MyID MFA and PSM

Version 5.3

Web Management Portal User Guide

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

Document reference: USR2080-5.3.0

October 2025

Copyright

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.

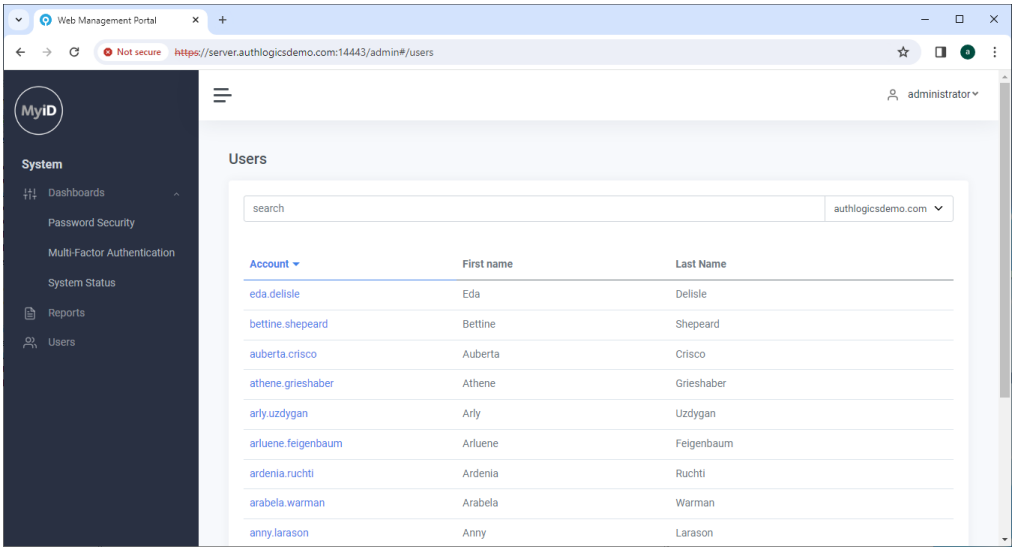
Contents

1 Introduction

The MyID Web Management Portal provides operational staff with an easy-to-use web-based interface to perform common administrative tasks. The Web Management Portal UI is well suited to tablets and other touch-based devices.

The Operators role gives you access to the Web Management Portal.

The Web Management Portal includes dashboards to provide a high-level overview of core Password Security and Multi-Factor Authentication events. The dashboard also provides administrators with the ability to generate reports.



Day-to-day user management functions available through the Web Management Portal include:

- Viewing all MyID events for the selected user.
- Enabling or disabling an account.
- Unlocking an account.
- Updating a Mobile / Cellular phone number.
- Resetting user passwords.
- Configuring Temporary Access Codes.
- Viewing, enabling, and disabling MFA devices.
- Configuring MFA settings.
- Resetting a Grid Pattern.
- Resetting Phrase answers.
- Resetting a One Time Code PIN.
- Verifying a One Time Code.
- Performing two-way identification.

The Web Management Portal does *not* allow the following actions:

- Modification of the global settings.
- Adding new user accounts.
- Provisioning MFA technologies.
- Changing the Pattern size.
- Changing logon times.

For these operations, you must use the MyID Management Console instead.

The Web Management Portal is compatible with multiple web browsers including Microsoft Edge, Google Chrome, Firefox, and Safari. Internet Explorer may function but is no longer recommended or supported.

2 Accessing the Web Management Portal

You can access the Web Management Portal using Forms-based authentication with MFA or passwords, or Windows-based authentication.

There is a start menu shortcut on the MyID server for easy access. Alternatively, you can use the following URL from any remote location:

```
https://<servername>:14443/admin
```

Where `<servername>` is the name of your MyID Authentication Server.

You can access the portal using HTTPS on port TCP:14443.

The installation process configures a self-signed SSL certificate for use with the MyID Authentication Server. You can replace this certificate with one from an internal or third-party trusted root when needed.

The methods available for logging in are determined by the Web Management Portal's internal authentication settings. For information on this, see the *Web Management Portal Properties* section in the ***MyID Authentication Server Installation and Configuration Guide***.

To access the Web Management Portal, you must have the **Administrators**, **Operators**, or **Auditors** role.

Users with the **Administrators** or **Operators** role have full access to the Web Management Portal. Users with the **Auditors** role have read-only access to the Web Management Portal – this allows them to view dashboards, reports, and individual user's settings but does *not* allow them to change user settings.

For information on setting user roles, see the *Roles* section of the ***MyID Authentication Server Installation and Configuration Guide***.

3 Web Management Portal dashboards

Web Management Portal dashboards give you a visual overview of MyID MFA and PSM on your system.

To use the Web Management Portal dashboards, in the System section of the Web Management Portal, click **Dashboards**.

The dashboards are broken into the following categories:

- System Status.

  See section *3.1*, *System Status*.

- Multi-Factor Authentication – the availability of this is dependent on your applied MFA and PSM licenses.

  See section *3.2*, *Multi-Factor Authentication*.

- Password Security – the availability of this is dependent on your applied MFA and PSM licenses.

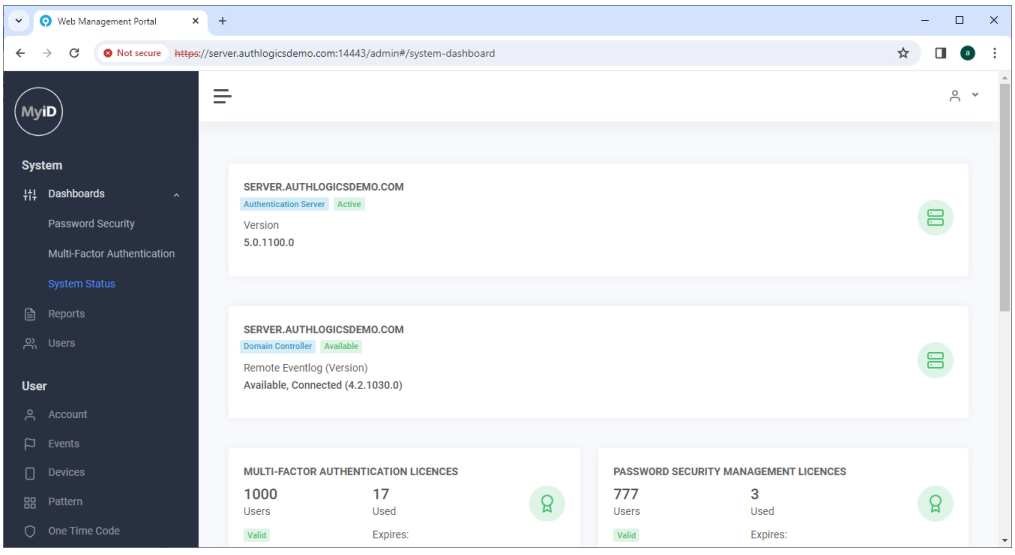
  See section *3.3*, *Password Security*.

3.1 System Status

The System Status dashboard shows all the MyID Authentication servers, Domain Controllers, and applied licenses through the deployment.

Each server listing shows the role of the server in the environment (whether it is a MyID Authentication Server and/or a Domain Controller), the server's availability state, and lists MyID's ability to access the server's Windows Event Logs.

The license components show the applied licenses, the validity of the licenses, the quantities of the license assigned and used, as well as the license's expiry date.



- **IKB-452 – Authentication servers appear inactive in the System Status dashboard when using a load balancer**

  The reporting service polls the web REST APIs on port 14443 for the server version to determine if the respective authentication server is online; however, if the web server is configured to another port (for example, 443, the default SSL port) this call fails to resolve, resulting in the server appearing inactive.

  To resolve this, set the following registry key:

  `HKLM\SOFTWARE\Authlogics\Authentication Server\AuthlogicsServerPort`

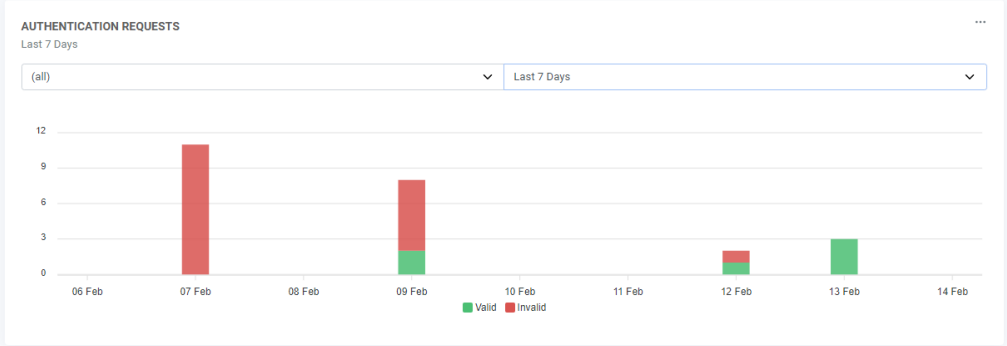
  to the port being used; for example, `443`.

  You can check the `AuthenticationServerManager.log` file for the `AuthenticationServerManager.load` call to see the exact server port configuration being loaded.

3.2 Multi-Factor Authentication

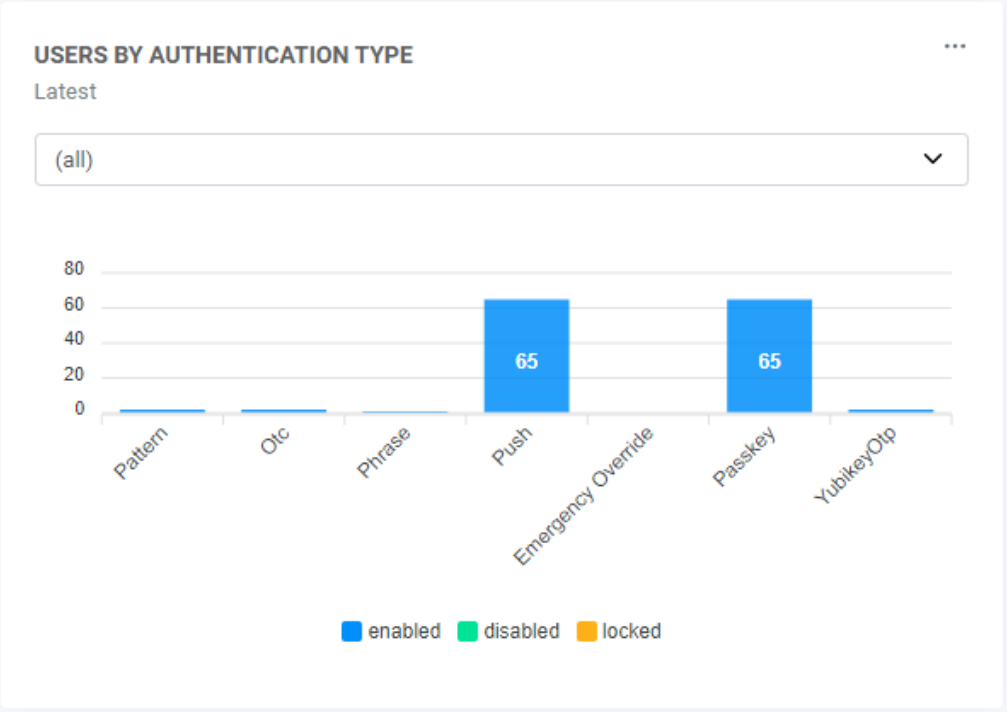
The Multi-Factor Authentication dashboard shows a near-live view of:

- **Authentication Requests** – displays all valid and invalid MFA authentication requests over the selected period.

