MyID MFA and PSM

Version 5.3.2

SIEM Integration 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: IMP2052-5.3.2

November 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

This document describes the Events codes generated by MyID Multi-factor Authentication (MFA) and Password Security Manager (PSM) solutions for analysis and integration within SIEM solutions. MyID Event codes are written to the MyID Authentication Server and Domain Controller Windows Application Event logs.

Note: MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly. The term 'Authlogics' may still appear in certain areas of the product.

MyID Event codes are broken down into the following categories:

- **Information**
- **Warning**
- **Error**

2 Multi-factor Authentication Event Codes

The following sections contain information on Multi-Factor Authentication event codes, sorted by why the event codes are generated:

- Valid and invalid logins.

  See section *2.1*, *Logins*.
- User actions and provisioning.

  See section *2.2*, *User actions and provisioning codes*.
- Errors due to issues with creating, updating, or deleting a user.

  See section *2.3*, *Failed user actions*.
- Warnings due to failures occurring.

  See section *2.4*, *Failed warnings*.

2.1 Logins

2.1.1 Valid logins

Event type: **Information**

The following codes are used if you have successfully authenticated.

Code	Descriptions
1494	Push via RADIUS
1496	Push via RADIUS and AD password
1497	MFA via RADIUS
1498	AD credentials via RADIUS
1502	Grid deviceless token, user must change pattern at next login
1503	Grid deviceless token
1504	Grid 2 factor token user must change pattern at next login
1505	Grid 2 factor token
1507	Phrase deviceless token, user must change answer at next logon
1508	Phrase deviceless token
1509	Phrase 2 Factor token
1510	One Time Code 2 Factor token , user must change PIN at next logon
1511	One Time Code 2 factor token
1512	Grid 2 factor token, user must change pattern at next login
1513	Grid 2 factor token
1523	Grid 2 factor token user must change pattern at next login
1524	Grid 2 factor token
1525	One Time Code 2 factor token
1526	Phrase 2 Factor token, user must change answers at next login
1527	Phrase 2 Factor token

Code	Descriptions
1528	Emergency Access code
1529	Emergency Access code via RADIUS
1530	Grid deviceless via RADIUS user must change pattern at next login
1531	Grid deviceless via RADIUS
1532	Grid 2 Factor via RADIUS user must change pattern at next login
1533	Grid 2 Factor via RADIUS
1534	Grid 2 Factor via RADIUS user must change pattern at next login
1535	Grid 2 Factor
1536	One Time Code 2 Factor token via RADIUS
1537	One Time Code 2 Factor token via RADIUS
1538	Phrase deviceless token via RADIUS
1539	Phrase deviceless token
1540	Phrase 2 Factor token via RADIUS
1541	Phrase 2 Factor token
1542	Phrase 2 Factor token via RADIUS, user must change answers
1543	Phrase 2 Factor token via RADIUS
1548	One Time Code soft-token, user must change PIN at next login
1607	YubiKey 2 Factor token
1608	YubiKey 2 Factor token via RADIUS
1765	Emergency override code using AD password
1766	Emergency override code using a static code
1780	User biometrically authenticated using Push
1781	User biometrically authenticated using Push via RADIUS
1782	User authenticated using Push
1783	User successfully authenticated using Push via RADIUS
1784	A Push notification was accepted
1785	A Push notification was rejected by the user
1893	OATH 2 Factor
1892	OATH via RADIUS
2052	FIDO token synced passkey (mobile)
2053	FIDO device-bound passkey
2054	Windows Password
2055	External Identity authenticated
2056	Windows Password
2057	Certificate Authentication
5020	Successfully authenticated using FIDO credentials

2.1.2 Invalid Logins

Event type: **Warning**

Code	Descriptions
1785	Push notification was rejected by the user
2495	Failed to authenticate user via RADIUS. Invalid AD password
2500	Account lockout settings prevented login
2501	Invalid passcode was provided
2505	Failed to authenticate Phrase user
2506	Failed to authenticate One Time Code user
2507	Failed to authenticate Grid user
2514	Invalid user account
2515	Invalid YubiKey token provided
2516	Invalid YubiKey token provided via RADIUS
2519	Invalid Grid transaction token entered
2520	Account lockout settings prevented login via RADIUS
2521	Failed to authenticate Grid user via RADIUS
2522	Failed to authenticate One Time Code user via RADIUS
2523	Failed to authenticate Phrase user via RADIUS
2524	Failed to authenticate Phrase user via RADIUS as user is not a member of the RADIUS user's role.
2545	Failed to authenticate the user. MFA account is locked.
2549	Failed to authenticate user via RADIUS from IP address. Invalid AD password.
2650	OTP failed is Web Operator Portal
2720	Invalid OTP
2760	Account locked out
2761	Failed login attempt #
2762	Failed to authenticate. Account is locked out.
2768	Invalid Emergency Override Code. Code has expired
2788	A push notification was Rejected as Not Requested by user
2950	Failed to authenticate Push user
2951	Failed PUSH via RADIUS
2952	Failed Grid no biometrics supplied
2953	Failed Grid transaction no biometrics supplied
2954	Failed One Time Code no biometrics supplied
2955	Failed One Time Code transaction no biometrics supplied
2956	Failed Phrase no biometrics supplied
2957	Failed OATH via RADIUS

