Authlogics

Authlogics SIEM Integration Guide

MFA and PSM Event Codes

Product Version: 4.0.1736.0

Publication date: August 2020

Call us on:	+44 1344 568 900 (UK/EMEA) +1 408 706 2866 (US)
Email us:	sales@authlogics.com

Table of Contents

Introduction

This document has been created to detail the Events codes generated by Authlogics Multi-factor Authentication and Password Security Manager solutions for analysis and integration within SIEM solutions. Authlogics Event codes are all written to the Authlogics Authentication Server and Domain Controller Windows Application Event logs.

Authlogics Event codes are broken down into 3 categories, these being:

- Information
- Warning
- Error

Multi-factor Authentication Event Codes

Logins

Valid Logins

Event Type : **Information**

Successfully authenticated using …

Code	Description
1498	AD credentials via RADIUS
1502	PINgrid deviceless token, user must change pattern at next login
1503	PINgrid deviceless token
1504	PINgrid 2 factor token user must change pattern at next login
1505	PINgrid 2 factor token
1507	PINphrase deviceless token, user must change answer at next logon
1508	PINphrase deviceless token
1509	PINphrase 2 Factor token
1510	PINpass 2 Factor token , user must change PIN at next logon
1511	PINpass 2 factor token
1512	PINgrid 2 factor token, user must change pattern at next login
1513	PINgrid 2 factor token
1523	PINgrid 2 factor token user must change pattern at next login
1524	PINgrid 2 factor token
1525	PINpass 2 factor token
1526	PINphrase 2 Factor token, user must change answers at next login
1527	PINphrase 2 Factor token
1528	Emergency Access code
1529	Emergency Access code via RADIUS
1530	PINgrid deviceless via RADIUS user must change pattern at next login
1531	PINgrid deviceless via RADIUS
1532	PINgrid 2 Factor via RADIUS user must change pattern at next login
1533	PINgrid 2 Factor via RADIUS
1534	PINgrid 2 Factor via RADIUS user must change pattern at next login
1535	PINgrid 2 Factor
1536	PINpass 2 Factor token via RADIUS
1537	PINpass 2 Factor token via RADIUS

1538	PINphrase deviceless token via RADIUS
1539	PINphrase deviceless token
1540	PINphrase 2 Factor token via RADIUS
1541	PINphrase 2 Factor token
1548	PINpass 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

Invalid Logins

Event Type : **Warning**

Code	Description
2500	Account lockout settings prevented login
2501	Invalid passcode was provided
2505	Failed to authenticate PINphrase user
2506	Failed to authenticate PINpass user
2507	Failed to authenticate PINgrid user
2514	Invalid user account
2515	Invalid YubiKey token provided
2516	Invalid YubiKey token provided via RADIUS
2519	Invalid PINgrid transaction token entered
2520	Account lockout settings prevented login via RADIUS
2521	Failed to authenticate PINgrid user via RADIUS
2522	Failed to authenticate PINpass user via RADIUS
2523	Failed to authenticate PINphrase user via RADIUS
2524	Failed to authenticate PINphrase user via RADIUS. User is not a member of the RADIUS user's role.
2650	OTP failed is Web Operator Portal
2720	Invalid OTP
2768	Invalid Emergency Override Code. Code has expired
3752	Invalid Emergency Override Code. Invalid Active Directory Password
3753	Invalid Emergency Override Code. Invalid Code

User Actions and Provisioning Codes

This section deals with the Event codes generated when user account settings are.

Success Actions

Event Type : **Information**

Code	Description
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
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 PINgrid
1675	User successfully provisioned for PINphrase
1676	User successfully provisioned for PINpass
1677	Successfully generated new PINgrid pattern
1678	Successfully sent security token
1682	Successfully generated new PINphrase code word
1683	Successfully generated new PINpass code
1684	Successfully enabled account for PINgrid
1685	Successfully enabled account for PINphrase
1686	Successfully enabled account for PINpass
1687	Successfully disabled account for PINgrid
1688	Successfully disabled account for PINphrase
1689	Successfully disabled account for PINpass
1698	Successfully changed PINgrid 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

Failed Actions

Event Type : **Warning**

Code	Description
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

Failed PINgrid, PINpass and PINphrase Change Actions

Event Type : **Warning**

Code	Description
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 PINpass PIN is smaller than the required PIN length
2766	The PINphrase answer is smaller than the required answer length
2782	The entered pattern does not contain a sufficient number of selected cells

Password Security Manager Event Codes

Change Success

Event Type : **Information**

Code	Description
1400	The provided password complies with Authlogics PSM has been accepted
1401	DisablePasswordPolicyAgent is enabled (On). The provided password complies with Authlogics PSM and has been accepted.
1418	Password is an Authlogics 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 Authlogics Password Security Management and has been accepted for use
1425	The provided password for complies with Authlogics Password Security Management and has been accepted for use by the Authlogics Authentication Server.

Change Failed

Event Type : **Warning**

Code	Description
2400	Password does not comply with Authlogics 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

Authlogics Licence Event Codes

Success Events

Event Type : **Information**

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

Failed Events

Event Type : **Warning**

Code	Description
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