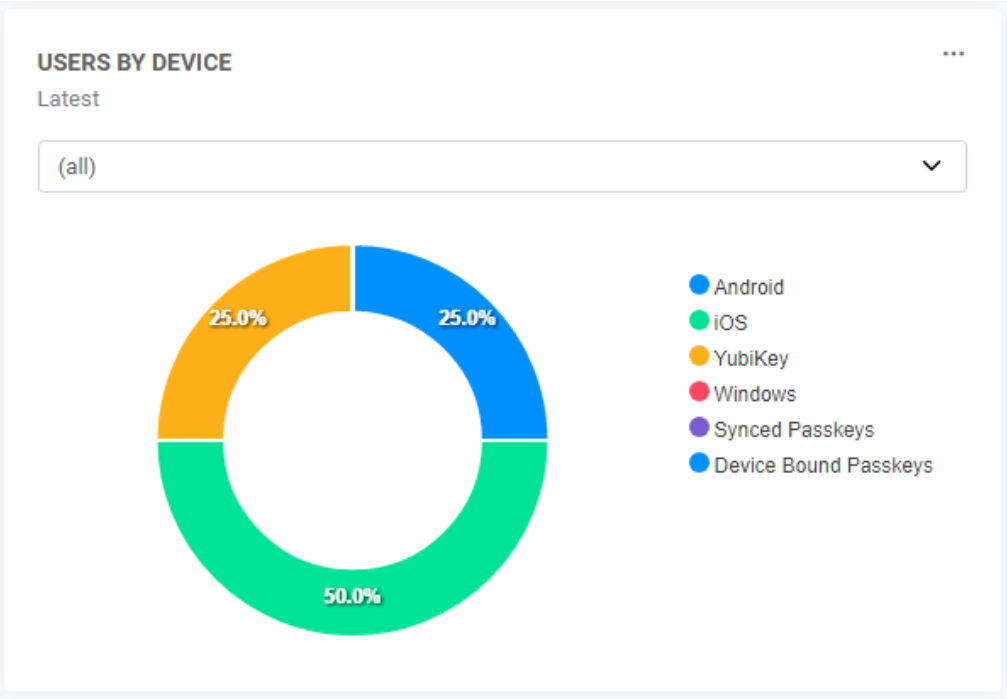


- **Authentication Request By Type** – breaks down successful authentication requests by MyID MFA authentication type.

- **Users By Authentication Type** – displays the total number of users who are provisioned to each MyID MFA authentication type.



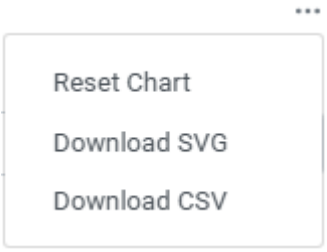
- **Users By Device** – displays the percentages of device types that are provisioned to users.



Multi-Factor Authentication dashboards reflect the information across the Active Directory forest or for each domain over the selected period.

To download a dashboard report:

1. In the top right hand corner of the dashboard report, click the options ... button.



2. Select the format that you want to download the dashboard report as.

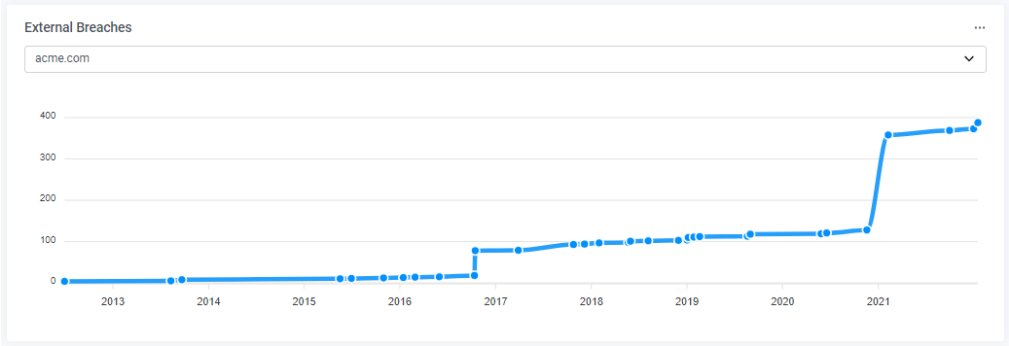
   This is either **Download SVG** or **Download CSV**.

3. The dashboard report is downloaded through your browser.

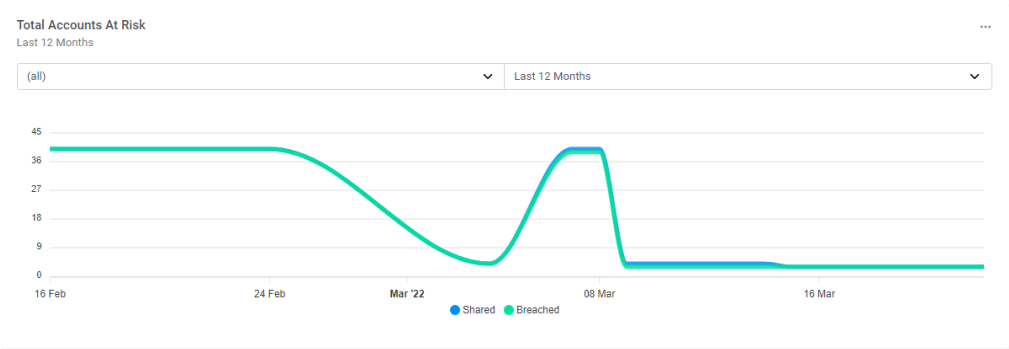
3.3 Password Security

The Password Security dashboard shows a near-live view of:

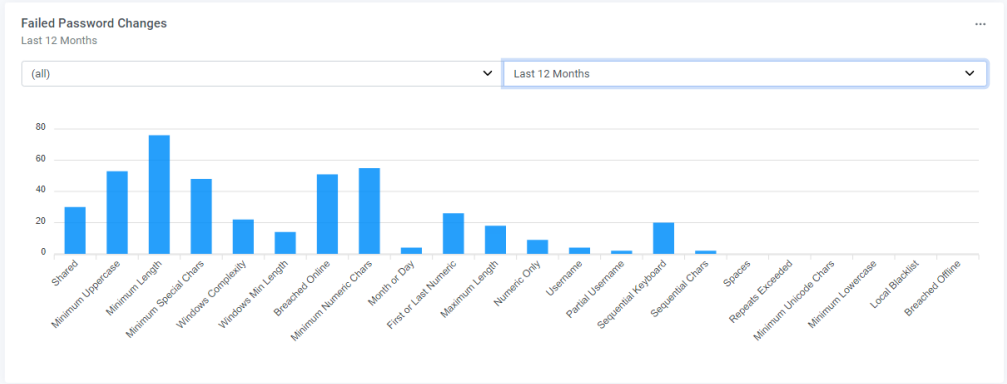
- **External Breaches** – shows the password breaches for the organization according to the MyID Password Breach database.



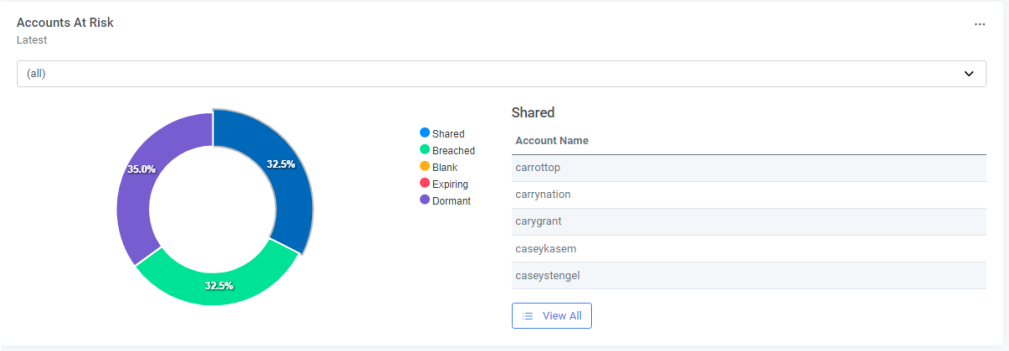
- **Total Accounts at Risk** – shows the number of accounts using breached or shared passwords as detected over the specified period.



- **Failed Password Changes** – shows the failed password changes and the reason for the password rejection over the selected time period.

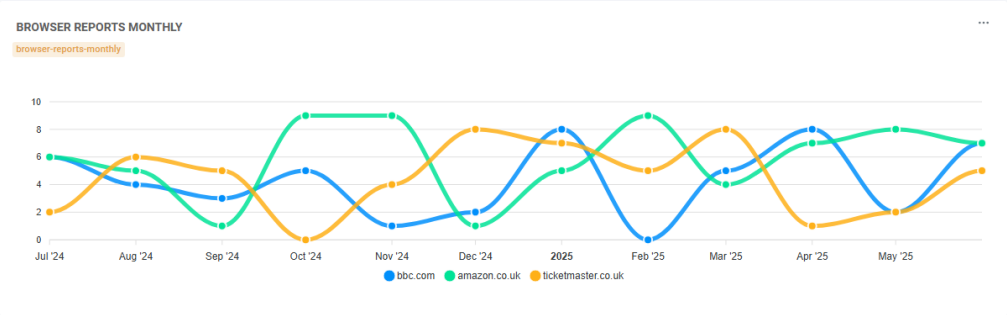


- **Users Accounts at Risk** – shows all the accounts with passwords that are shared, breached, blank, or soon to expire. This dashboard also shows dormant accounts.



