

IA 2:User Identification and Authentication - Event Detail Expanded

Reporting Filter Information

Begin Time: 12/13/2006 1:11:07 AM

End Time: 12/13/2006 10:11:07 AM

Created On: 12/17/2006 1:15:03 PM

Computer: <ALL>

Domain: <ALL>

User: <ALL>

Computer Group: ECC ECAR for Sarbanes-Oxley Act - Windows Security Events

Event ID: <ALL>

ECC Enterprise Compliance Auditing & Reporting

PURPOSE

ECAR IA-2: User Identification and Authentication

FEATURES

Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

CONFIGURATION

Supplemental Guidance: Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein. FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication. For other than remote situations, when users identify and authenticate to information systems within a specified security perimeter which is considered to offer sufficient protection, NIST Special Publication 800-63 guidance should be applied as follows: (i) for low impact information systems, tokens that meet Level 1, 2, 3, or 4 requirements are acceptable; (ii) for moderate-impact information systems, tokens that meet Level 2, 3, or 4 requirements are acceptable; and (iii) for high-impact information systems, tokens that meet Level 3 or 4 requirements are acceptable. In addition to identifying and authenticating users at the information system level, identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Control Enhancements: (1) The information system employs multifactor authentication. SOURCE: NIST 800-53

© 2000-2006 Enterprise Certified Corporation, all rights reserved.

Event ID	Date Time	Type	Domain	Computer	User
528	12/13/2006 8:25:49 AM	Audit Success	WORKGROUP	ECAREVAL	LOCAL SERVICE

Event ID	Date Time	Type	Domain	Computer	User
Description:	Successful Logon: User Name: LOCAL SERVICE Domain: NT AUTHORITY Logon ID: (0x0,0x3E5) Logon Type: 5 Logon Process: Advapi Authentication Package: Negotiate Workstation Name: Logon GUID: - Caller User Name: ECAREVAL\$ Caller Domain: WORKGROUP Caller Logon ID: (0x0,0x3E7) Caller Process ID: 452 Transited Services: - Source Network Address: - Source Port: -				
528	12/13/2006 8:25:49 AM	Audit Success	WORKGROUP	ECAREVAL	NETWORK SERVICE
Description:	Successful Logon: User Name: NETWORK SERVICE Domain: NT AUTHORITY Logon ID: (0x0,0x3E4) Logon Type: 5 Logon Process: Advapi Authentication Package: Negotiate Workstation Name: Logon GUID: - Caller User Name: ECAREVAL\$ Caller Domain: WORKGROUP Caller Logon ID: (0x0,0x3E7) Caller Process ID: 452 Transited Services: - Source Network Address: - Source Port: -				
528	12/13/2006 8:25:49 AM	Audit Success	WORKGROUP	ECAREVAL	SYSTEM

Event ID	Date Time	Type	Domain	Computer	User
Description:	Successful Logon: User Name: SYSTEM Domain: NT AUTHORITY Logon ID: (0x0,0x3E7) Logon Type: 0 Logon Process: - Authentication Package: - Workstation Name: - Logon GUID: - Caller User Name: - Caller Domain: - Caller Logon ID: - Caller Process ID: 4 Transited Services: - Source Network Address: - Source Port: -				
540	12/13/2006 8:26:55 AM	Audit Success	WORKGROUP	ECAREVAL	ANONYMOUS LOGON
Description:	Successful Network Logon: User Name: Domain: Logon ID: (0x0,0x9A34) Logon Type: 3 Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: Logon GUID: - Caller User Name: - Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: - Source Port: -				
680	12/13/2006 8:26:55 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: Administrator Source Workstation: ECAREVAL Error Code: 0x0				
552	12/13/2006 8:26:55 AM	Audit Success	WORKGROUP	ECAREVAL	SYSTEM

Event ID	Date Time	Type	Domain	Computer	User
Description:	Logon attempt using explicit credentials: Logged on user: User Name: ECAREVAL\$ Domain: WORKGROUP Logon ID: (0x0,0x3E7) Logon GUID: - User whose credentials were used: Target User Name: Administrator Target Domain: ECAREVAL Target Logon GUID: - Target Server Name: localhost Target Server Info: localhost Caller Process ID: 452 Source Network Address: - Source Port: -				
528	12/13/2006 8:26:55 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Successful Logon: User Name: Administrator Domain: ECAREVAL Logon ID: (0x0,0x9880) Logon Type: 5 Logon Process: Advapi Authentication Package: Negotiate Workstation Name: ECAREVAL Logon GUID: - Caller User Name: ECAREVAL\$ Caller Domain: WORKGROUP Caller Logon ID: (0x0,0x3E7) Caller Process ID: 452 Transited Services: - Source Network Address: - Source Port: -				
680	12/13/2006 8:27:02 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: Administrator Source Workstation: ECAREVAL Error Code: 0x0				
528	12/13/2006 8:27:02 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator

