IDENTITY AUTOMATION

WHITEPAPER

RapidIdentity Security

RapidIdentity Security

This white paper covers security topics and information, relative to RapidIdentity.

PASSWORDS

ACCESSING PASSWORD CHANGES FROM ACTIVE DIRECTORY

RapidIdentity uses a Microsoft API to capture password pages prior to them being encrypted by the domain controller. For this functionality to work, a custom password filter DLL is 'hooked' into the system running Local Security Authority Subsystem Service (LSASS), through which password changes are processed. This is the same method utilized by Google Apps Password Sync (GAPS) password filter and other available password synchronization solutions.

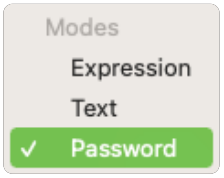
Password changes are protected with 2048-bit RSA Encryption. When password changes are detected by the RapidIdentity password filter, they are encrypted using the RSA algorithm, and stored in the idauto-pwdPrivate attribute on the individual user object. The public key (2048-bit) for this encryption resides on a Domain Controller, allowing RapidIdentity Connect to decrypt the idauto- pwdPrivate attribute value for synchronizing to target systems with the private key stored in the RapidIdentity database.

STORING CHALLENGE QUESTIONS

Challenge questions and responses are stored as values of the idautoChallengeSet attribute on the user. The question types (ADMIN, HELPDESK, USER-DEFINED) and questions are in plaintext. The answers are encrypted using AES 256-bit encryption.

STORING PROPERTIES FLAGGED AS "PASSWORD" TYPE IN RAPIDIDENTITY CONNECT

Within RapidIdentity Connect action sets, certain actions allow for a property to be set as a password field. This property can be selected like most any other field (*shown at right).* When the 'Password' type is chosen, the data is obfuscated from view.



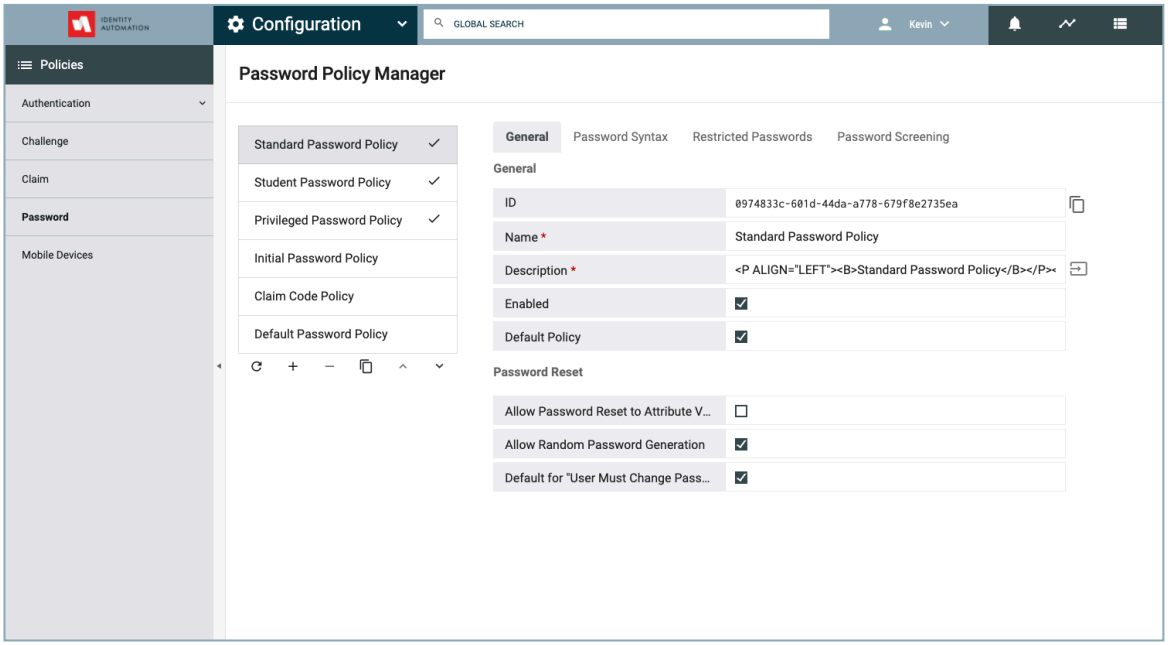
Password: <*Password*>

If an administrator needs to utilize a password for an actionset, best practice is configure the password setting to refer to a global variable that is input (with the encrypt() syntax) in a global properties file, rather than setting the password directly in the action itself. Passwords stored in global properties files are protected with 256-bit AES encryption.