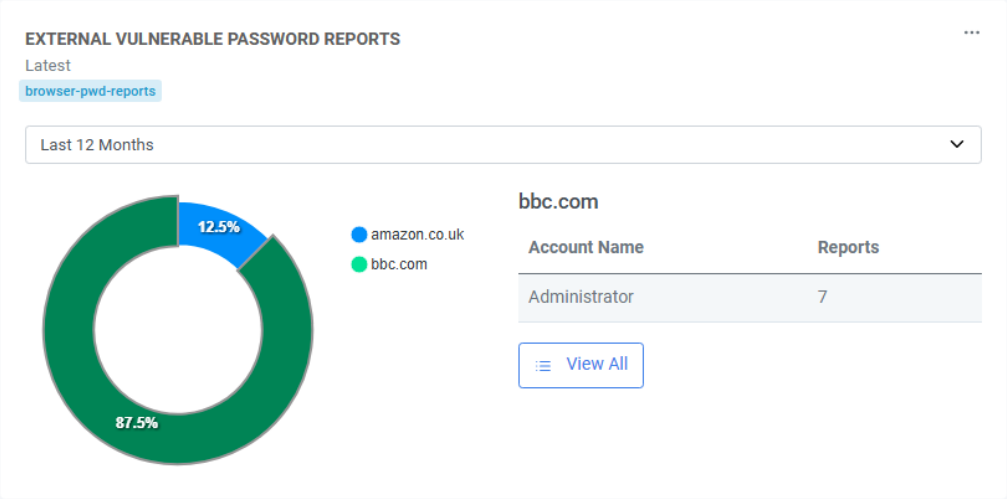
If you click **View All**, all the accounts that fall under the highlighted category are displayed.

- **Browser Reports Monthly** – shows where your users are using breached passwords over time.



Note: Only the domains specified in the **Domain Whitelist** on the Browser Password Domain Monitoring screen of the Password Security Management Wizard are displayed. For more information, see the *Starting the Password Security Management Wizard* section of the ***MyID Authentication Server Installation and Configuration Guide***.

- **External Vulnerable Password Reports** – shows which users are repeatedly attempting to use breached passwords on which websites.

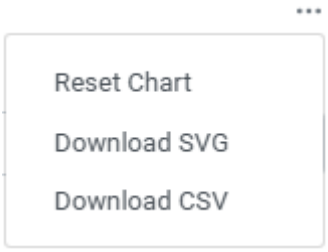


Note: Only the domains specified in the **Domain Whitelist** on the Browser Password Domain Monitoring screen of the Password Security Management Wizard are displayed. For more information, see the *Starting the Password Security Management Wizard* section of the ***MyID Authentication Server Installation and Configuration Guide***.

Password Security dashboards reflect the information across the Active Directory forest or for each domain over the selected period.

To download a dashboard report:

1. In the top right hand corner of the dashboard report, click the options ... button.



2. Select the format that you want to download the dashboard report as.
   This is either **Download SVG** or **Download CSV**.
3. The dashboard report is downloaded through your browser.

4 Reports

You can view reports through the Web Management Portal.

The following reports are available:

- The Authentication servers report.

  See section *4.1*, *Authentication servers report*.
- The Domain Controllers report.

  See section *4.2*, *Domain Controllers report*.
- The Domains report.

  See section *4.3*, *Domains report*.
- The Licences report.

  See section *4.4*, *Licences report*.
- The Provisioned Devices Summary report.

  See section *4.5*, *Provisioned Devices Summary report*.
- The Provisioned Users Summary report.

  See section *4.6*, *Provisioned Users Summary report*.
- The Public Breach Data report.

  See section *4.7*, *Public Breach Data report*.
- The Users report.

  See section *4.8*, *Users report*.
- The Browser Password Reports report.

  See section *4.9*, *Browser Password Reports report*.

You can export reports. For information on exporting reports, see section *4.10*, *Exporting reports*.

4.1 Authentication servers report

The Authentication Servers report lists the following information about each MyID MFA and PSM authentication server in the system:

- `Name` – the name of the authentication server. You can sort the results by this field.
- `Version` – the version of MyID MFA and PSM installed on the authentication server.
- `Valid` – is the server available on the network and is it running a compatible version of the authentication server?
- `Is Primary` – whether this is the primary MyID MFA and PSM authentication server.
- `Rpc available` – whether the Remote Procedure Call service is available.

4.2 Domain Controllers report

The Domain Controllers report lists the following information about each Domain Controller in the system:

- `Name` – the name of the Domain Controller. You can sort the results by this field.
- `Rpc Available` – whether the Remote Procedure Call service is available.
- `Connected` – whether the Domain Controller is currently reachable from the authentication server through which you are viewing the report.
- `Agent Version` – the version of the MyID Domain Controller Agent installed on the Domain Controller.

4.3 Domains report

The domains report lists the following information about each domain in the system:

- `Name` – the name of the domain. You can sort the results by this field.

4.4 Licences report

The Licences report contains the following information on your current licenses.

- `Product` – the product that this license is for – MFA or PSM.
- `Percentage Used` – the percentage of the licenses used in this set.
- `Used` – the number of the licenses used in this set.
- `Quantity` – the total number of licenses in this set.
- `Used Grace Exceeded` – whether the number of licenses used is over the allowed grace limit.
- `Expiry Date` – the date that this set of licenses expires.

4.5 Provisioned Devices Summary report

The Provisioned Devices Summary report contains the number of provisioned devices of each of the following device types:

- `Android`
- `iOS`
- `YubiKey`
- `Windows Synced Passkeys`
- `Device Bound Passkeys`

You can generate this report for each domain on your system.

4.6 Provisioned Users Summary report

The Provisioned Users Summary report contains the number of users provisioned for each of the following authentication types:

- `Pattern-enabled` – the number of users with Grid Patterns enabled.
- `OTC-enabled` – the number of users with One Time Codes enabled.
- `Phrase-enabled` – the number of users with Phrases enabled.
- `Push-enabled` – the number of users with Mobile Push enabled.
- `Temporary Access-enabled` – the number of users with temporary access codes enabled.
- `Passkey-enabled` – the number of users with Passkeys enabled.
- `YubiKey OTP-enabled` – the number of users with YubiKey One Time Pins enabled.
- `Pattern-disabled` – the number of users with Grid Patterns disabled.
- `OTC-disabled` – the number of users with One Time Codes disabled.
- `Phrase-disabled` – the number of users with Phrase disabled.
- `Push-disabled` – the number of users with Mobile Push disabled.
- `Passkey-disabled` – the number of users with Passkeys disabled.
- `YubiKey OTP-disabled` – the number of users with YubiKey One Time Pins disabled.
- `Pattern-locked` – the number of users with Grid Patterns locked.
- `OTC-locked` – the number of users with One Time Codes locked.
- `Phrase-locked` – the number of users with Phrase locked.
- `Push-locked` – the number of users with Mobile Push locked.
- `Passkey-locked` – the number of users with Passkeys locked.
- `YubiKey OTP-locked` – the number of users with YubiKey One Time Pins locked.

You can generate this report for each domain on your system.

4.7 Public Breach Data report

The Public Breach Data report contains the following information on the breaches that contain breached data relating to the selected report:

- `Name` – the name of the website that was breached or the collection in which the breached data was found. You can sort the results by this field.
- `Description` – a description of the breached data.
- `Date` – the date that the data was breached.
- `Status` – how reliable the breached data is. This is one of the following:
  - `Verified` – the data shown to be accurate when verifying with real life users.
  - `Unverified` – we have no proof that the data is legitimate.
- `Type` – the type of data breach. This is one of the following:
  - `Breach` – a direct breach of a website
  - `Combo` – a collection of compiled breached and/or hash cracked data.
- `Total` – the total number of known credentials from your domain found in the breached data.
- `Additions` – the number of credentials in the breached data for which this is the oldest known breached location of the credential.

The domains that you generate this report on do not have to be local domains; this report uses the domains configured on the Public Email Domain Breach Monitoring page of the Password Security Management Wizard. For more information, see the *MyID Password Security Management Wizard* section in the ***MyID Authentication Server Installation and Configuration Guide***.

4.8 Users report

The Users report provides the following information for each user on the system:

- `Account Name` – the user's account name. You can sort the results by this field.
- `First Name` – the user's first name.
- `Last Name` – the user's last name.
- `Status` – if the user is provisioned for MyID MFA or MyID PSM.
- `Enabled` – if the user is enabled in the Active Directory.
- `Locked` – if the user's account is locked.
- `Password Not Required` – if the user does not require a password.
- `Password Never Expires` – if the user's password is set to never expire.
- `Password Last Set` – the date when the user's password was most recently set.
- `Last Logon` – the date when the user last logged on.
- `Mobile Private` – is the user's mobile phone number kept private? If it is kept private, it is encrypted in the Active Directory.
- `Valid From` – the date that the user account starts or started being valid.
- `Valid To` – the date that the user account stops being valid.
- `Randomise Ad Password` – is the user's Active Directory password randomized?
- `Pattern Enabled` – are Patterns enabled for this user?
- `Otc Enabled` – are One Time Codes enabled for this user?
- `Phrase Enabled` – are Phrases enabled for this user?
- `YubiKey Enabled` – is YubiKey enabled for this user?
- `EmergencyOverride Enabled` – are Temporary Access codes enabled?
- `Pattern MIP Must Change` – does the user need to change the Grid Pattern on their next log in?
- `Pattern MIP Never Expires` – is the Grid Pattern set to have no expiry date?
- `Pattern Enable 2FA` – does the user have Grid Patterns enabled for Multi-Factor Authentication?
- `Phrase Enable 2FA` – does the user have Phrases enabled for Multi-Factor Authentication?
- `Phrase Require 2FA` – is the user required to use a device when authenticating with Phrases?
- `Phrase Answers Must Change` – does the user need to change their Phrases on their next log in?

You can generate this report for each domain on your system.

Note: This is different from the **Users** search. You cannot click through to manage a user from this report.

4.9 Browser Password Reports report

The Browser Password Reports report provides the following information on each user account that has been reported as attempting to use a breached password in a browser:

- `Account` – The user's account name.
- For each website on which a breached password has been used, a column is included in the report containing the number of times the user has attempted to use a breached password on that website.
- `Total Reports` – The total number of times that the user has been reported as attempting to use a breached password on an external website.

You can search for a specific user on this report. You cannot click through to manage a user from this report.

4.10 Exporting reports

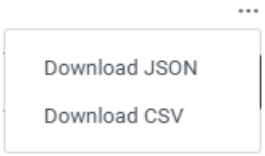
You can export all reports as either JSON or CSV files.

To export a report:

1. Run the report that you want to export.

   If the report can be run on multiple domains, ensure that it is being run on the desired domain.

2. In the top right hand corner of the report, click the options ... button.



3. Select the format that you want to download the report as.

   This is either **Download JSON** or **Download CSV**.

   The report is downloaded through your browser.

5 Managing a user

To locate a user to manage through the Web Management Portal:

1. In the System section of the Web Management Portal, click **Users**.
2. Select the domain in the forest that contains the user that you want to administer. If there is only a single domain then it is selected automatically.
3. Enter some or all of the user's first name, last name, or account name.
4. Press Enter.
5. Click on a user, then use the subsections under the **User** section to manage them.

   The options available for managing the user depend on the technologies for which the user is enabled.

This section contains information on:

- Updating a user's account details.

  See section *5.1*, *Updating a user's account details*.
- Assigning a temporary access code to a user

  See section *5.2*, *Assigning a temporary access code to a user*.
- Viewing user events.

  See section *5.3*, *Viewing all events for a user*.
- Viewing and disabling devices.

