



## Identisphere™ ID-Enforce™ and Meeting FISMA Compliance



The Federal Information Security Management Act of 2002 (FISMA) is a federal law enacted in 2002. The Act has brought information security to the attention of the Federal Government and has increased awareness regarding the protection of information and securing the networks in which it resides. FISMA imposes a mandatory set of processes that must be followed for all information systems used or operated by a US Government federal agency or by a contractor or other organization on behalf of a US Government agency. These processes must follow a combination of Federal Information Processing standards (FIPS) documents, the special publications SP-800 series issued by NIST, and other legislation pertinent to federal information systems.

Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST Special Publication 800-53 revision 1, which contains the management, operational, and technical safeguards or countermeasures prescribed for an information system. NIST SP 800-53A – the latest iteration of the publication - provides guidance on the assessment methods, policies, procedures and continuous monitoring where applicable to individual controls.

### **The Need for Identity Aware Networks**

Applied Identity is a leading provider of enterprise-class, identity aware network solutions that allow organizations to:

- Audit user access and resource usage based on user identity
- Unify multiple disparate identity stores to create a single authoritative source
- Define new or redefine existing access policies based on user identity rather than IP address
- Enforce user access policies at the network layer
- Leverage existing identity stores such as Microsoft Active Directory, SUNOne, Novell eDirectory, and other LDAP and non-LDAP compliant identity repositories

Applied Identity is the only vendor to provide a complete policy lifecycle management solution that enables global policy creation and network-level enforcement based on user identity.

### **ID-Enforce**

Applied Identity's ID-Enforce is an identity aware network access gateway solution that enables organizations to cost effectively manage the risk associated with inappropriate access to critical resources. ID-Enforce ties access policies with user network identity (via LDAP integration), and network resources, for authorization and audit of network activities. Access policies are created based upon role, group and individual identity, simplifying policy creation and management while ensuring consistent enforcement. ID-Enforce sits inline, close to the resources it protects which ensures that all users must pass through it in order to access data and applications.

### **Comparing ID-Enforce to NIST 800-53A Requirements**

The feature set of Applied Identity's ID-Enforce solution has been mapped to the following controls and control enhancements within the Access Control (AC) section of the NIST SP 800-53A publication. Additional NIST SP 800-53A mappings for the Audit and Accounting (AU) section are addressed separately by Applied Identity's ID-Audit solution in a separate document.

**Note:** The 20 Controls outlined in the Access Control section (AC-1 through AC-20) have additional control enhancements that provide greater clarification and functionality requirements and are listed below in the following format AC-3(1).1, AC-4(1).1, AC-4(2).1. etc.

Controls and Control Enhancements in the following sections have been omitted as they are either a) written policy or internal procedures b) Non-applicable functionality c) Non supported functionality; AC-1, AC-2, AC-15, AC-17, AC-18, and AC-19

800-53A CNTL NO.	800-53A CONTROL NAME	Applied Identity Support	Applied Identity Function
<b>AC - 3</b>	Access Enforcement		
<b>AC-3</b>	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	Supported	Single point of management to point of enforcement based upon domain identity.
<b>AC-3(1).1</b>	The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.	Supported	Single point of management to point of enforcement based upon domain identity.
<b>AC - 4</b>	Information Flow Enforcement		
<b>AC-4</b>	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Supported	Information flow is enforced at the destination IP address/service/port level for all transactions involving identity (user-to-resource). Packet marking by ID-Mark client for non-repudiation of events.
<b>AC-4(1).1</b>	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Supported	Information flow is enforced at the destination IP address/service/port level for all transactions involving identity (user-to-resource). Packet marking by ID-Mark client for non-repudiation of events.
<b>AC-4(2).1</b>	The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.	Supported	Information flow is enforced at the destination IP address/service/port level for all transactions involving identity (user-to-resource). Can also be enforced around network segments and IP ranges.
<b>AC-4(3).1</b>	The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.	Supported	ID-Enforce Support for Dynamic User Policy Updates via ID-Enforce.
<b>AC-5</b>	Separation of Duties		
<b>AC-5</b>	The information system enforces separation of duties through assigned access authorizations.	Supported	Separation of duties is implicit based upon the UserID and associated roles established at the directory level and enforced at the destination IP address/service/port level.
<b>AC-6</b>	Least Privilege		
<b>AC-6</b>	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	Supported	Least privilege access is implicit based upon roles established at the directory level, default deny. At the system administration level, policy implementation can require oversight approval prior to activation.
<b>AC-7</b>	Unsuccessful Login Attempts		
<b>AC-7</b>	The information system enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to [Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.	No direct feature mapping due to ID-Enforce overriding functionality	Protected resources are obfuscated prior to authentication. Enforced by leveraging the Directory level account policies.

