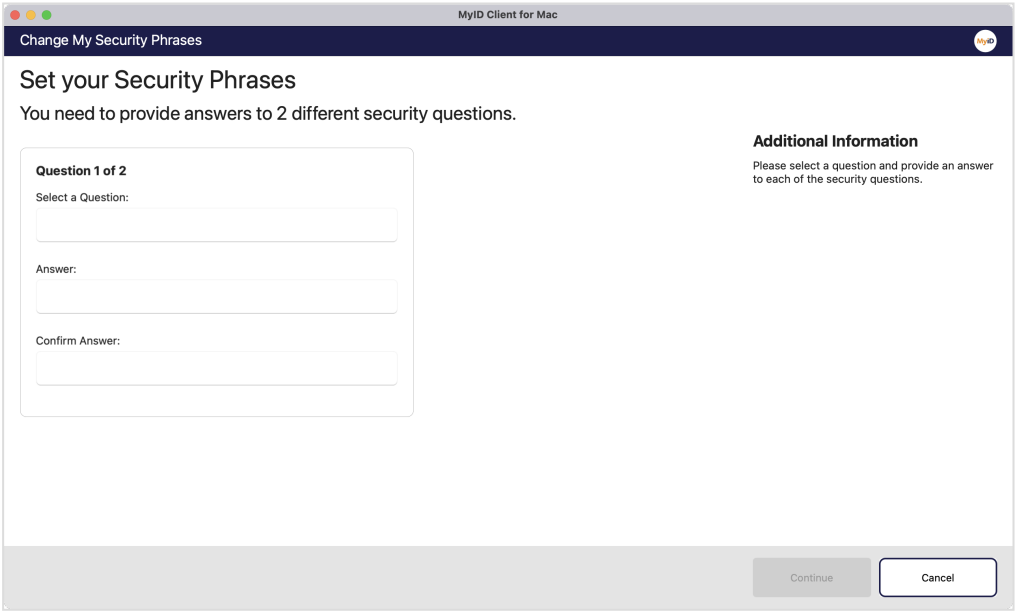
To authenticate using an external identity provider (for example, Microsoft Entra), click the link and authenticate using the external website.



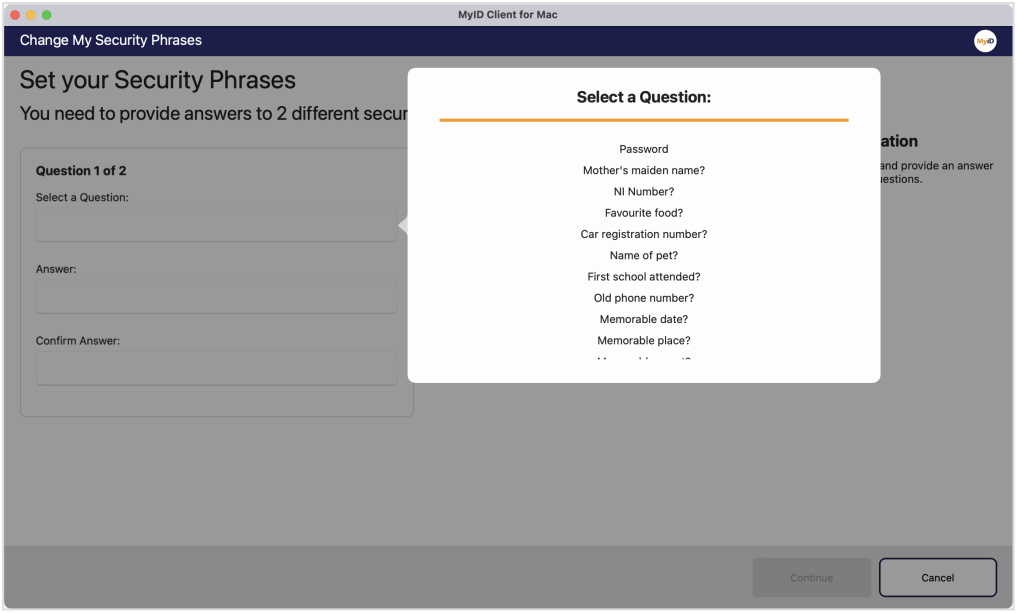
To try an alternative method of authentication, click **I cannot login with an external provider**.

For details of using external identity providers, see the *Setting up an external identity provider* section in the ***MyID Authentication Guide***.

Once you have authenticated, you can set your security phrases.



3. Select a question from the list.



4. Type your answer and confirm it, then click **Continue**.

   Note: By default, MyID is configured for two security phrases, except for the startup user, which requires only one. The number of security phrases is determined by the **Number of security questions to register** option on the **PINs** page of the **Security Settings** workflow in MyID Desktop. Repeat the process of selecting a question and typing your answer for each required security question.