  See section *5.4*, *Viewing and disabling devices for a user account*.
- Managing a user's Grid Patterns.

  See section *5.5*, *Managing Grid Patterns*.
- Managing a user's Phrase authentication.

  See section *5.6*, *Managing Phrase authentication*.
- Managing a user's One Time Codes.

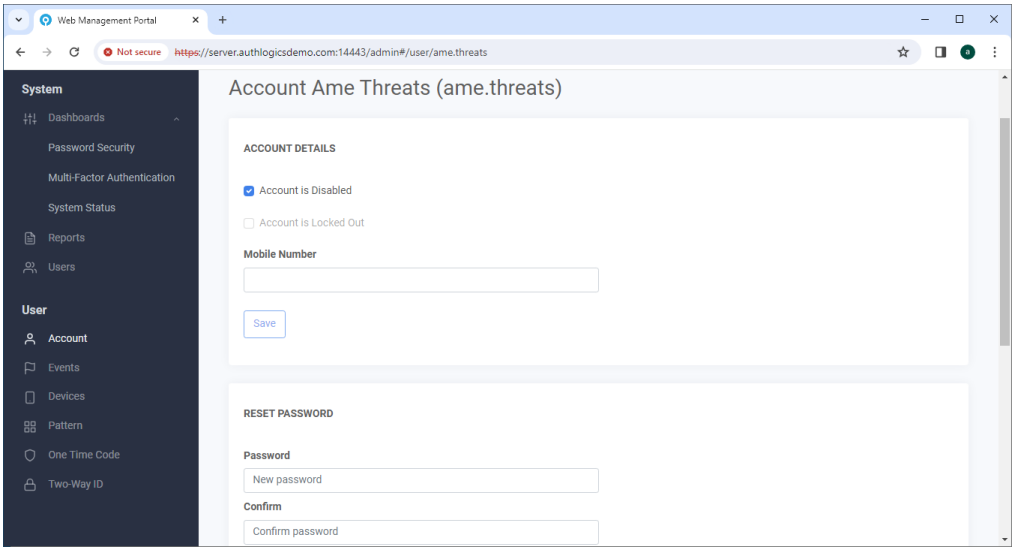
  See section *5.7*, *Managing One Time Codes*.
- Managing a user's devices.

  See section *5.8*, *Managing a user's devices*.
- Performing two-way identification.

  See section *5.9*, *Two-way identification*.

5.1 Updating a user's account details

To make changes to a user's basic account details, select the user account for which you want to edit the details. This brings you to the **Account** section for that user.



You can change the user's details, their password, and enable temporary access for the user from this page. For more information on assigning a temporary access code to a user, see section *5.2*, *Assigning a temporary access code to a user*.

A record of changes made to user accounts is kept in the MyID Server Application Event Log.

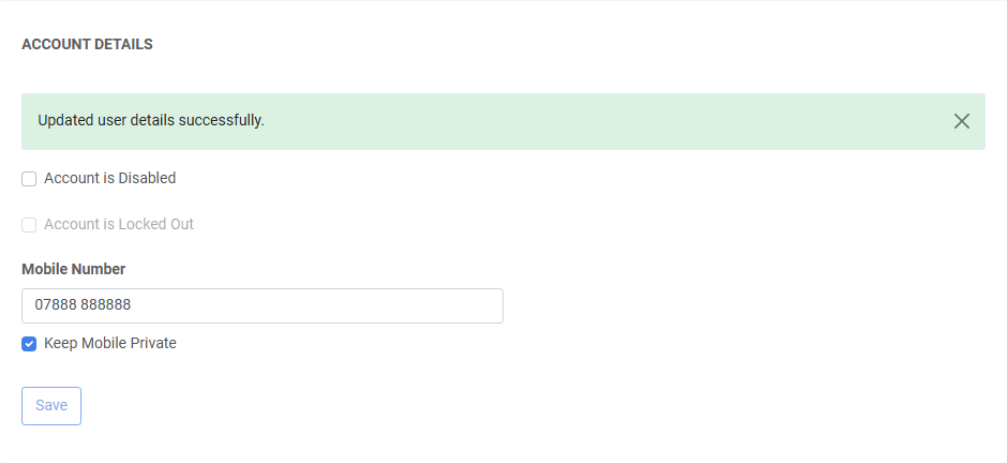
5.1.1 Updating a user's basic account details

To update the user's basic account details, in the Account Details section of the Account section for the user:

1. To disable a user's account, select **Account is Disabled**.
2. To lock a user's account, select **Account is locked out**.
3. To change the user's mobile phone number, enter a new **Mobile Number**.
4. If you have added a mobile phone number, you can select **Keep Mobile Private** to ensure that the mobile phone number is encrypted in the Active Directory.

   If you do not select this option, the mobile phone number is stored as clear text in the default mobile phone field in the Active Directory.
5. If you have made changes to a user's basic account details, click **Save**.

   A notification at the top of the section displays if the update is successfully saved.



5.1.2 Resetting a user's password

Note: If you cannot reset a user's password, your administrator may have disabled this functionality. For more information, see the *Disabling password changing* section in the ***MyID Authentication Server Installation and Configuration Guide***.

To set a new password for the user:

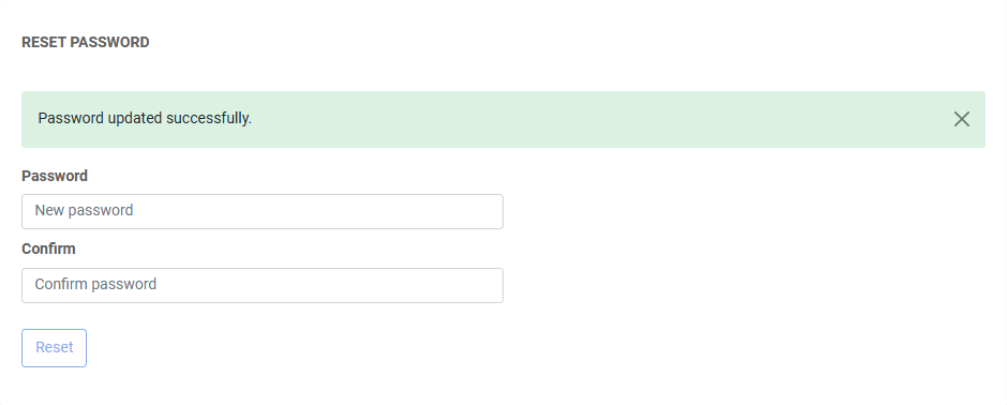
1. In the Reset Password section of the Account section for the user, type the new **Password**.

   A pop-up balloon may appear that helps guide you through choosing a new password for the user that meets your company policy and is secure.

2. Repeat the password to **Confirm** it.

3. Click **Reset**.

   If the password was successfully updated, a notification tells you that. If the password reset was not successful, the notification tells you why.



5.2 Assigning a temporary access code to a user

Note: To use this feature, you must ensure that **Allow Temporary Access Codes** is enabled on the global settings General tab of the MMC. For more information, see the *General tab* section of the ***MyID Authentication Server Installation and Configuration Guide***.

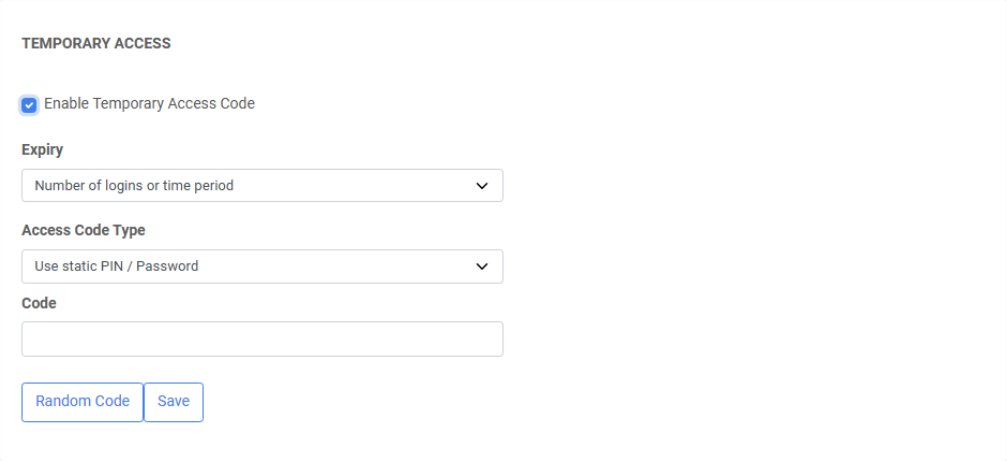
To enable temporary access for the user:

1. Select the user account to which you want to assign a temporary access code.

   This brings you to the **Account** section for that user.

   If you are already editing the user to whom you want to assign a temporary access code, in the User section, click **Account**.

2. In the Temporary Access section of the Account section for the user, select **Enable Temporary Access Code**.



3. Select the **Expiry** type.

   This is what causes the temporary access code to expire – whether the temporary access code is disabled after the preset **Number of logins**, **Time period**, or whichever runs out first – the **Number of logins or time period**.

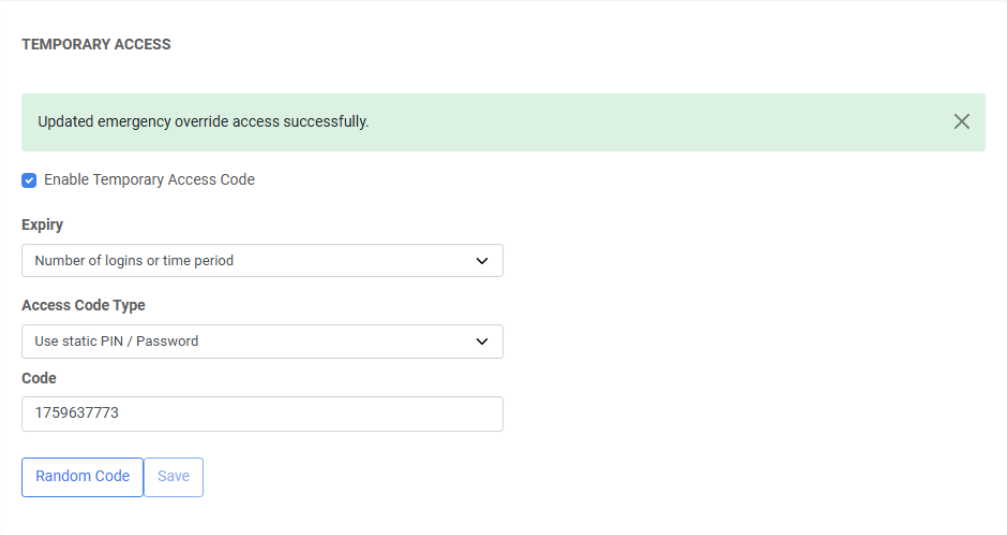
4. Select the **Access Code Type**:

   - **Use Active Directory password** – the temporary access code is the user's Active Directory password.
   - **Use static PIN / Password** – the temporary access code is code set by you.