800-53A CNTL NO.	800-53A CONTROL NAME	Applied Identity Support	Applied Identity Function
<b>AC-7</b>	Unsuccessful Login Attempts		
<b>AC-7(1).1</b>	The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	No direct feature mapping due to ID-Enforce overriding functionality	Protected resources are obfuscated prior to authentication. Enforced by leveraging the Directory level account policies.
<b>AC-8</b>	System Use Notification		
<b>AC-8</b>	The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.	Indirect Support	This is currently a function of Microsoft GINA or via customization of the Web Auth for authentication.
<b>AC-9</b>	Previous Logon Notification		
<b>AC-9</b>	The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.	NA Functionality leveraged by ID-Enforce	*This feature is a Directory function but these are attributes that ID-Enforce can leverage for authentication services. Web Auth does provide users with session time elapsed and remaining time of session.
<b>AC-10</b>	Concurrent Session Control		
<b>AC-10</b>	The information system limits the number of concurrent sessions for any user to [Assignment: organization-defined number of sessions].	Indirect Support	ID-Mark or Web Auth can limit one user login session per machine (hardware id).
<b>AC-11</b>	Session Lock		
<b>AC-11</b>	The information system prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	Supported	ID-Mark and Web Auth times out after 60 minutes by default. The user is forced to re-authenticate in that interval to maintain connectivity. Active sessions will keep the connection open. Once Idled out, the user must re-authenticate.
<b>AC-12</b>	Session Termination		
<b>AC-12</b>	The information system automatically terminates a remote session after [Assignment: organization-defined time period] of inactivity.	Supported	ID-Mark and Web Auth times out after 60 minutes by default. The user is forced to re-authenticate in that interval to maintain connectivity. Active sessions will keep the connection open. Once Idled out, the user must re-authenticate.
<b>AC-12(1).1</b>	Automatic session termination applies to local and remote sessions.	Supported	ID-Mark and Web Auth are location agnostic and times out after 60 minutes by default. The user is forced to re-authenticate in that interval to maintain connectivity. Active sessions will keep the connection open. Once Idled out, the user must re-authenticate.

800-53A CNTL NO.	800-53A CONTROL NAME	Applied Identity Support	Applied Identity Function
<b>AC-13</b>	Supervision and Review—Access Control		
<b>AC-13</b>	The organization employs automated mechanisms to facilitate the review of user activities.	Supported	Audit trails created on authorized and unauthorized user access to protected resources. Administrator audit log of the implementation, changes and removal of policy.
<b>AC-13(1).1</b>	The organization employs automated mechanisms to facilitate the review of user activities.	Supported	Audit trails created on authorized and unauthorized user access to protected resources. Administrator audit log of the implementation, changes and removal of policy.
<b>AC - 14</b>	Permitted Actions without Identification or Authentication		
<b>AC-14(1).1</b>	The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.	Supported	This is a case for global policies. Nested groups etc may not come into effect since the user is not authenticated.
<b>AC - 16</b>	Automated Labeling		
<b>AC-16</b>	The information system appropriately labels information in storage, in process, and in transmission.	Indirect Support (in transmission)	Packet marking by ID-Mark client for non-repudiation of events.
<b>AC - 20</b>	Use of External Information Systems		
<b>AC-10</b>	The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system.	Indirect Support	If policy stated that no device can access the network without client driver, no external information system could log in.