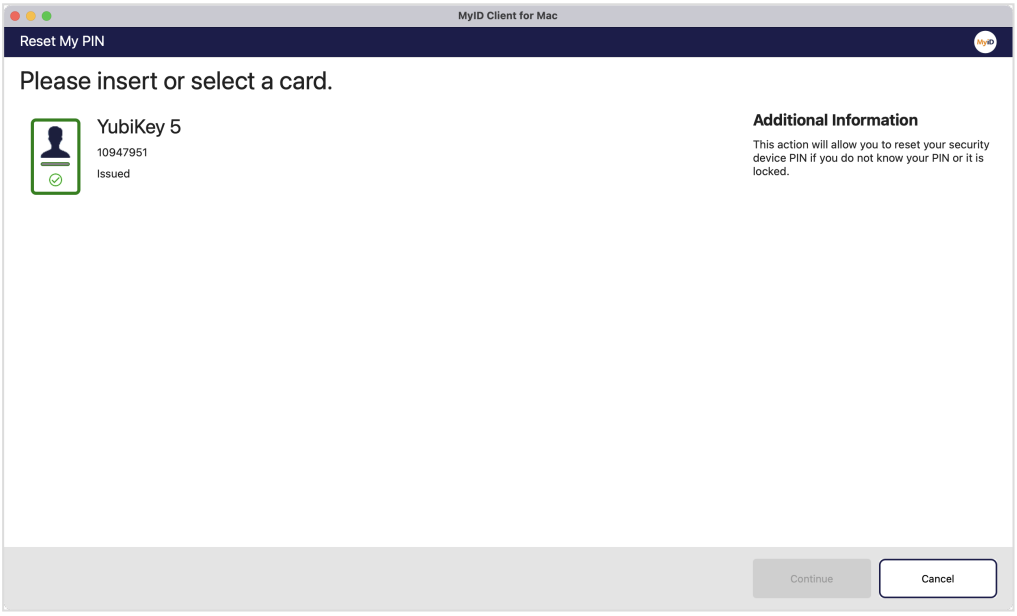
6.3 Resetting your PIN

To change the PIN on your device, you must have a role that has access to the **Unlock My Card** workflow.

For PIV systems, you must also carry out additional configuration. See the *Configuring self-unlock* section in the ***Web Service Architecture*** guide for details of editing the `AllowSelfUnlockForPIV` setting.

To reset the PIN of your device:

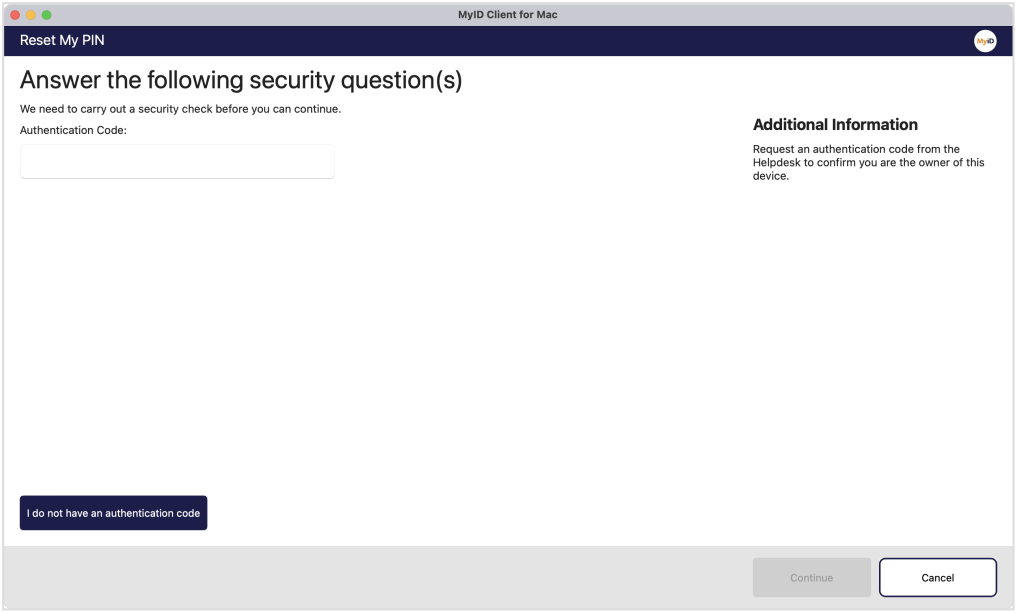
1. From the **Actions** list, click **Reset My PIN**.



2. Insert your device into the card reader or USB slot, then select it from the list of displayed devices and click **Continue**.

   Note: The authentication methods that you must carry out before resetting your PIN is determined by the **Logon Priority** tab in the **Security Settings** workflow in MyID Desktop, or through the **Self-Service Unlock Authentication** option in the credential profile.

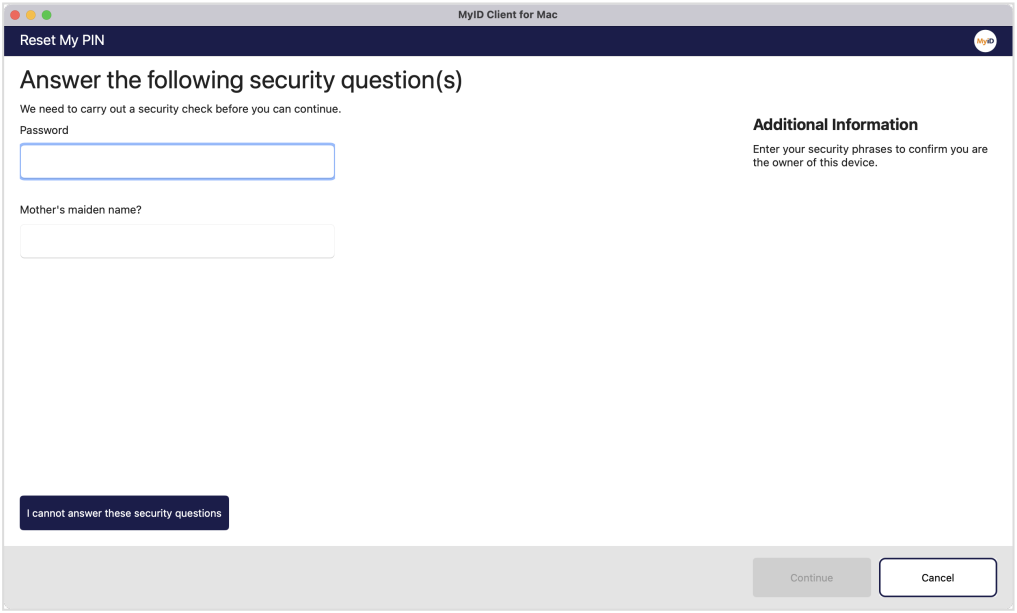
To authenticate using an authentication code, type your authentication code to continue.