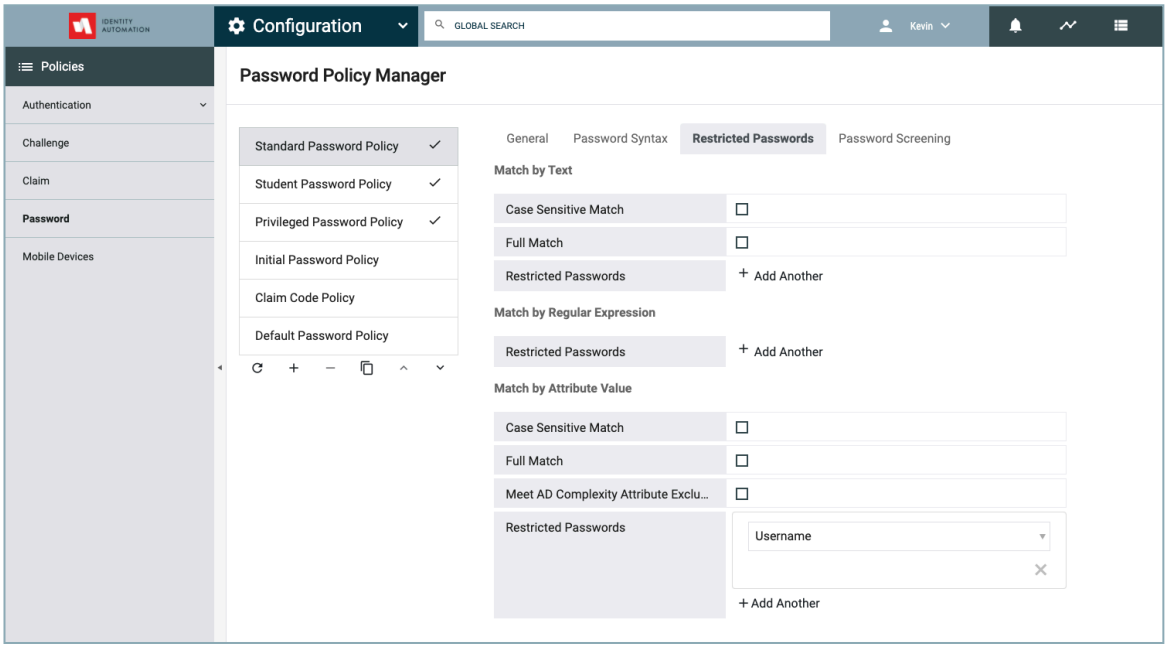
ENFORCE PASSWORD POLICIES PASSWORD STRENGTH, BLACKLISTING, EXPIRATION, & RE-USE

In general, policy complexity can be configured within the Portal configuration. Additionally, further enforcement capabilities can be configured by setting blacklisted passwords (by text, regular expression matching, or matching specific attribute values like sn, givenName, company, etc). In addition to custom blacklisting capabilities for restricting passwords, RapidIdentity Cloud provides automatic Password screening for compromised passwords. This service is provided by Have I Been Pwned and licensed under a Creative Commons Attribution 4.0

