strongdm

SOLUTION GUIDE

How StrongDM Helps with NIST 800-53 Access Controls

NIST Special Publication 800-53 is a framework developed by the National Institute of Standards and Technology. It outlines requirements of security and privacy controls to heighten the security information systems used within the federal government to help reduce the risk of cyberattacks on critical infrastructure.

Below are the specific requirements where strongDM can help you meet NIST 800-53 requirements.

Logical & Physical Access Controls

Requirement	Detail	strongDM Features
AC-3(1)	ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS [Withdrawn: Incorporated into AC-6].	
AC-3(2)	ACCESS ENFORCEMENT | DUAL AUTHORIZATION Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	StrongDM allows you to authenticate and/or provision users & groups through your identity provider. With Access Workflows you can require multple team members to approve access requests.
AC-3(3)	ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy, and where the policy: a. Is uniformly enforced across the covered subjects and objects within the system; b. Specifies that a subject that has been granted access to information is constrained from doing any of the following; 1. Passing the information to unauthorized subjects or objects; 2. Granting its privileges to other subjects;	StrongDM supports Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) policies. Additionally, strongDM enables you to grant temporary or just-in-time access with least-privilege by default.

Logical & Physical Access Controls (Cont)

Requirement	Detail	strongDM Features
AC-3(3) (Cont)	3. Changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components; 4. Choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and 5. Changing the rules governing access control; and c. Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints.	
AC-3(4)	ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following: a. Pass the information to any other subjects or objects; b. Grant its privileges to other subjects; c. Change security attributes on subjects, objects, the system, or the system's components; d. Choose the security attributes to be associated with newly created or revised objects; or e. Change the rules governing access control.	StrongDM defines the perimeter around the covered set of resources. Organizations have control within the defined area to verify, detect, and audit all access requests.
AC-3(5)	ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION Prevent access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states.	StrongDM governs access control lists and security configurations that protect against low privilege users. When these users access in a native state they are unable to inspect configurations. Security-relevant information is isolated and protected by fine grain permissions.

Logical & Physical Access Controls (Cont)

Requirement	Detail	strongDM Features
AC-3(6)	ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION [Withdrawn: Incorporated into MP-4, SC-28]	
AC-3(7)	ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].	User access privileges are derived from their assigned roles or attributes with a comprehensive audit trail to detect the who, what, where, and when of every interaction with backend infrastructure. Roles can be defined in StrongDM or synced with an identity provider.
AC-3(8)	ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].	Instantly revoke permanent or just-in-time access to resources through the strongDM admin UI or through your identity provider.
AC-3(9)	ACCESS ENFORCEMENT | CONTROLLED RELEASE Release information outside of the system only if: a. The receiving [Assignment: organization-defined system or system component] provides [Assignment: organization-defined controls]; and b. [Assignment: organization-defined controls] are used to validate the appropriateness of the information designated for release.	StrongDM enforces access policies across all employees customers, and vendors. Configure users to allow temporary or project-based access. All activities are logged to view actions taken against a resource.
AC-3(10)	ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions] by [Assignment: organization-defined roles].	When configuring StrongDM, we recommend customers configure break glass accounts in the unlikely event that StrongDM is unavailable. If using those accounts, we recommend that the customer also configure auditing of account usage (for example through a SIEM) to ensure that the accounts are being used appropriately.

Logical & Physical Access Controls (Cont)

Requirement	Detail	strongDM Features
AC-3(11)	ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES Restrict access to data repositories containing [Assignment: organization-defined information types].	Customers can configure resources in StrongDM to have a limited set of permissions or available commands. Those permissions can then be inherited by the StrongDM users through role-based access, attribute-based access, or tags.
AC-3(12)	ACCESS ENFORCEMENT | ASSERT AND ENFORCE APPLICATION ACCESS a. Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [Assignment: organization-defined system applications and functions]; b. Provide an enforcement mechanism to prevent unauthorized access; and c. Approve access changes after initial installation of the application.	The StrongDM gateway is the policy enforcement point to assert and enforce application access.
AC-3(13)	ACCESS ENFORCEMENT | ATTRIBUTE-BASED ACCESS CONTROL Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].	User access privileges are derived from their assigned roles or attributes with the exception of temporary access and no role assigned. StrongDM's Access Worklfows can be used to grant temporary access based on attributes such as environment tags, resource names, or time of day.
AC-3(15)	ACCESS ENFORCEMENT | DISCRETIONARY AND MANDATORY ACCESS CONTROL a. Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy; and b. Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes; access can be permanent or temporary. Comprehensive permissions auditing is available for all access types.