A MyID operator can use the View Device screen in the MyID Operator Client to send or read out an authentication code for your device that you can use to continue.

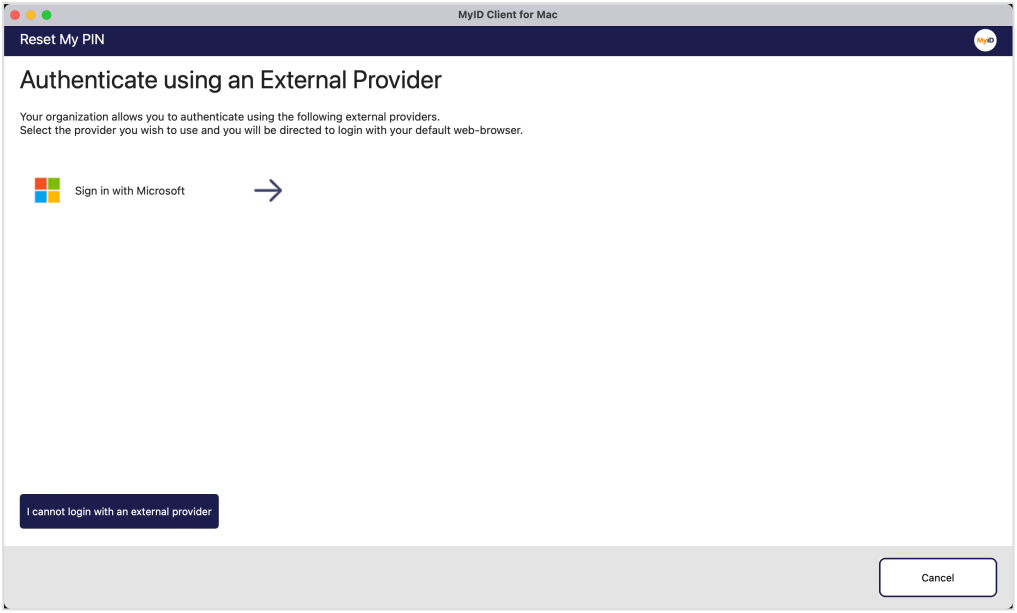
If you do not have an authentication code, click **I do not have an authentication code**.

To authenticate using security phrases, provide your security phrases to continue.



To try an alternative method of authentication, click **I cannot answer these security questions**.

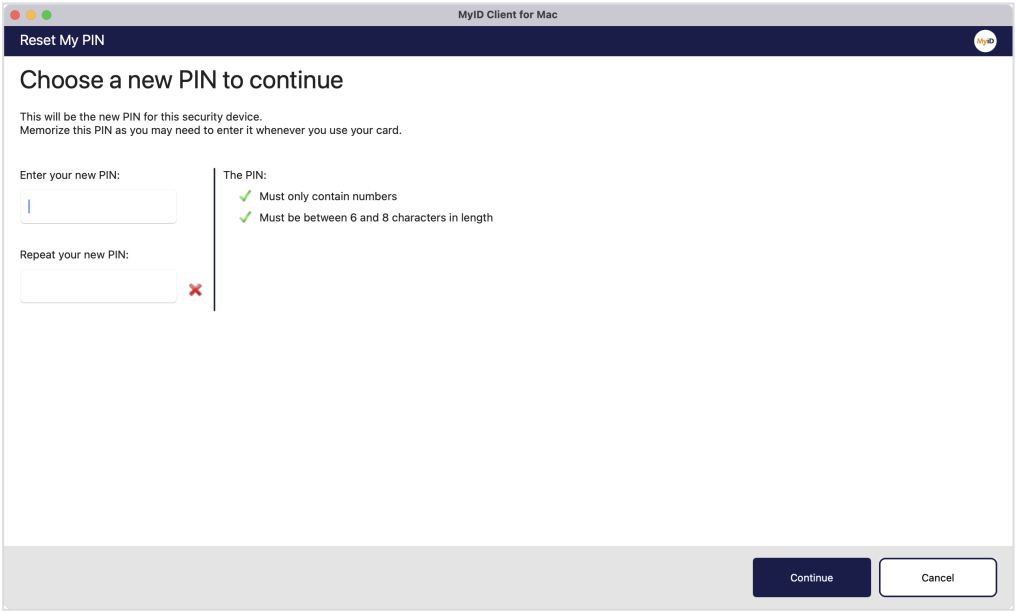
To authenticate using an external identity provider (for example, Microsoft Entra), click the link and authenticate using the external website.