     You can either:

     - Type a code in the **Code** field.
     - Click **Random Code**. A randomly generated temporary access code is now displayed in the **Code** field.

5. Click **Save**.



5.2.1 Known issues

- **IKB-441 – Unable to carry out an offline logon after using a temporary access code**

  When the **Manage the Windows password** option is enabled on the **FIDO2** tab of the global settings, if you use a temporary access code before going offline, all cached credentials are cleared, preventing you from carrying out an offline logon with either biometric or non-biometric FIDO devices, even if you have successfully logged in with FIDO devices before.

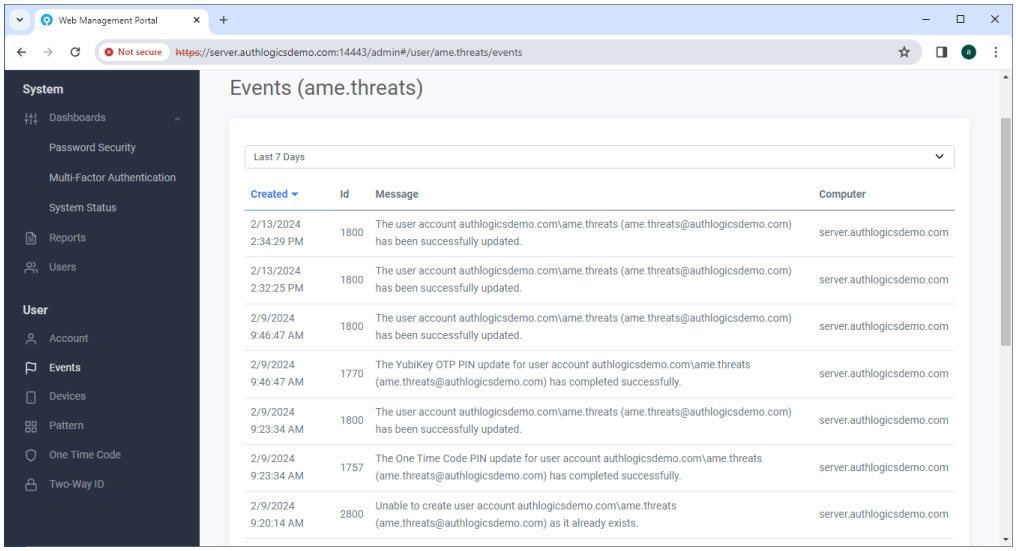
5.3 Viewing all events for a user

Every user-related event is registered in the Windows Events log on the MyID Authentication Server or Domain Controller that processed the request. In environments containing multiple MyID Authentication Servers and Domain Controllers, it can be challenging to locate the server containing the required log data.

The Web Management Portal Events view consolidates events from all servers into a single view for each user.

To view a user's events:

1. Select the user account for which you want to access events.
2. In the User section, click **Events**.



The following information is displayed for each event:

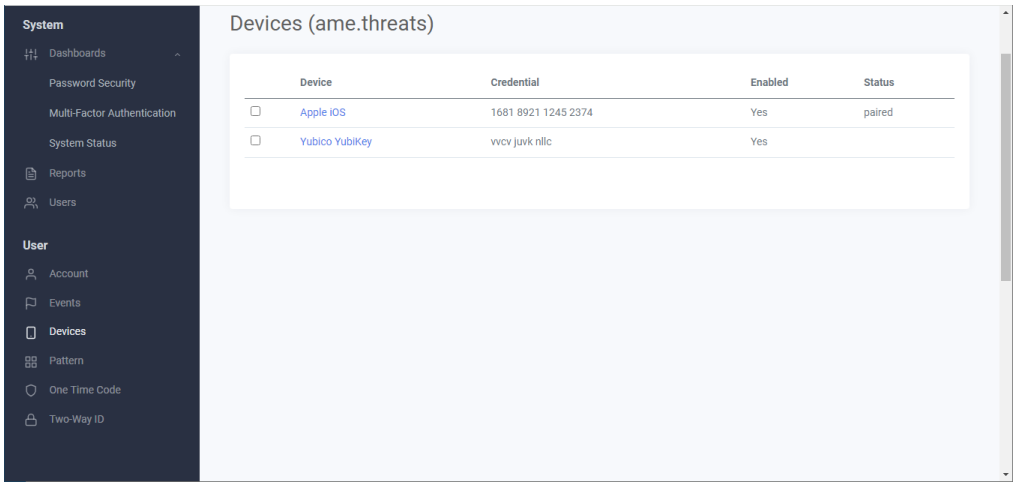
- `Created` – the time and date of the event.
- `Id` – the ID of the event type.
- `Message` – a description of the event.
- `Computer` – the server that the user was connected to or authenticated against during the event.

5.4 Viewing and disabling devices for a user account

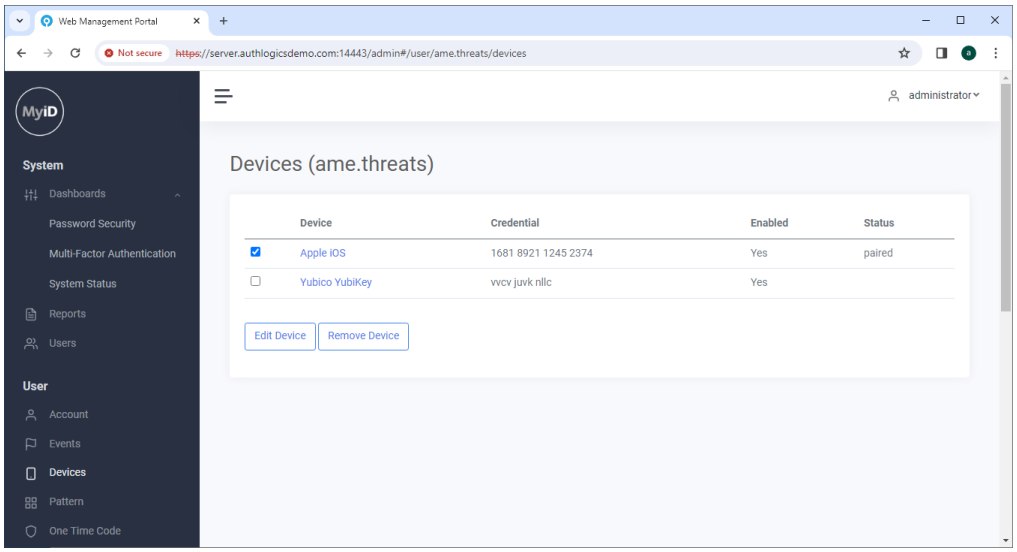
A user account can be linked to up to ten devices running a soft token app. These can be assigned through the Web Management Portal, the MyID Management Console, or the User Self Service Portal.

To view or disable a device:

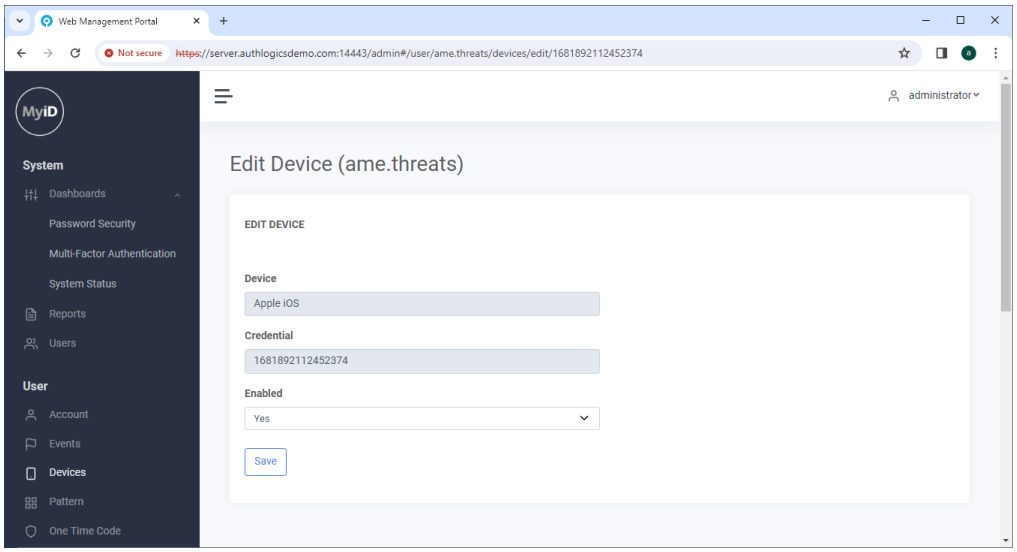
1. Select the user account that owns the device.
2. In the User section, click **Devices**.



3. Select the device to modify.

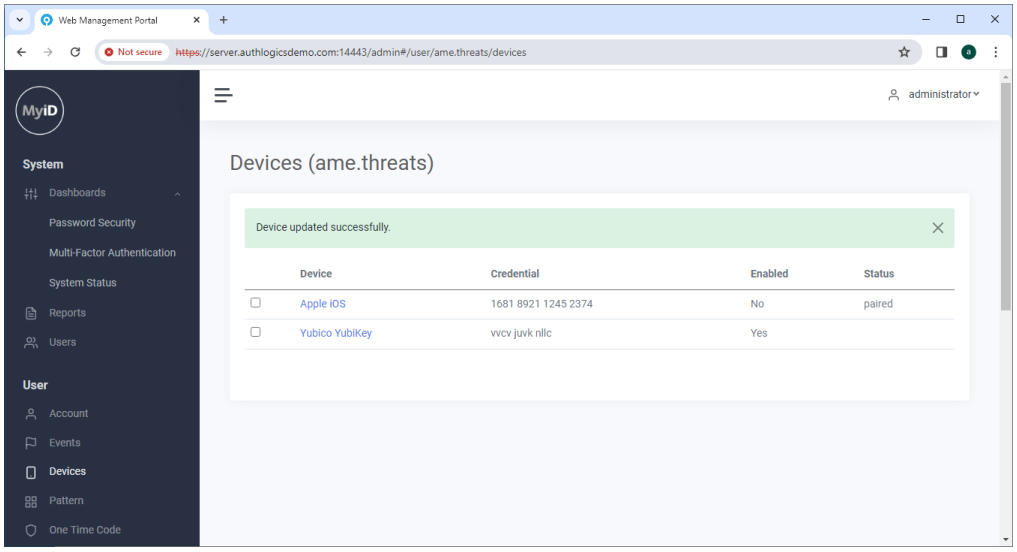


4. Click **Edit Device**.



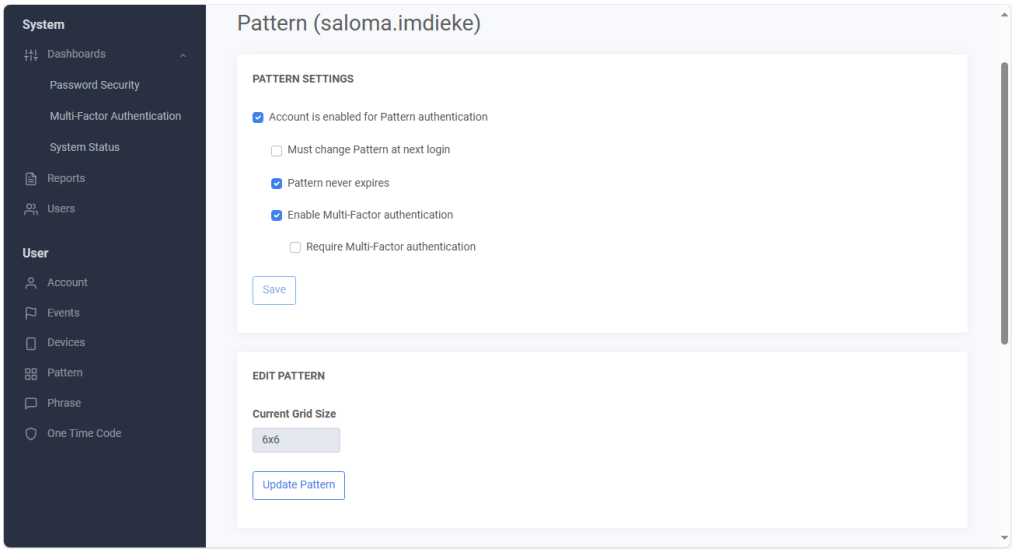
You are now viewing the details of the device.

