XTON
technologies

Xton Access Manager for NIST 800-171 Compliance

XTON TECHNOLOGIES, LLC | PHILADELPHIA

Contents

About NIST.SP.800-171

NIST Special Publication 800-171 provides guidelines to protect controlled unclassified information in nonfederal information systems and organizations.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and its collaborative activities with industry, government, and academic organizations.

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations. NIST.SP.800-171 publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI.

Various government agencies refer to NIST.SP.800-171 when describing security requirements for non-government partners and subcontractors. For example, As of December 2015, Defense Federal Acquisition Regulation Supplement (DFARS 225.204-7012) requires contractors to implement NIST Special Publication (SP) 800-171 standards "as soon as practical, but not later than December 31, 2017."

About Xton Access Manager

Xton Access Manager (XTAM) is an agentless, cross-platform privileged access management solution with unlimited licensing model built from the ground up with an enterprise feature set. Simple to implement, without your typical enterprise cost and effort.

A privileged account refers to non-individual, often shared, user accounts frequently used by machines for or by administrators to perform maintenance activities. Examples of such accounts include:

- Accounts used by machines to communicate between each other;
- Shared accounts shared by groups of people (external billing, corporate representatives);
- Accounts for Database Administrators, database schema, application pool owners, global administrators;
- Local computer accounts (root, administrator, tomcat, jenkins, jira);
- Built-in IoT accounts (sensors, printers, routers, coffee machines, cameras, beacons).

XTAM provides out-of-the-box features to discover, manage, access and monitor privileged accounts:

- A secure AES-256 encrypted Identity Vault to maintain total administrative control over all your passwords, certificates, key, files, secrets and privileged accounts.
- Privileged session recording to ensure all sessions are retained and can be used for diagnosis or forensic investigations.
- Integrated job and policy engine to automate password resets, privileged account discovery and repetitive tasks.
- Full system event and user audit trails that can trigger notifications and in-application alerts.

Recommended XTAM Workflow

XTAM supports multiple use cases and can be used as a part of several security and productivity enhancement workflows. To help organizations to comply with NIST.SP.800-171 requirements we recommend the following workflow.

Step	Description
Discover	Discover privileged accounts in the network using XTAM discovery facilities.
Import	Import privileged accounts to the XTAM vault from the discovery process or from other sources using the import facilities. Enter undiscovered privileges accounts into the XTAM vault.
Manage	Define password rotation policy for imported or entered privileged accounts describing when and how the passwords should be rotated for groups of accounts or individual accounts. Grant and revoke access to privileged account records or groups of records in the XTAM vault for the organization of users and groups. Use Microsoft Active Directory, LDAP based user directory or local XTAM user directory as a directory of the organization of users and groups
Rotate	Let the XTAM engine change passwords for managed accounts. Alternatively, change privileged accounts passwords manually and update the XTAM vault. After this step all privileged account activities will be performed using the XTAM instance because the actual password would be unknown to all users.
Unlock	Authorize XTAM users to unlock passwords or certificates in XTAM vault when needed.
Access	Authorize XTAM users to connect to managed privileged accounts without disclosing credentials when needed using XTAM session manager.
Execute	Authorize XTAM users to execute privileged commands and scripts on managed information systems without disclosing credentials when needed using the XTAM job engine.
Monitor	Use XTAM notification facilities, audit log, history, job execution history and session history reports to monitor system activity. Stream system logs to your organization's SIEM system for global analysis.

Mapping XTAM Functions to the Guideline Requirements

The following pages contain tables that summarize how the XTAM functionality maps to the guideline requirements to ensure compliance with the NIST.SP.800-171 framework. Note that only relevant product mappings are included here. Other requirements in this standard as well as ensuring compliance with areas of the organization security practices not covered by the XTAM recommended workflow, should be addressed separately.

Addressing § 3.1 Access Control Requirements

Number	Control	Description
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	XTAM provides account-level permission controlled access of named user accounts or processes to shared privileged accounts. XTAM controls access to information systems based on the authorization of an individual user or a process permissioned to access an information system even in case the system itself uses shared privileged accounts.
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	XTAM allows execution of scripts and commands with elevated privileges by authorized users and processes while rejecting execution of any other commands on the remote information system or even console access to the system.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	XTAM granular account-level permission scheme enables fine control over segregation of privileged accounts duties among several users. XTAM extensive notifications and logging mechanism up to session recording allows independent review of the user's activity in the system.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	XTAM granular account-level permission scheme over privileged accounts and transactions allows for the reduction of the named user's privileges on the information system.
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	XTAM encourages the use of a minimal number of rarely used shared privileged accounts for sensitive operations accessible only through XTAM while using low-privileged named user accounts for the daily non-security activities.
3.1.7	Prevent non-privileged users from executing privileged	XTAM automated password reset functionality for privileged accounts blocks access of non-privileged users to sensitive information systems

	functions and audit the execution of such functions.	without using XTAM's permission controlled and audited system for access.
3.1.8	Limit unsuccessful logon attempts.	XTAM establishes an information system access only through XTAM interface enforcing individual user login policies to access XTAM system even for information systems that do not natively support login policies.
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	XTAM establishes an information system access session only through XTAM instance blocking direct access to the information system and enforcing information system session timeout.
3.1.11	Terminate (automatically) a user session after a defined condition	XTAM establishes an information system access session only through XTAM instance blocking direct access to the information system and enforcing session termination rules defined by XTAM.
3.1.12	Monitor and control remote access sessions.	XTAM establishes an information system access session only through XTAM instance blocking direct access to the information system and enforcing session monitor, control as well as session recording.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	XTAM establishes an information system access session only through XTAM instance blocking direct access to the information system and enforcing HTTPS protocol while streaming session data.
3.1.14	Route remote access via managed access control points.	XTAM establishes an information system access session only through XTAM instance blocking direct access to the information system by using a periodic password rotation routine.
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	XTAM allows execution of scripts and commands on the remote information systems with elevated privileges by authorized users and processes. XTAM uses a record-level permission scheme to control visibility of the data collected by the executed scripts.
3.1.20	Verify and control/limit connections to and use of external information systems.	XTAM delivers all functionality including access to information systems agentlessly using a browser based interface. It simplifies control over accessing the system from the external information systems.