To try an alternative method of authentication, click **I cannot login with an external provider**.

For details of using external identity providers, see the *Setting up an external identity provider* section in the ***MyID Authentication Guide***.

Once you have authenticated, you can set your new PIN.



3. Type and confirm your new PIN.

   The MyID Client for Mac updates your device with the new PIN.

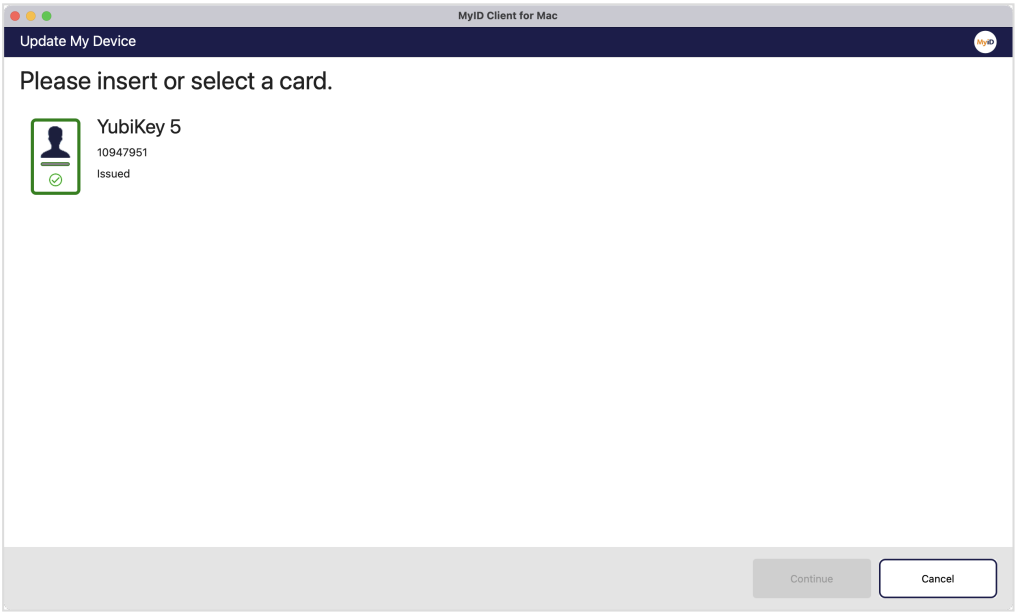
6.4 Updating your device

To carry out an update for your device, you must have a role that has access to the **Collect My Updates** and **Update My Device** workflows.

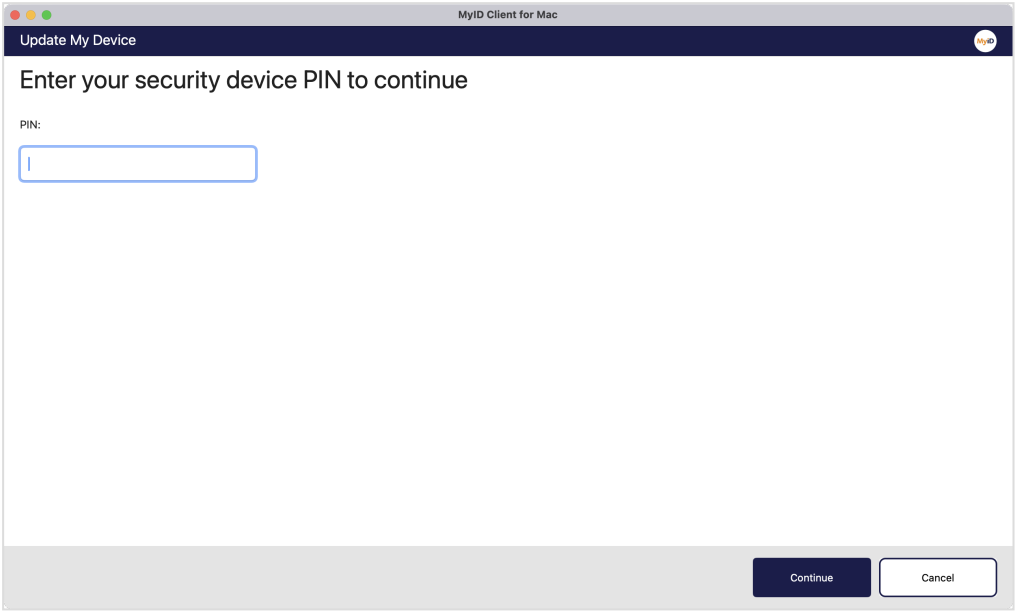
Note: Self-service device update requires additional configuration, as it may not be suitable for all organizations. This configuration also determines what sort of device update is available; you may be able to update your device to the latest credential profile, or you may be able to reprovision your device completely. See section *3.2*, *Setting up self-service device update*.