5. To change the enabled status of the device:
   - To disable the device, set **Enabled** to `No`.
   - To enable the device, set **Enabled** to `Yes`.
6. To confirm the enabled status of the device, click **Save**.



The enabled status of the device is now changed.

5.5 Managing Grid Patterns



5.5.1 Managing the Grid Pattern settings

To manage a user's Grid Pattern Settings:

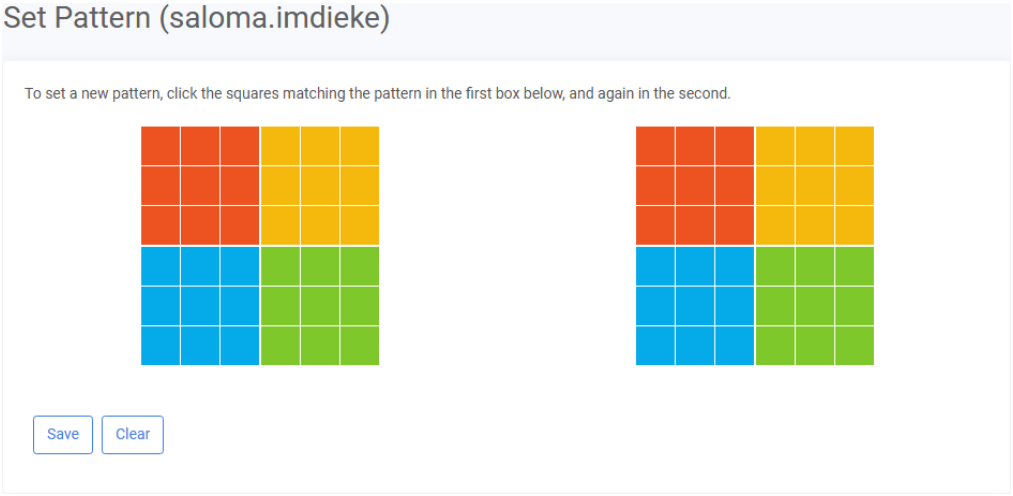
1. Select the user account of the user that you want to manage.
2. In the User section, click **Pattern**.
3. To enable the user account for Grid Patterns, ensure that **Account is enabled for Pattern authentication** is selected.
4. Select if the user **Must change Pattern at next logon**.
5. Select if the **Pattern never expires**.
6. If you want the user to be enabled to use Grid Patterns for multi-factor authentication, select **Enable Multi-Factor authentication**.
7. If you have enabled the user to use Grid Patterns for multi-factor authentication, you can force them to use Grid Patterns for multi-factor authentication only by selecting **Require Multi-Factor authentication**.
8. Click **Save**.

Note: You cannot set the size of the user's Pattern Grid from the Web Management Portal. To change the size of a user's Grid Pattern, run the Grid Management wizard against the user. For more information, see the *Setting up a user for Grid Pattern Authentication* section of the ***MyID Authentication Server Installation and Configuration Guide***.

5.5.2 Changing the pattern

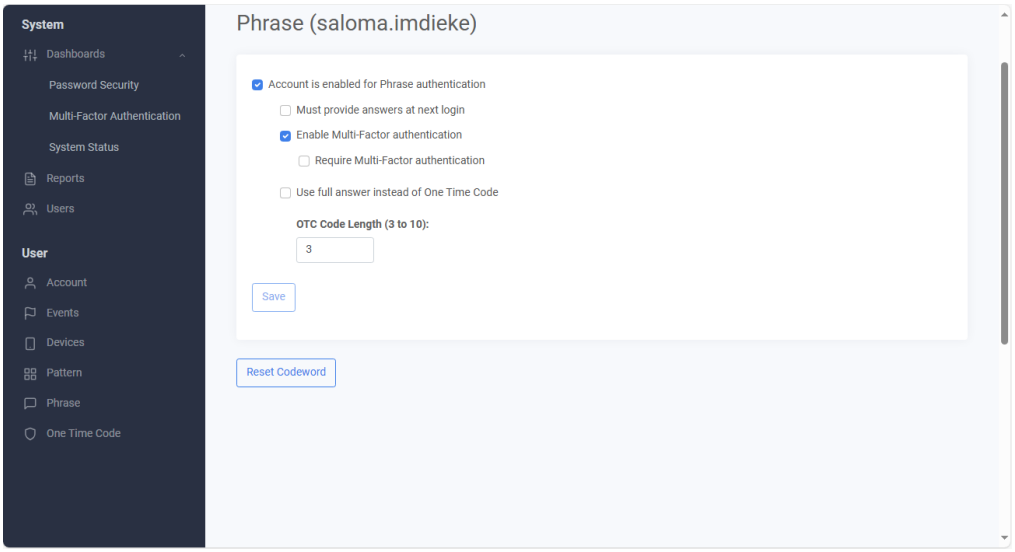
To update the user's Grid Pattern:

1. Click **Update Pattern**.



2. Click the required number of squares in a pattern on the left-hand Grid.
3. Repeat the pattern on the right-hand Grid.
4. Click **Save**.

5.6 Managing Phrase authentication



5.6.1 Managing a user's Phrase authentication

To manage a user's Phrase authentication:

1. Select the user account of the user that you want to manage.
2. In the User section, click **Phrase**.
3. To enable the account for Phrases, select **Account is enabled for Phrase authentication**.
4. To force the user to change their Phrase answers at next logon, click **Must provide answers at next login**.
5. If you want the user to be enabled to use Phrases for multi-factor authentication, select **Enable Multi-Factor authentication**.
6. If you have enabled the user to use Phrases for multi-factor authentication, you can force them to use Phrase for multi-factor authentication only by selecting **Require Multi-Factor authentication**.
7. If you want the user to use their full Phrase answers when authenticating with Phrases, select **Use full answer instead of One Time Code**.
8. If the user is not using their full Phrase, you can select how many characters the user must use from the user's Phrase. You can set this to a number from `1` to `10`.

   For example, if you select `3`, on attempted log in, the user might be asked to:

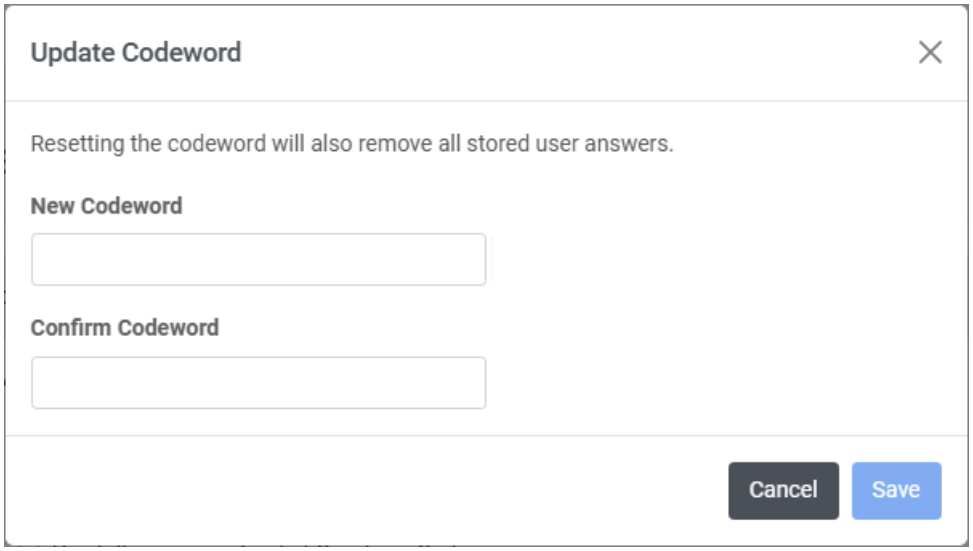
   `Enter the 1st, 2nd and last characters from your Codeword.`

   Where the Phrase question is `What is... your Codeword`.

5.6.2 Resetting a user's Codeword

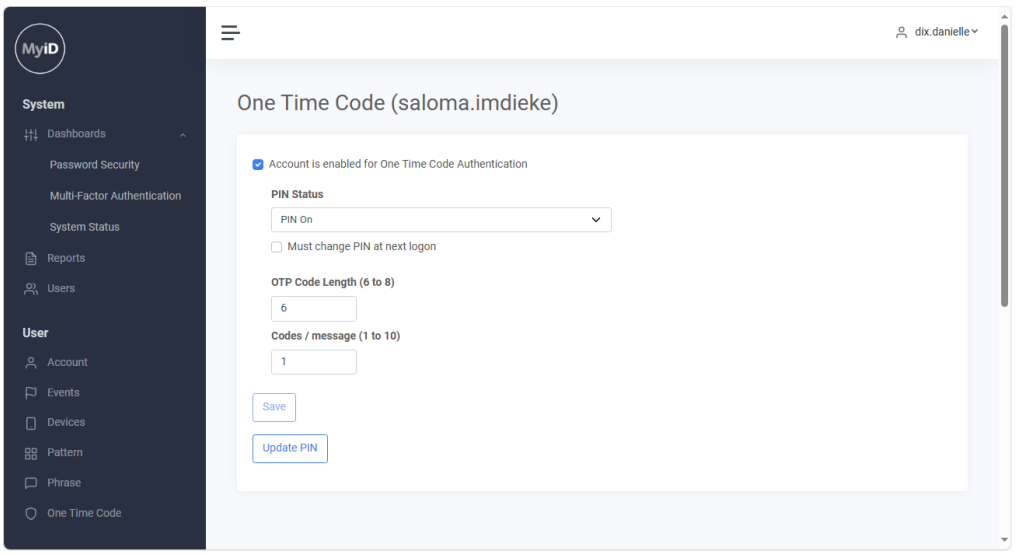
The default Phrase question is `What is... your Codeword`. If you have not added more Phrases, you can reset this Codeword with the Web Management Portal. To change a user's Codeword:

1. Click **Reset Phrase**.



2. Type a **New Codeword**.
3. Confirm the codeword.
4. Click **Save**.

5.7 Managing One Time Codes



5.7.1 Managing a user's One Time Code

To manage a user's One Time Code (OTC):

1. Select the user account of the user that you want to manage.
2. In the User section, click **One Time Code**.
3. To enable the account for One Time Codes, select **Account is enabled for One Time codes**. Otherwise, deselect it.
4. Select a **PIN Status**.