Event ID	Date Time	Type	Domain	Computer	User
Description:	Successful Logon: User Name: Administrator Domain: ECAREVAL Logon ID: (0x0,0x1009E) Logon Type: 5 Logon Process: Advapi Authentication Package: Negotiate Workstation Name: ECAREVAL Logon GUID: - Caller User Name: ECAREVAL\$ Caller Domain: WORKGROUP Caller Logon ID: (0x0,0x3E7) Caller Process ID: 452 Transited Services: - Source Network Address: - Source Port: -				
552	12/13/2006 8:27:02 AM	Audit Success	WORKGROUP	ECAREVAL	SYSTEM
Description:	Logon attempt using explicit credentials: Logged on user: User Name: ECAREVAL\$ Domain: WORKGROUP Logon ID: (0x0,0x3E7) Logon GUID: - User whose credentials were used: Target User Name: Administrator Target Domain: ECAREVAL Target Logon GUID: - Target Server Name: localhost Target Server Info: localhost Caller Process ID: 452 Source Network Address: - Source Port: -				
552	12/13/2006 8:27:03 AM	Audit Success	WORKGROUP	ECAREVAL	NETWORK SERVICE

Event ID	Date Time	Type	Domain	Computer	User
Description:	Logon attempt using explicit credentials: Logged on user: User Name: NETWORK SERVICE Domain: NT AUTHORITY Logon ID: (0x0,0x3E4) Logon GUID: - User whose credentials were used: Target User Name: Administrator Target Domain: ECAREVAL Target Logon GUID: - Target Server Name: localhost Target Server Info: localhost Caller Process ID: 1744 Source Network Address: - Source Port: -				
680	12/13/2006 8:27:03 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: administrator Source Workstation: ECAREVAL Error Code: 0x0				
528	12/13/2006 8:27:03 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Successful Logon: User Name: Administrator Domain: ECAREVAL Logon ID: (0x0,0x115B6) Logon Type: 2 Logon Process: Advapi Authentication Package: Negotiate Workstation Name: ECAREVAL Logon GUID: - Caller User Name: NETWORK SERVICE Caller Domain: NT AUTHORITY Caller Logon ID: (0x0,0x3E4) Caller Process ID: 1744 Transited Services: - Source Network Address: - Source Port: -				
680	12/13/2006 8:27:03 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: administrator Source Workstation: ECAREVAL Error Code: 0x0				
528	12/13/2006 8:27:03 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator

Event ID	Date Time	Type	Domain	Computer	User
Description:	Successful Logon: User Name: Administrator Domain: ECAREVAL Logon ID: (0x0,0x117E4) Logon Type: 2 Logon Process: Advapi Authentication Package: Negotiate Workstation Name: ECAREVAL Logon GUID: - Caller User Name: NETWORK SERVICE Caller Domain: NT AUTHORITY Caller Logon ID: (0x0,0x3E4) Caller Process ID: 1744 Transited Services: - Source Network Address: - Source Port: -				
528	12/13/2006 8:27:03 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Successful Logon: User Name: Administrator Domain: ECAREVAL Logon ID: (0x0,0x11C2E) Logon Type: 4 Logon Process: DCOMSCM Authentication Package: Negotiate Workstation Name: ECAREVAL Logon GUID: - Caller User Name: ECAREVAL\$ Caller Domain: WORKGROUP Caller Logon ID: (0x0,0x3E7) Caller Process ID: 652 Transited Services: - Source Network Address: - Source Port: -				
552	12/13/2006 8:27:03 AM	Audit Success	WORKGROUP	ECAREVAL	NETWORK SERVICE

Event ID	Date Time	Type	Domain	Computer	User
Description:	Logon attempt using explicit credentials: Logged on user: User Name: NETWORK SERVICE Domain: NT AUTHORITY Logon ID: (0x0,0x3E4) Logon GUID: - User whose credentials were used: Target User Name: Administrator Target Domain: ECAREVAL Target Logon GUID: - Target Server Name: localhost Target Server Info: localhost Caller Process ID: 1744 Source Network Address: - Source Port: -				
680	12/13/2006 8:27:03 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: administrator Source Workstation: ECAREVAL Error Code: 0x0				
552	12/13/2006 8:27:03 AM	Audit Success	WORKGROUP	ECAREVAL	SYSTEM
Description:	Logon attempt using explicit credentials: Logged on user: User Name: ECAREVAL\$ Domain: WORKGROUP Logon ID: (0x0,0x3E7) Logon GUID: - User whose credentials were used: Target User Name: Administrator Target Domain: ECAREVAL Target Logon GUID: - Target Server Name: localhost Target Server Info: localhost Caller Process ID: 652 Source Network Address: - Source Port: -				
680	12/13/2006 8:27:04 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: administrator Source Workstation: ECAREVAL Error Code: 0x0				
552	12/13/2006 8:27:04 AM	Audit Success	WORKGROUP	ECAREVAL	SYSTEM

