



STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



STANDARD 630S1: Authenticator Management

VERSION NUMBER	Standard 630S1-02
VERSION DATE	January 16, 2019
STANDARD TITLE	Authenticator Management
GOVERNING POLICY	This standard is governed by Policy 630: Identification and Authentication, regardless of revision.
OBJECTIVE	The objective of this standard is to define the requirements for authenticated access to state information systems and provide the requirements to manage implementation, safeguard, and use of password-based authentication and token-based multi-factor authentication (MFA).
REQUIREMENTS	<p>Users must uniquely identify themselves to a system or network resource and verify that identity with one or more authentication factors. Authentication factors include something a person <i>knows</i> (a password, pass-phrase, PIN, etc.), something a person <i>has</i> (a token, access card, etc.), or something a person <i>is</i> (biometric data which includes fingerprints, palm prints, DNA, iris, or facial recognition).</p> <p>1. GENERAL SECURITY REQUIREMENTS</p> <p>The following general security requirements apply to all types of authentication factors and/or processes:</p> <p>1.1. Authentication factors must never be shared, cached, stored in any readable form, or kept in locations where unauthorized persons might discover them. [IA-5h.]</p> <p>1.2. Ensure systems obscure feedback of authentication information during the authentication process. [IA-6]</p> <p>1.3. A biometric may be used for user identification to a device (such as a smartphone, tablet, or laptop) after authentication to the system or network (using password or multi-factor) has been achieved.</p>

1.4. A biometric may be used for authentication only as a component of two- or three-factor authentication. A biometric may not be used as the single authentication factor. Biometric security guidelines are provided in [Guideline 630G1: Biometric Authentication](#).

2. PASSWORD REQUIREMENTS

2.1. Password Policy Settings: Password policy settings for enterprise systems shall be configured by group policy at the domain level. The following password policy settings control the complexity and lifetime of passwords. The required minimum settings for passwords are outlined in Table 1. Agencies may establish stricter settings where required. [IA-5 (CE1)]

Table 1: Password Policy Settings

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age (non-privileged accounts)	90 days
Maximum password age (privileged accounts)	60 days
Minimum password age	1 day
Minimum password length	8 characters *
Password must meet complexity requirements **	Enabled
Store password using reversible encryption for all users in the domain	Disabled
Temporary password for system logon with an immediate change to a permanent password [IA-5 (CE1(f))]	Enabled

2.1.1. * For privileged accounts (such as Domain Administrator accounts) and service accounts, a minimum password length of 15 characters is recommended. [IA-5 (CE1(a))]

2.1.2. ** Complexity Requirements: Passwords shall use a combination of upper and lowercase characters, numbers, and special characters (punctuation symbols such as !@#%&*). Note: RACF special (National) characters are limited to @, #, and \$. [IA-5 (CE1(a))]

2.2. Password Selection: The individual user is responsible for selecting a complex password (or pass-phrase) that is not easily guessed. Password selection shall comply with the following requirements:

2.2.1. Passwords shall not be a dictionary word.

2.2.2. Passwords shall not be a proper name.

2.2.3. Passwords shall not be the same as the user ID.

2.2.4. Users shall employ different passwords on each system to which they are granted access (unless the system uses Active Directory logon credentials for authentication).

2.3. Password Storage and Control:

2.3.1. Passwords shall not be written down nor stored where they can be viewed by others. [IA-5h.]

2.3.2. Passwords must never be cached. Never use the “Remember Password” feature of any application, browser, or website.

2.3.3. Passwords must never be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, or in computers without access control. [IA-5h.]

2.3.4. Passwords shall only be stored and transmitted in an encrypted or hashed format. [IA-5 (CE1 (c))]

2.3.5. Keep passwords secure and do not share accounts. Do not reveal your account password to anyone or allow use of your account by others. [IA-5h.]

2.4. Service Account Passwords: For service accounts that run under system or root, or that run as administrator or with other elevated privilege, the passwords on such accounts:

2.4.1. Shall not be null, [IA-5 (CE1(a))]

2.4.2. Shall not be set to never expire, and [IA-5 (CE1(d))]

2.4.3. Shall be changed at least annually. [IA-5 (CE1(d))]

3. MULTI-FACTOR AUTHENTICATION (MFA) REQUIREMENTS

3.1. Application:

3.1.1. All Virtual Private Network (VPN) access shall require MFA utilizing a user-defined password with an assigned hard or soft token. [IA-2 (CE1, CE2)]

3.1.2. Mainframe users will require a hard token for MFA access. [IA-2 (CE2)]

3.1.3. If a user requires a hard token for mainframe access, that same token may also be used to access VPN or other MFA-enabled systems. [IA-2 (CE2)]

3.1.4. Users shall NOT be issued multiple tokens or both a hard token and a soft token for access to the same system(s); however, users may utilize a soft token for access to one system (e.g., network resource) and a hard token to access another system (e.g., mainframe resource) though it is neither necessary nor recommended.