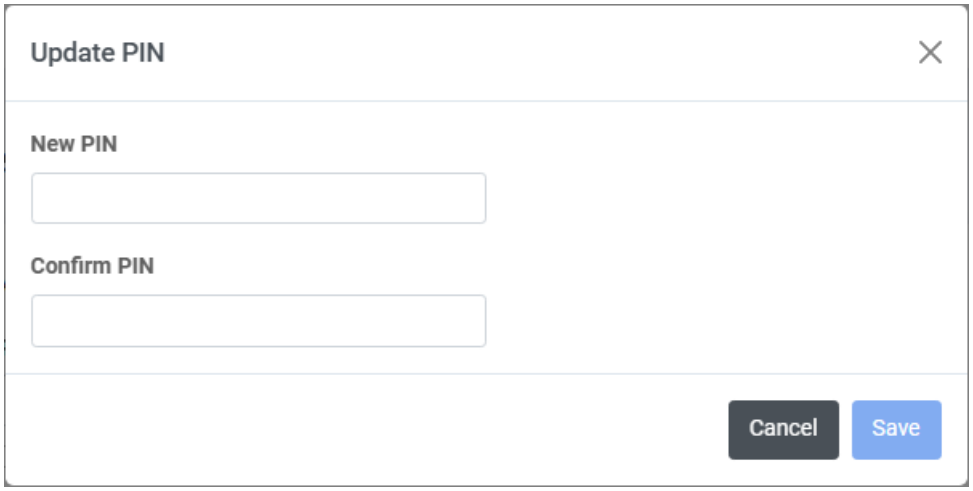
   This can be one of the following:

   - `PIN On` – the user must additionally use their set MyID MFA OTC PIN to authenticate when using One Time Codes.
   - `PIN Off` – the user is only required to use their One Time Code when authenticating with One Time Codes. Setting this option removes your ability to do further OTC management.
   - `Use AD password as PIN` – the user must additionally use their set Active Directory password to authenticate when using One Time Codes.
5. Select if the user **Must change PIN at next logon**.
6. Set the **OPT Code Length**. This is the length of the code sent to the user. This can be set to a number from `6` to `8`.
7. Set the **Codes / Messages** to the number of codes to be sent to the user at a time. This can be set to a number from `1` to `10`.
8. Click **Save**.

5.7.2 Changing a user's PIN

To change the user's PIN:

1. Click **Update PIN**.



2. Type a **New PIN**.
3. Confirm the PIN.
4. Click **Save**.

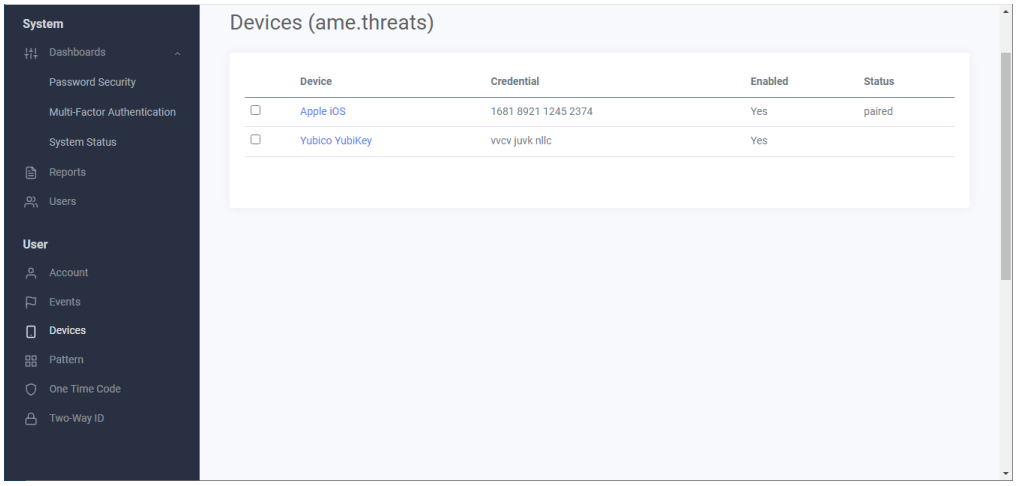
5.8 Managing a user's devices

You can use the Web Management Portal to remove devices from a user's account, change the name of a user's device, or enable and disable a user's device.

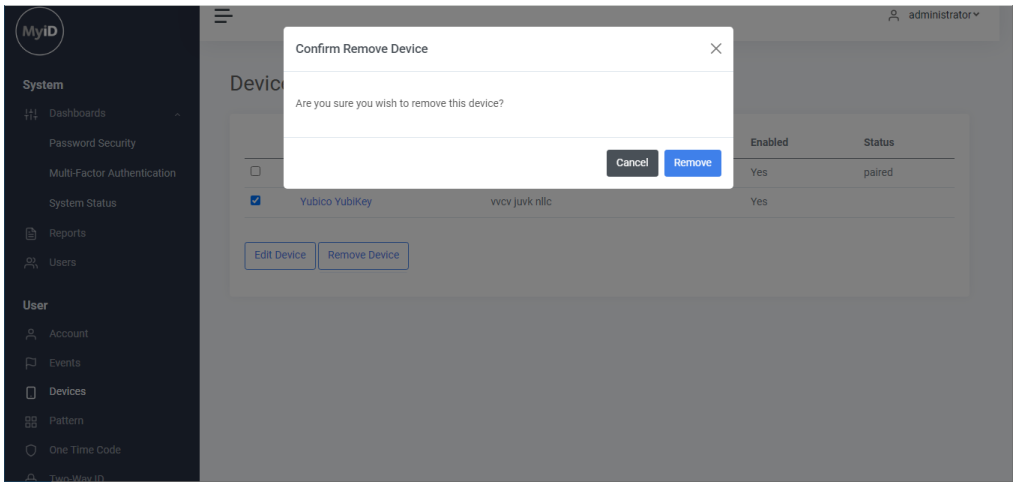
5.8.1 Removing a device from a user account

To remove a device:

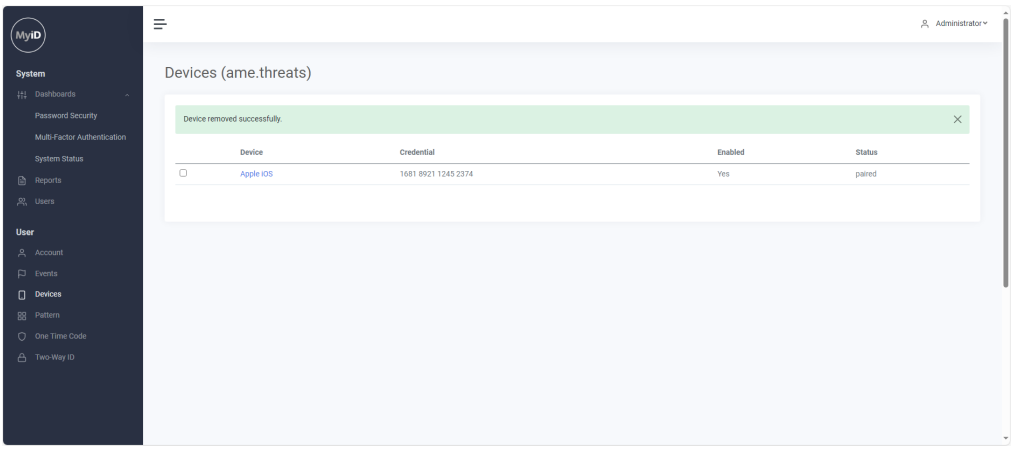
1. Select the user account from which you want to remove the device.
2. In the User section, click **Devices**.



3. Select the device that you want to remove.
4. Click **Remove Device**.



5. Click **Remove** to confirm that you want to remove the device.

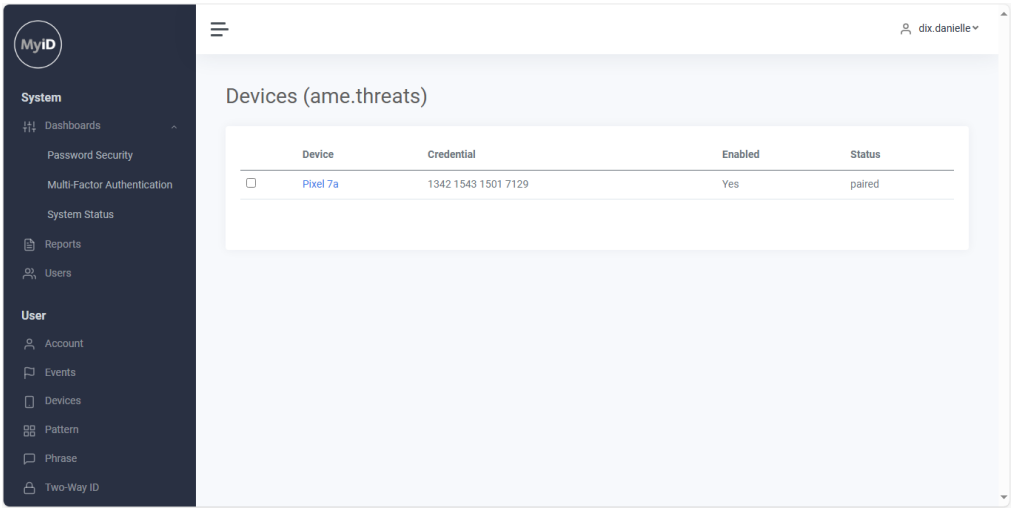


The device is now removed.