Code	Descriptions
2958	Failed OATH authentication
3752	Invalid Emergency Override Code. Invalid Active Directory Password
3753	Invalid Emergency Override Code. Invalid Code

2.2 User actions and provisioning codes

This section deals with the event codes generated related to user actions and provisioning.

2.2.1 Successful actions

Event type: **Information**

Code	Descriptions
1514	Successfully delivered token via email
1515	Successfully delivered token via email
1516	Successfully delivered token via SMS
1517	Successfully delivered token via SMS
1518	Successfully delivered token via email
1519	Successfully delivered token via SMS
1520	Successfully delivered SMS
1521	Successfully delivered token via email
1522	Successfully delivered token via SMS
1630	Successfully added a Yubikey hardware token
1631	Successfully removed a Yubikey hardware token
1632	Successfully enabled a Yubikey hardware token
1633	Successfully disabled a Yubikey hardware token
1652	Users AD Password changed
1655	Updated the Single Sign-On Active Directory password for account
1656	Updated the Active Directory password for account
1668	Successfully reset AD password
1669	Secure vault stored password updated
1671	New hardware token successfully added
1672	Hardware token successfully removed
1673	Hardware token successfully change status
1674	User successfully provisioned for Grid
1675	User successfully provisioned for Phrase
1676	User successfully provisioned for One Time Code
1677	Successfully generated new Grid pattern
1678	Successfully sent security token
1682	Successfully generated new Phrase code word
1683	Successfully generated new One Time Code code

Code	Descriptions
1684	Successfully enabled account for Grid
1685	Successfully enabled account for Phrase
1686	Successfully enabled account for One Time Code
1687	Successfully disabled account for Grid
1688	Successfully disabled account for Phrase
1689	Successfully disabled account for One Time Code
1698	Successfully changed Grid pattern
1701	Emergency Override Access enabled for user
1702	Emergency Override Access disabled for user
1712	SSO password for user account removed
1714	SSO password for user account set
1723	Online Vault Password successfully updated for account
1724	Successfully authenticated via a password reset code
1780	User biometrically authenticated using Push
1781	User biometrically authenticated using Push over RADIUS
1782	User authenticated using Push
1783	User authenticated using Push over RADIUS
1784	Push notification was accepted
1785	Push notification was rejected
1800	The user account has been successfully updated
1801	The user account has been successfully deleted.
1803	The Active Directory password for the user account has been successfully reset
1804	The user account has been successfully unlocked.
1805	The user account has been successfully created.
2052	Successfully authenticated using synced passkey (mobile)
2053	Successfully authenticated using device-bound passkey
2054	Successfully authenticated using Windows password
2055	Successfully authenticated using external authentication provider
2056	Successfully authenticated using Windows password
2057	Successfully authenticated using certificate authentication
2788	Push notification was rejected by user as not requested by user
5010	YubiKey OTP for user successfully updated
5011	Credentials for user has been created via SSP
5012	Credentials for user has been created via SSP

2.3 Failed user actions

Event type: **Error**

Code	Descriptions
2800	Unable to create user account as it already exists
2807	Unable to create user account as the AD account does not exist
2815	Unable to reset the Active Directory password for user account
2816	Unable to unlock user account
2844	Unable to create user account as the Realms Container could not be found
2845	Unable to create user account as the specified Realm does not exist.
2846	Unable to create user account as either the Realm or Account Name were not specified.
3806	Unable to update account
3809	Unable to delete user account