3.1.5. All in-bound connection requests shall be routed through the token authentication server. If the user (requester) has been issued a token they will be required to present the token code for MFA. [IA-2]

3.1.6. At the request of the agency's IT Manager or their designee, contractors and vendors shall be issued temporary (maximum 90-day) tokens. If a longer period of use is required, the token may be renewed. Exception: This requirement need not be applied if the contractor's period of performance is expected to be 1 year or more. [IA-8]

3.2. Token Administration and Registration:

3.2.1. Agencies with workgroup, domain, or organizational unit (OU) administrative personnel, shall designate a Token Administrator who will act as the token registration authority for their organization. For all other organizations, OIT will serve as the token registration authority for IT resources on the OIT-managed network. [IA-5d.]

3.2.2. Agencies shall inform the OIT who their Token Administrator is.

3.2.3. The Token Administrator shall be responsible for managing, inventorying and tracking token assignments. [IA-5d.]

3.2.4. Agency Token Administrators shall submit a request to the OIT Help Desk for initial and additional allotments of tokens for their agency (unless the agency acquires their own tokens).

3.2.5. Agency Token Administrators may return any unassigned tokens or over-allocation of tokens to OIT by contacting the OIT Help Desk and arranging the token transfer back to OIT.

3.2.6. Agency Token Administrators shall utilize the Active Roles administration server to register, activate, and deactivate tokens. [IA-5j.]

3.2.7. The Token Administrator shall validate the token recipient's identity prior to issuing an authentication token to that person. The registration process to receive a token shall (whenever possible) be carried out in person before a designated registration authority authorized by organizational management. [IA-5 (CE3)]

3.2.8. If it is necessary to mail a token (when the token recipient cannot appear in person), the following requirements apply: [IA-5h.]

3.2.8.1. Only non-activated tokens may be mailed.

3.2.8.2. Tokens shall be de-activated before mailing them back to the Agency Token Administrator or to OIT; token-holders shall contact the Agency Token Administrator or the OIT Help Desk for token deactivation before placing the token in the mail.

3.2.8.3. Mail tokens with a confirmation of receipt or some form of delivery acknowledgement.

3.2.9. When e-mailing token activation codes, the activation code shall be set to expire after no more than 1 day. If the token is not activated within the allowed time, the token-holder will need to contact their Agency Token Administrator or the OIT Help Desk for a new activation code.

3.3. Token Safeguard and Use:

3.3.1. Tokens are individually assigned and are authorized for use by the assigned token-holder only. [IA-5f.]

3.3.2. Do not share your token with another person. It is linked to your unique user name (User ID) and password. Reminder: user accounts and passwords must never be shared. [IA-5h.]

3.3.3. Do not leave your token where others can access it. If someone learns your system user ID and password and also has your token, they can log in as you on that system. [IA-5h.]

3.3.4. Tokens are not transferable and until returned are the responsibility of the person to whom issued.

3.3.5. Token Holders shall maintain accountability for their token(s), protecting them from loss, theft, or damage. [IA-5h.]

3.3.6. If a token is lost, the token holder shall immediately notify their Agency Token Administrator, Agency IT Manager or their designee, or the OIT Help Desk.

3.3.7. Token Holders shall notify their Agency Token Administrator, Agency IT Manager or their designee, or the OIT Help Desk of any changes in access requirements (such as when a token is no longer required or needs to be deactivated for any reason).

3.3.8. Token Administrators shall check at least monthly the last logon date for tokens and disable or revoke any tokens that have not been used for more than 60 days. [IA-5d.] [AU-6a.]

3.3.9. Soft Tokens:

3.3.9.1. Soft tokens require a smart phone or similar portable computing device. Users shall identify the device type prior to token issuance to ensure the proper instructions are provided.

3.3.9.2. Smart phones or other devices used to render a soft token shall utilize a device lock or other protection mechanism to prevent unauthorized access.

3.3.9.3. Soft token applications (on smart phones or similar devices) shall be uninstalled prior to device replacement or discontinuance of use or upon changes in employment (transfer, resignation, retirement, termination, etc.).

3.3.9.4. If the token-rendering device is lost, stolen, or in an unusable state, notify the OIT Help Desk or the issuing authority. If possible, mobile device management administrators may perform a remote data wipe to remove or disable a token.

3.3.10. Hard Tokens: Hard Tokens, when no longer required (e.g., change of duties or employment status) or when no longer usable (e.g., battery has drained), shall be returned to the issuing authority.

SUPPORTING DOCUMENTS

The following documents support this standard:

- [Policy 630: Identification and Authentication](#)


EFFECTIVE DATE

This standard is effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

SUPERSEDES

This standard supersedes version 630S1-01.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this standard to be adopted as of the 29th day of January, 2019.



Jim Purcell
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
630S1-01	08/10/2018	Initial version
630S1-02	01/16/2019	Added references, numbering, and service account requirements