To request and collect an update for your device:

1. From the **Actions** list, click **Update My Device**.

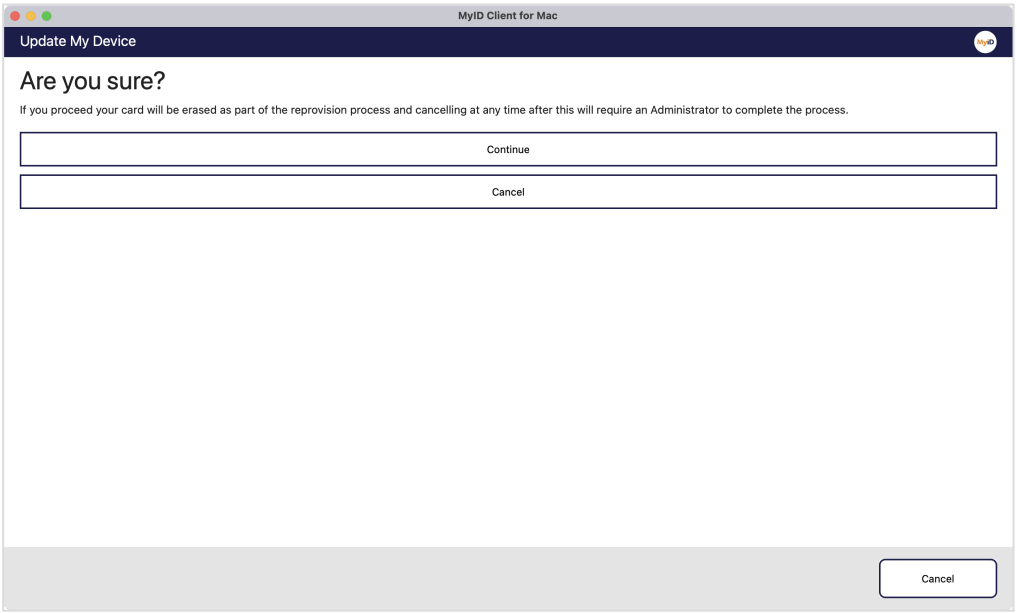


2. Insert your device into the card reader or USB slot, then select it from the list of displayed devices and click **Continue**.

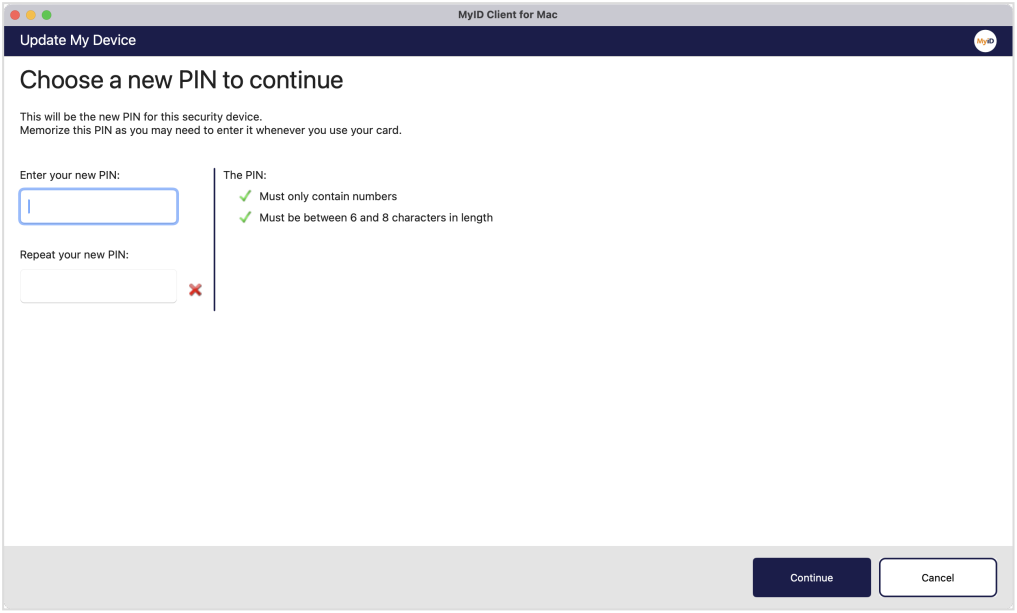


3. Type the PIN for your device, then click **Continue**.

   If your system has been configured to carry out a full reprovision for self-service device updates, the MyID Client for Mac displays a confirmation screen.



Click **Continue**.



4. Type and confirm your new PIN, then click **Continue**.

   The MyID Client for Mac updates your device.

7 Configuring the MyID Client for Mac

You can configure the MyID Client for Mac in the following ways:

- Using the Configuration screen within the MyID Client for Mac.

  See section *7.1*, *Setting configuration options within the MyID Client for Mac*.
- Using an administrator override configuration file.

  See section *7.2*, *Setting up an administrator configuration override file*.

7.1 Setting configuration options within the MyID Client for Mac

To set the configuration options:

1. Select the **Configuration** option.

   The configuration screen appears.
2. Scroll to the appropriate section and set the relevant options.

   Note: Your administration may have restricted your ability to change some or all of your configuration options.
3. Click **Apply Changes**.

   To revert to the previous settings, click **Revert Changes**.

   To go back without making any changes, click **Back**.

7.1.1 Administrator-configured options

Your administrator may have set up a configuration override file that provides default values or prevents you from changing values; see section *7.2*, *Setting up an administrator configuration override file*.