Event ID	Date Time	Type	Domain	Computer	User
Description:	Logon attempt using explicit credentials: Logged on user: User Name: ECAREVAL\$ Domain: WORKGROUP Logon ID: (0x0,0x3E7) Logon GUID: - User whose credentials were used: Target User Name: Administrator Target Domain: ECAREVAL Target Logon GUID: - Target Server Name: localhost Target Server Info: localhost Caller Process ID: 652 Source Network Address: - Source Port: -				
528	12/13/2006 8:27:04 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Successful Logon: User Name: Administrator Domain: ECAREVAL Logon ID: (0x0,0x123C8) Logon Type: 4 Logon Process: DCOMSCM Authentication Package: Negotiate Workstation Name: ECAREVAL Logon GUID: - Caller User Name: ECAREVAL\$ Caller Domain: WORKGROUP Caller Logon ID: (0x0,0x3E7) Caller Process ID: 652 Transited Services: - Source Network Address: - Source Port: -				
538	12/13/2006 8:27:04 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	User Logoff: User Name: Administrator Domain: ECAREVAL Logon ID: (0x0,0x123C8) Logon Type: 4				
680	12/13/2006 8:47:01 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: Administrator Source Workstation: ECAREVAL Error Code: 0x0				

Event ID	Date Time	Type	Domain	Computer	User
528	12/13/2006 8:47:01 AM	Audit Success	WORKGROUP	ECAREVAL	Administrator
Description:	Successful Logon: User Name: Administrator Domain: ECAREVAL Logon ID: (0x0,0x56C3F) Logon Type: 2 Logon Process: User32 Authentication Package: Negotiate Workstation Name: ECAREVAL Logon GUID: - Caller User Name: ECAREVAL\$ Caller Domain: WORKGROUP Caller Logon ID: (0x0,0x3E7) Caller Process ID: 408 Transited Services: - Source Network Address: 127.0.0.1 Source Port: 0				
552	12/13/2006 8:47:01 AM	Audit Success	WORKGROUP	ECAREVAL	SYSTEM
Description:	Logon attempt using explicit credentials: Logged on user: User Name: ECAREVAL\$ Domain: WORKGROUP Logon ID: (0x0,0x3E7) Logon GUID: - User whose credentials were used: Target User Name: Administrator Target Domain: ECAREVAL Target Logon GUID: - Target Server Name: localhost Target Server Info: localhost Caller Process ID: 408 Source Network Address: 127.0.0.1 Source Port: 0				
540	12/13/2006 8:47:47 AM	Audit Success	WORKGROUP	ECAREVAL	IUSR_ECAREVAL

Event ID	Date Time	Type	Domain	Computer	User
Description:	Successful Network Logon: User Name: IUSR_ECAREVAL Domain: ECAREVAL Logon ID: (0x0,0x6646E) Logon Type: 8 Logon Process: Advapi Authentication Package: Negotiate Workstation Name: ECAREVAL Logon GUID: - Caller User Name: NETWORK SERVICE Caller Domain: NT AUTHORITY Caller Logon ID: (0x0,0x3E4) Caller Process ID: 2652 Transited Services: - Source Network Address: - Source Port: -				
552	12/13/2006 8:47:47 AM	Audit Success	WORKGROUP	ECAREVAL	NETWORK SERVICE
Description:	Logon attempt using explicit credentials: Logged on user: User Name: NETWORK SERVICE Domain: NT AUTHORITY Logon ID: (0x0,0x3E4) Logon GUID: - User whose credentials were used: Target User Name: IUSR_ECAREVAL Target Domain: ECAREVAL Target Logon GUID: - Target Server Name: localhost Target Server Info: localhost Caller Process ID: 2652 Source Network Address: - Source Port: -				
680	12/13/2006 8:47:47 AM	Audit Success	WORKGROUP	ECAREVAL	IUSR_ECAREVAL
Description:	Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: IUSR_ECAREVAL Source Workstation: ECAREVAL Error Code: 0x0				
538	12/13/2006 9:22:12 AM	Audit Success	WORKGROUP	ECAREVAL	IUSR_ECAREVAL

Event ID	Date Time	Type	Domain	Computer	User
Description:		User Logoff:			
		User Name: IUSR_ECAREVAL			
		Domain: ECAREVAL			
		Logon ID: (0x0,0x6646E)			
		Logon Type: 8			