3.1.21	Limit use of organizational portable storage devices on external information systems.	XTAM delivers all functionality including access to information systems agentlessly using a browser based interface. It simplifies control over accessing the system from the external information systems.
3.1.22	Control information posted or processed on publicly accessible information systems.	XTAM delivers all functionality including access to information systems agentlessly using a browser based interface. It simplifies control over accessing the system from the external information systems.

Addressing § 3.3 Audit and Accountability Controls Requirements

Since XTAM handles traffic to all privileged sessions, it helps to address the privileged accounts portion of the Audit and Accountability Controls despite the audit facilities described in this chapter being limited to the XTAM system.

Number	Control	Description
3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	XTAM generates extensive audit event logs about activities inside the system including information systems access as well as session recordings. XTAM internal logs could be optionally integrated with other security analytics tools via the syslog service. This information could be used as a basis for organizational wide audit log management.
3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	XTAM provides permission controlled access from individual user accounts or processes to shared privileged accounts. XTAM records audit log activity related to shared privileged accounts referencing the original named user account to track the activity back to the real user.
3.3.3	Review and update audited events.	XTAM provides system audit log events about changes to the system configuration, permissions and the access of information systems. XTAM optionally integrates with syslog servers to stream events for organizational wide analysis.
3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of	XTAM provides system audit log events about changes to the system configuration, permissions and the access of sensitive information systems. XTAM optionally integrates with syslog servers to stream events for organizational wide analysis.

	inappropriate, suspicious, or unusual activity.	
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	XTAM provides system audit log events about changes to the system configuration, permissions and the access of sensitive information systems. XTAM optionally integrates with syslog servers to stream events for organizational wide analysis.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	XTAM provides read only system audit log events about changes to the system configuration, permissions and the access of sensitive information systems. XTAM optionally integrates with syslog servers to stream events for organizational wide analysis.
3.3.9	Limit management of audit functionality to a subset of privileged users.	XTAM uses role based access to system functionality allowing access of audit logs to authorized personnel only.

Addressing § 3.4 Configuration Management Controls Requirements

Number	Control	Description
3.4.1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	XTAM provides a discovery option to detect privileged accounts that should be used as a part of the inventory process.

Addressing § 3.5 Identification and Authentication Controls Requirements

Number	Control	Description
3.5.1	Identify information system users, processes acting on behalf of users, or devices.	XTAM provides account-level permission controlled access of authenticated named user accounts or processes to shared privileged accounts. XTAM controls access to information systems based on the authorization of individual user or a process permissioned to access an information system even in case the system itself uses shared privileged accounts.
3.5.2	Authenticate (or verify) the identities of those users,	XTAM provides account-level permission controlled access of authenticated named user

	processes, or devices, as a prerequisite to allowing access to organizational information systems.	accounts or processes to shared privileged accounts. XTAM controls access to information systems based on the authorization of individual user or a process permissioned to access an information system even in case the system itself uses shared privileged accounts.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	XTAM establishes an information system access session only through the XTAM instance using the HTTPS protocol blocking direct access to the information system by using periodic password rotation routine. The XTAM authentication process includes several multi-factor authentication options.
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	XTAM establishes an information system access session only through the XTAM instance using the HTTPS protocol blocking direct access to the information system by using periodic password rotation routine. The XTAM authentication process includes replay resistant option.
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	XTAM uses automated policy driven password reset routine for managed privileged accounts with randomly generated passwords and the option to specify password complexity.
3.5.8	Prohibit password reuse for a specified number of generations.	XTAM uses automated policy driven password reset routine for managed privileged accounts with randomly generated passwords and the option to specify password complexity.

Addressing § 3.11 Risk Assessment Controls Requirements

Number	Control	Description
3.11.2	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	XTAM discovery process scans network to detect accounts with factory default and pre-defined passwords.
3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	XTAM automated password reset routine optionally resets factory default and pre-defined passwords of privileged accounts.

Conclusion

By partnering with Xton Technologies, organizations can address their compliance and security requirements as defined in NIST.SP.800-171 guidelines, leaving fewer gaps and improving efficiency over their privileged access management practices.

About Us

Philadelphia, PA based Xton Technologies makes it easy and affordable to have high security for your privileged access. Our enterprise grade XT Access Manager (XTAM) is purpose built to protect against malicious or accidental access from both within and beyond your firewall. The XTAM platform works across the corporate network, third party cloud infrastructure and is accessible using any modern browser on the desktop or mobile.

Xton Access Manager software is brought to you by industry veterans focusing on enterprise software development helping IT administrators in cyber security and content management areas since 2004. With more than 3000 customers around the globe and an experience in organic growth of a business from a small startup to an acquisition the team aligns its goals with the success of its clients.

The team goal is to disrupt the market with simple to install, to evaluate, to buy, to implement and to maintain software at the reasonable price point. The software that removes complexity barriers for the majority of businesses, large and small, to protects their IT infrastructure. Let's make the world better connected and more secure – together.