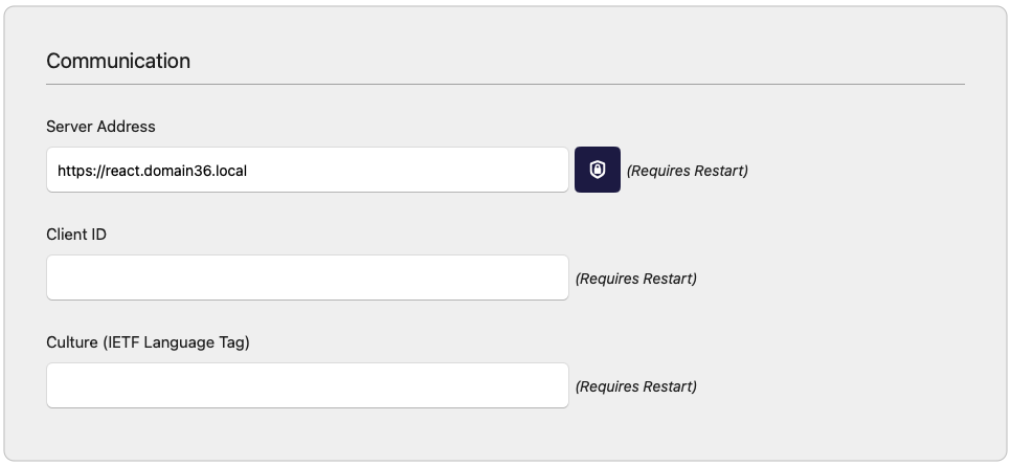
The MyID Client for Mac displays icons next to the option fields for administrator-configured options:

Icon	Description
	The value was provided by an administrator configuration override file.
	The value was provided by an administrator configuration override file, and the current value is different from the administrator-provided value; click the icon to revert to the administrator-configured value.

7.1.2 Setting communication options

To set the communication options:

1. Select the **Configuration** option.



2. In the Communication section, set the following options:
   - **Server Address** – type the address of the MyID web services server.

     For example:

     `https://myid.example.com`

     Note: You must start the server address with `https://`.
   - **Client ID** – optionally, type a unique identifier that the MyID Client for Mac uses to identify itself to the server.

     You can capture this information in the audit to determine which workstation originated a request. See the *Logging the client IP address and identifier* section in the ***Administration Guide*** for details.
   - **Culture (IETF Language Tag)** – provide an IETF language tag (for example, `en-US`) that overrides the default behavior of using the language culture setting of the operating system; for example, you may have a UK English system but want to display the MyID Client for Mac interface in US English.
3. Click **Apply Changes**.

Note: For these settings to take effect, you must restart the MyID Client for Mac.

7.1.3 Setting authentication options

To set the authentication options:

1. Select the **Configuration** option.

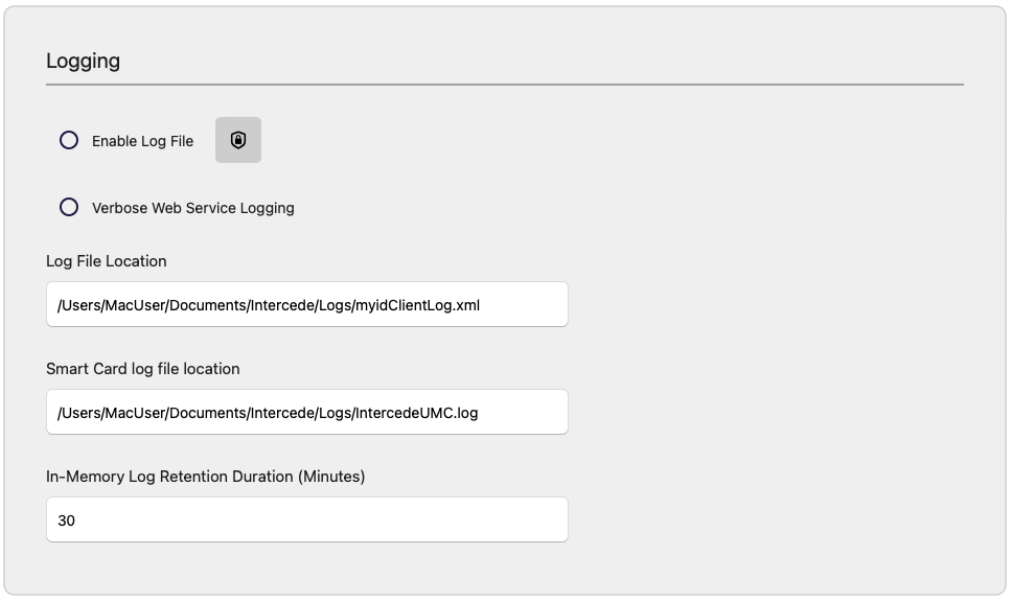
2. In the Authentication section, set the following options:
   - **Username** – optionally, type the username you want to the MyID Client for Mac to use each time you start it up.
   - **Enable 'Remember Me'** – select this option to allow users to store their username between sessions.
3. Click **Apply Changes**.

Note: For these settings to take effect, you must restart the MyID Client for Mac.