2.4 Failed warnings

Event type: **Warning**

Code	Descriptions
2508	Failed to deliver email
2509	Failed to deliver SMS
2510	Failed to deliver email
2511	Failed to deliver SMS
2512	Failed to send MFA token via email
2513	Failed to send MFA token via SMS
2528	Failed to send email via Primary SMTP server
2529	Failed to send email via Secondary SMTP server
2533	SMS Password reset cannot be delivered
2760	Account has been locked out due to bad login attempts.
2774	Licence activation grace period has expired.
2777	Licence has expired
2778	Licence grace period has expired
6030	Failed minimum client version

2.4.1 Failed grid, one time code, or phrase change actions

Event type: **Warning**

Code	Descriptions
2750	Entered pattern failed complexity check: Block Sequential Straight Lines
2751	Entered pattern failed complexity check: Block Single Plane
2752	Entered pattern failed complexity check: Restrict Sequential Linear Adjacencies
2753	Entered pattern failed complexity check: Restrict Cell Repeat Usage
2754	Entered pattern failed complexity check: Pattern has been previously used
2755	The pattern has already been changed within the last # of days.
2756	The pattern generated on a grid smaller than the specified minimum grid size
2760	Account has been locked due to excessive # of bad logons
2765	The One Time Code PIN is smaller than the required PIN length
2766	The Phrase answer is smaller than the required answer length
2782	The entered pattern does not contain a sufficient number of selected cells
2789	Push could not be sent as the user is currently being throttled

3 Password Security Manager Event Codes

The following sections contain information on Password Security Manager event codes, sorted by why the event codes are generated:

- A successful password change.

  See section *3.1*, *Change success*.

- A failed password change.

  See section *3.2*, *Change failure*.

3.1 Change success

Event type: **Information**

Code	Descriptions
1400	The provided password complies with MyID PSM and has been accepted
1401	DisablePasswordPolicyAgent is enabled (On). The provided password complies with MyID PSM and has been accepted.
1418	Password is an MyID auto-generated password
1420	User is a member of AD security group. PSM checks will be performed on this password
1421	User is not a member of AD security group and exception checks are disabled.
1422	User is not a member of AD security group. Password passed exception policy password checks.
1423	OverridePasswordCheckforNewAccounts is enabled (On). Password has been accepted for use.
1424	The provided password for complies with MyID Password Security Management and has been accepted for use
1425	The provided password for complies with MyID Password Security Management and has been accepted for use by the MyID Authentication Server.

3.2 Change failure

Event type: **Warning**

Code	Descriptions
2400	Password does not comply with MyID Password Security Management policy
2404	Password provided is invalid. The Password is already in use by another user
2405	Password is empty and rejected as Fail-Safe is enabled
2406	Password is empty and accepted as Fail-Safe is disabled
2407	Password failed DisallowSpaces complexity check
2408	Password failed DisallowMonthandDay complexity check
2409	Password failed MaxSequentialKeyBoardChars complexity check
2410	Password failed MaximumAllowedPartialUsername complexity check
2411	Password failed AllowUsername complexity check
2412	Password failed MaxSequentialChars complexity check
2413	Password failed MaxRepeatingChars complexity check
2414	Password failed MinUnicodeChars complexity check
2415	Password failed MinSpecialChars complexity check
2416	Password failed MinNumericChars complexity check
2417	Password failed MinUpperCaseChars complexity check
2418	Password failed MinLowerCaseChars complexity check
2419	Password failed MaxLength complexity check
2420	Password failed MinLength complexity check
2421	Password failed Local Blacklist complexity check
2422	Password failed Cloud Blacklist complexity check
2425	Password failed MaxConsecutiveRepeatingChars complexity check
2433	Accountname is invalid
2434	Accountname is invalid. Password has been accepted as Fail-Safe is disabled
2443	Password failed Cloud Blacklist complexity check
2444	Password fails MimicWindowsComplexity check
2445	Password fails MimicMinLength complexity check
2446	Password fails Windows Exception complexity check
2447	Password fails Windows Exception MinLength complexity check
2454	Password has been rejected
2455	Password has been rejected

4 MyID Licence Event Codes

The following sections contain information on MyID Licence event codes event codes, sorted by why the event codes are generated:

- Successful license events.

  See section *4.1*, *Success events*.

- Failed license events.

  See section *4.2*, *Failed events*.

4.1 Success events

Event type: **Information**

Code	Descriptions
1404	Licence successfully installed
1405	Licence successfully activated
1406	Licence successfully updated

4.2 Failed events

Event type: **Warning**

Code	Descriptions
2423	No licence found
2424	Licence could not be activated because it has expired
2427	Licence is invalid
2428	Licence is invalid
2774	Licence activation grace period has expired
2777	Licence has expired
2778	Licence activation grace period has expired