5.8.2 Changing device names

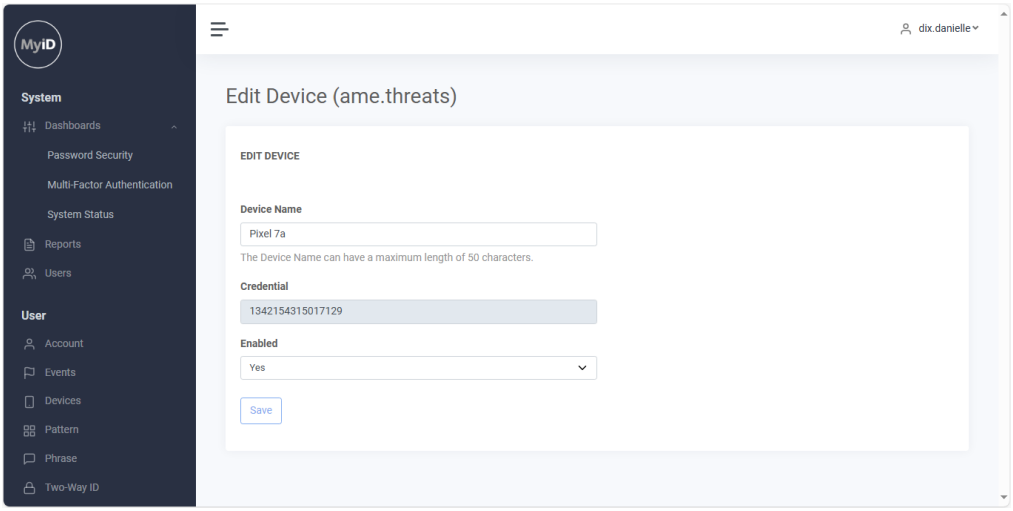
To change the name of a device:

1. Select the user account with the device that you want to rename.
2. In the User section, click **Devices**.

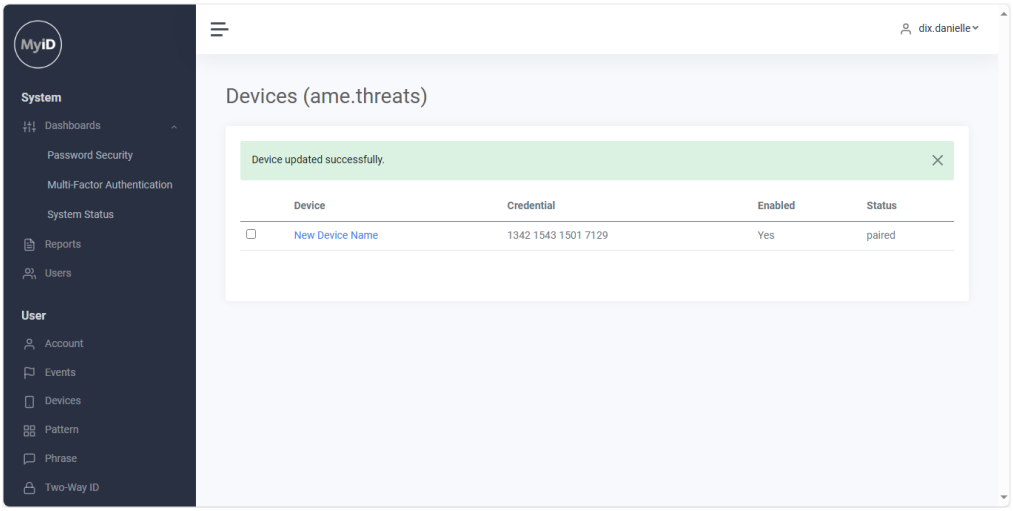


3. Click the name of the device for which you want to change the name.

   Alternatively, select the device and click **Edit Device**.



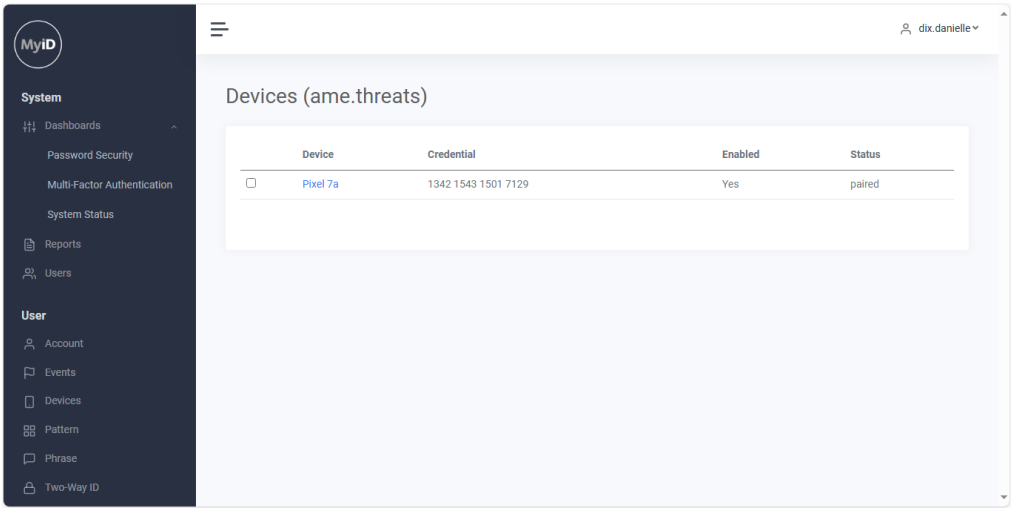
4. Type the new **Device Name**.
5. Click **Save**.



5.8.3 Enabling and disabling devices

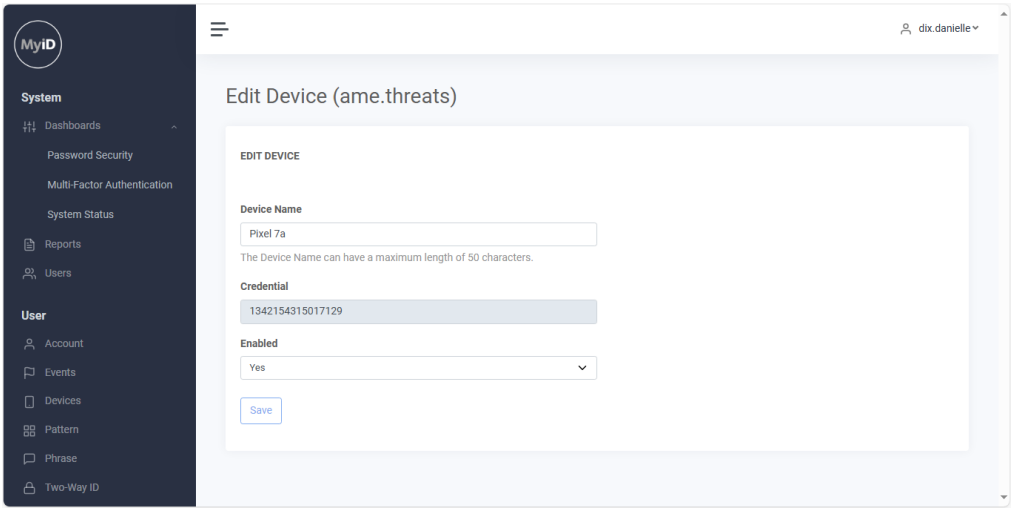
To enable or disable a user's device:

1. Select the user account with the device that you want to enable or disable.
2. In the User section, click **Devices**.



3. Click the name of the device that you want to enable or disable.

   Alternatively, select the device and click **Edit Device**.



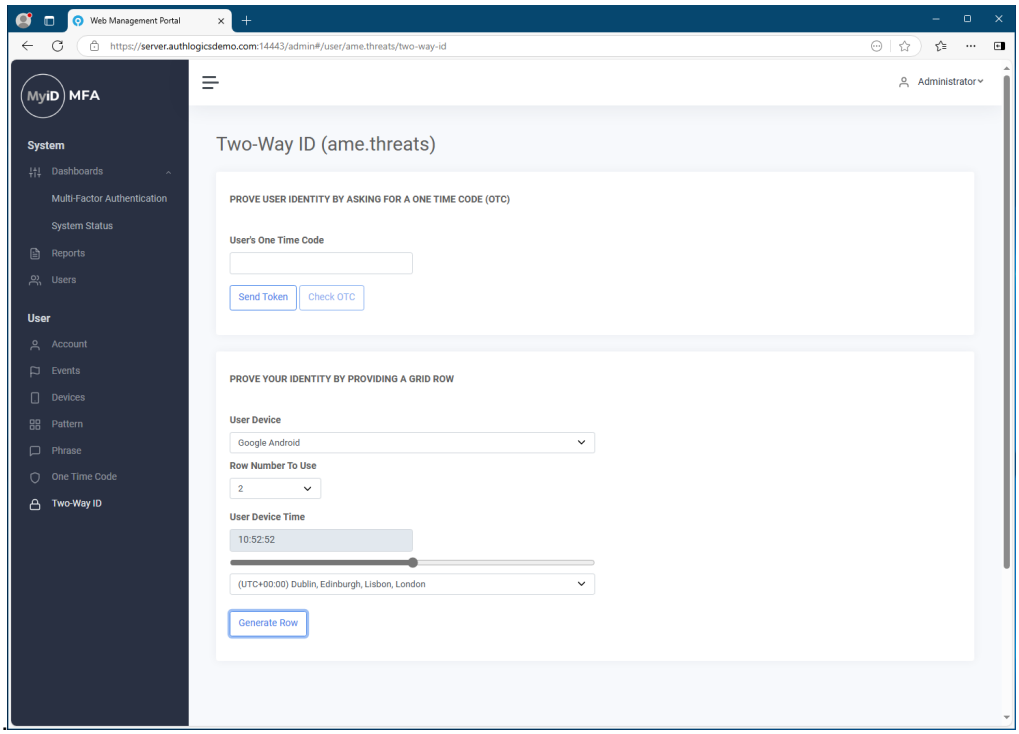
4. Set the **Enabled** option to `Yes` to enable the user's device. Set the **Enabled** option to `No` to disable the device.
5. Click **Save**.

5.9 Two-way identification

Note: The visible options for a user depend on what is enabled for the user. If you do not have Grid patterns or One Time Codes enabled, this page is not visible.

To carry out two-way identification, you ask the user to prove their identity to you, and then prove your identity to the user:

1. Select the user account for which you want to carry out two-way identification.
2. In the User section, click **Two-Way ID**



3. In the **Prove user identity by asking for a One Time Code (OTC)** section, if you want to send an OTC through an SMS or e-mail, click **Send Token**.

   To configure sending a token through SMS or email, set the **Delivery Method** on the Multi-Factor Token Delivery Settings page of the Grid User Management Wizard to `SMS / Text` or `Email`. For more information, see *Setting up a user for Grid Pattern Authentication* in the ***MyID Authentication Server Installation and Configuration Guide***.

   If the user has a device with One Time Codes or Grid patterns configured, they can use the OTC or Grid pattern from their device to verify themselves to you instead.
4. Type the user's token into the **User's One Time Code** text box.
5. Click **Check OTC**.
6. If the user's One Time Code was correct, a message appears that the user account was successfully validated.

   This verifies the user's identity to you.

7. In the **Prove your identity by providing a Grid row** section, select a **User Device**.
8. Select a row of the Grid pattern from the drop-down list.
9. Click **Generate Row**.

   The selected row of the user's current Grid pattern is displayed.
10. Tell the user the generated row. This verifies yourself to the user.