7.1.4 Setting logging options

To set the logging options:

1. Select the **Configuration** option.



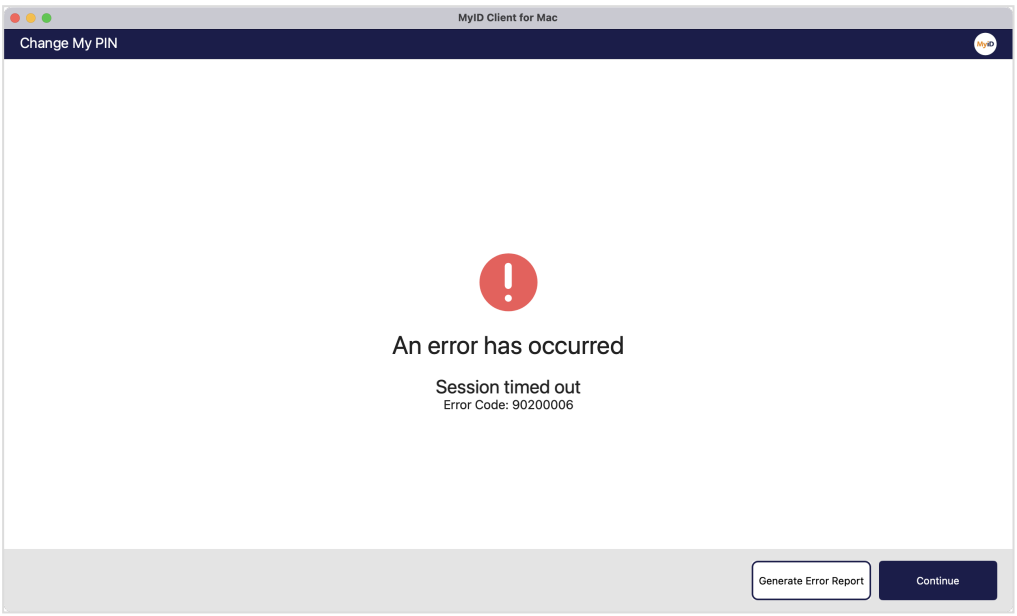
2. In the Logging section, set the following options:
   - **Enable Log File** – select this option to enable logging.
   - **Verbose Web Service Logging** – select this option to log all network communication with MyID. You are recommended to use this only for diagnostics, as it may result in sensitive information being included in the logs.
   - **Log File Location** – type the location to which you want to write the log file.
   - **Smart Card log file location** – type the location to which you want to write the smart card log file.

     Smart card log events are stored separately from general log events.
   - **In-Memory Log Retention Duration (Minutes)** – type the number of minutes of log entries to retain in memory. This log is used for just-in-time error reports. After the configured number of minutes, log events are discarded. By default, reports contain the last 30 minutes of log entries.
3. Click **Apply Changes**.

You can also generate a just-in-time log when an error occurs; this does not require logging to be enabled, but is always available.

To generate a just-in-time error report:

1. Carry out an operation that generates an error.



2. Click **Generate Error Report**.
3. Select the folder into which you want to write the report, then click **Open**.
4. Click **OK**.

7.1.5 Setting accessibility options

You can set the page timeout for the MyID Client for Mac screens. The page timeout is used for security reasons; for example, when setting a new PIN for your device. You may want to increase the timeout value if, for example, you are using a screen reader that increases the time it takes to use the screen.

To change the page timeout:

1. Select the **Configuration** option.

2. In the Accessibility section, set the following option:
   - **Page Timeout** – type the number of seconds that you want to allow before the page times out.
3. Click **Apply Changes**.

7.1.6 Setting advanced options

You can set advanced configuration options for which there is no dedicated field on the configuration screen.

For example, if you are using a version of MyID CMS earlier than 12.11, you must set the `UseLegacySsaPlatform` configuration option to `true` to allow the MyID Client for Mac to impersonate the Self-Service App and be recognized by the server.

To set a custom configuration option:

1. Select the **Configuration** option.

2. In the Advanced Configuration section, type a **Key** and a **Value** for the option.

   For example:

   - **Key** – `UseLegacySsaPlatform`
   - **Value** – `true`

3. Click **Add**.
4. Click **Apply Changes**.

7.1.6.1 Advanced configuration options

The following advanced configuration options are available:

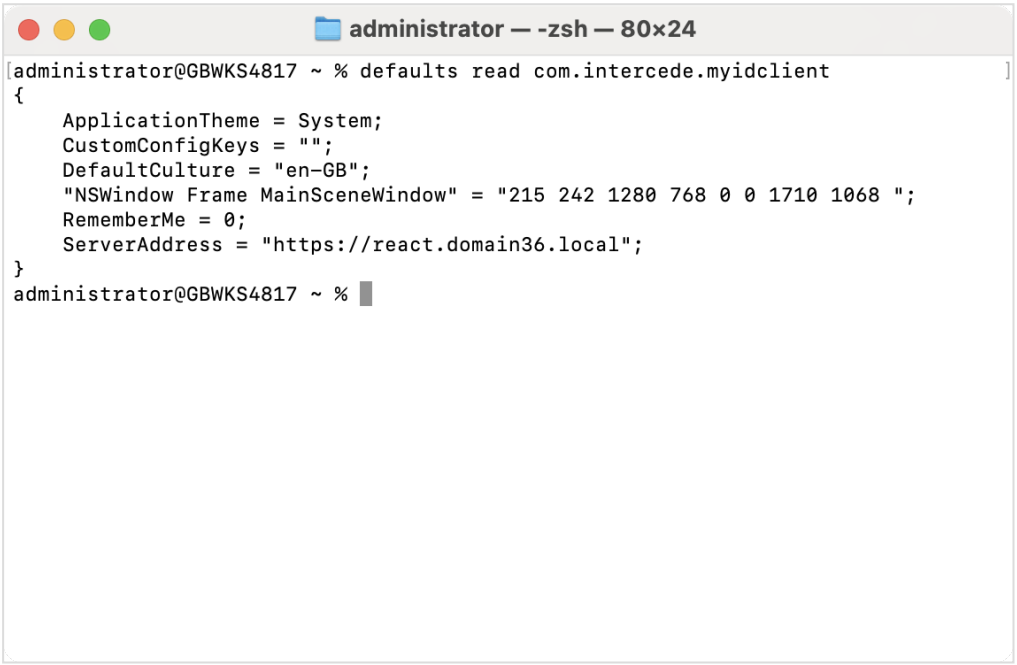
Option	Description
`UseLegacySsaPlatform`	If you are using a version of MyID CMS earlier than 12.11, you must set the `UseLegacySsaPlatform` configuration option to `true` to allow the MyID Client to impersonate the Self-Service App and be recognized by the server.
`UseLegacyPassphraseCollection`	If you are using a version of MyID CMS earlier than 12.12, you must set the `UseLegacyPassphraseCollection` configuration option to `true` allow the MyID Client to use the old web-service endpoint; if you set this configuration option, support for authentication using external identity providers is disabled.
`CardPickerHeaderPrecedence`	When displaying devices for selection, the MyID Client tries to use the most recognizable information available as the header for the device in the list. By default, the precedence is: • Device Friendly Name. • Cardholder Name. • Device Type Name. If you want to change this precedence, set the `CardPickerHeaderPrecedence` option to a semi-colon delimited list of the options in your preferred order. • `dfn` – Device Friendly Name. • `chn` – Cardholder Name. • `dtn` – Device Type Name. For example: • `dfn;chn;dtn` – the default precedence. • `chn;dfn;dtn` – prefer the cardholder name over the device friendly name where available. • `dtn` – always use device type name.

7.1.7 Accessing configuration options from the Terminal

The MyID Client for Mac configuration options are stored under `com.intercede.myidclient` in the user's defaults registry.

To view the configuration options for the current user, at the Terminal, type:

```
defaults read com.intercede.myidclient
```



To write a user setting, type:

```
defaults write com.intercede.myidclient MyCustomKey MyValue
```

To delete all user settings for the current user, type:

```
defaults delete com.intercede.myidclient
```

7.2 Setting up an administrator configuration override file

As an administrator, you can provide a configuration file that provides overrides to the user's preferences; you can also specify whether the user can override these defaults.

To provide a configuration override file, create the following file:

`/Library/Intercede/MyID Client/MyIDClientConfig.xml`

For example:

```
<configuration>
    <appSettings>
        <add key="ServerAddress" value="http://myid.example.com"/>
        <add key="Username" value="susan.smith"/>
        <add key="EnableRememberMe" value="true"/>
        <add key="ClientID" value="c522dd89-a35d-4de6-b8d8-35d97614fc69"/>
        <add key="UseLegacySsaPlatform" value="true"/>
        <add key="UseLegacyPassphraseCollection" value="false"/>
        <add key="EnableLogging" value="false" isUserOverridable="true"/>
        <add key="LogFilePath" value="~/Documents/myidlog.xml" isUserOverridable="true"/>
        <add
key="UmcLogFilePath" value="~/Documents/umclog.xml" isUserOverridable="true"/>
        <add key="EnableWebServiceLogging" value="false" isUserOverridable="false"/>
        <add key="CardPickerHeaderPrecedence" value="dfn;chn;dtn">
    </appSettings>
</configuration>
```

Each option contains a `key` and a `value`. By default, if the option exists in the configuration file, the user cannot use the Configuration screen in the MyID Client for Mac to override it; if you want the user to be able to override it, you can add `isUserOverridable="true"` to the option.

The following options are available:

- `ServerAddress` – corresponds to the **Server Address** field in the Communication section.
- `Username` – corresponds to the **Username** field in the Authentication section.
- `EnableRememberMe` – corresponds to the **Enable 'Remember Me'** option in the Authentication section.
- `ClientID` – corresponds to the **Client ID** field in the Communication section.
- `UseLegacySsaPlatform` – set this option to `true` to allow you to use the MyID Client for Mac with MyID CMS servers from version 12.4 to version 12.10. This setting is not required for MyID 12.11 or later.
- `UseLegacyPassphraseCollection` – set this option to `true` to allow you to use the MyID Client for Windows with MyID CMS servers earlier than version 12.12. This setting is not required for MyID 12.12 or later.

  Note: If you set this configuration option, support for authentication using external identity providers is disabled.
- `EnableLogging` – corresponds to the **Enable Log File** option in the Logging section.
- `LogFilePath` – corresponds to the **Log File Location** field in the Logging section.
- `UmcLogFilePath` – corresponds to the **Smart Card log file location** field in the Logging section.
- `EnableWebServiceLogging` – corresponds to the **Verbose Web Service Logging** option in the Logging section.
- `CardPickerHeaderPrecedence` – allows you to set the precedence for the label used when selecting a device. See section *7.1.6.1*, *Advanced configuration options* for details.