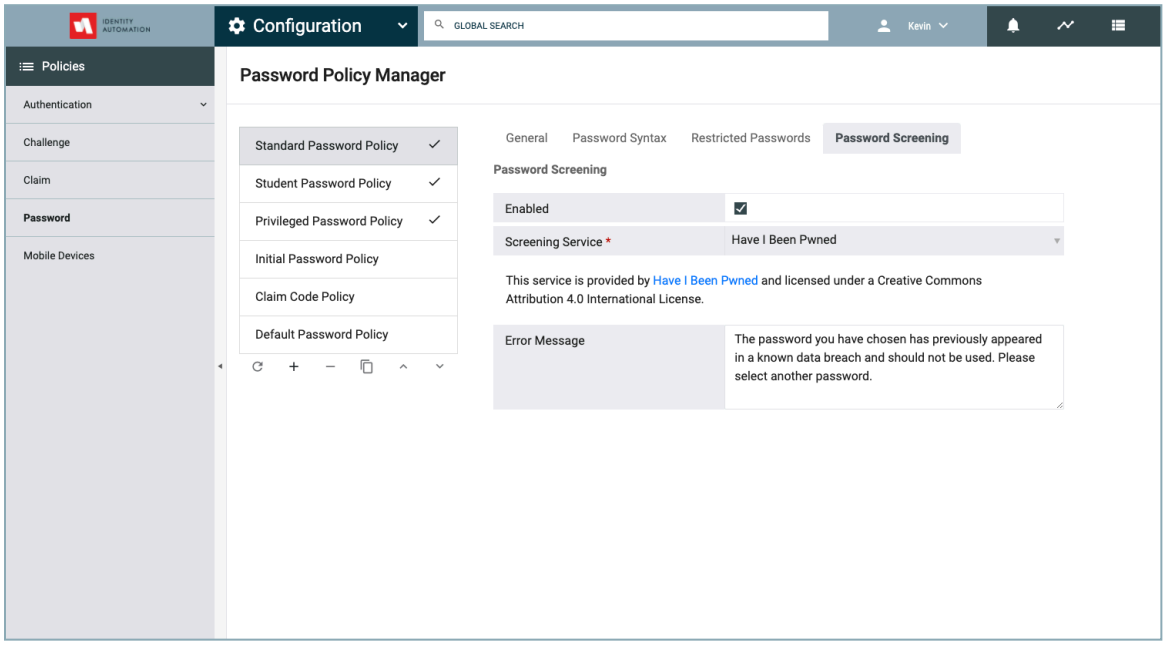
International License. Configuration for Password policy syntax, restrictions, and screening is done via the 'Configuration' button, in the left hand pane of RapidIdentity Portal, 'Policies', 'Password Policy Manager'. With regard to password expiration and re-use, those are managed by the underlying LDAP directory, and any password policies therein.



RapidIdentity allows Administrators to create and manage multiple Password policies through Password Policy Manager.



RapidIdentity allows Administrators to customize complexity requirements and restricted passwords.



RapidIdentity provides Administrators the ability to enable Embedded Password Screening and custom messaging for Complexity requirements.

COMPLIANCE AND SECURITY CERTIFICATIONS

For our RapidIdentity Cloud offering, we work with Amazon Web Services (AWS) to maintain numerous compliance certifications that can be viewed in the Identity Automation Trust Center. For on-premise deployments, the software implementation can be configured to fit within the compliance requirements of the organization.

RapidIdentity Security Statement Addendum

1. PENETRATION TESTING

Identity Automation enlists the use of third parties to perform testing on a periodic basis. Results can be provided on a limited basis upon request. An 'overall' finding will be produced for customers, however, we will not directly provide complete details of any findings, unless / until engineering has had time to review and rectify any issues. Even then, specifics will generally not be provided, as our findings are internal, not publicly disclosed (such as via Mitre or NIST), enabling us to minimize the impact due to early public disclosure, before customers have time to be contacted to address the issues.

2. SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) CONTROLS

At Identity Automation, we employ various controls throughout our development processes to deliver secure and stable software.

Throughout the conceptual, functional, technical requirement and design phases, we ensure that ideas are thoroughly analyzed for usability and security, via group discussion and peer review taking into account current information security industry standards and methodologies.

In coding, our engineering staff performs peer review to ensure security and conformity to standards. Additionally, engineering works with, and involves, our Information Security team for additional resources on any questions that arise regarding findings or processes that might require refinement for vulnerability, compliance and regulatory issues.

Solution testing is performed by Quality Assurance engineers and technical support, to determine any issues; while security-specific testing (vulnerability scanning / penetration testing) is periodically performed by certified third parties in order to find and eliminate security issues both before (design), during (deployment), and after (maintenance) phases of the release cycle.

During software implementations, or as questions arise, the support, engineering and information security teams discuss any additional security needs, such as backup, access control, encryption of data, etc, that are relevant to our specific customer environment.

Identity Automation has a bug tracking system in place, whereby our bugs are entered, reviewed and remediated, and go through a workflow process whereby testing and validation occur before fixes, patches or upgrades are released.

Finally, Identity Automation uses strict version control, and does internal development

nightly builds that are committed on a consistent basis, to give our teams adequate time to test and validate all changes.

3. INTEGRATION WITH SPLUNK AND OTHER SEIM SYSTEMS

Direct Splunk or Security Information and Event Management (SEIM) specific usage information is outside the area of focus for Identity Automation as a company. However, identity events that occur with RapidIdentity Portal can be sent to any syslog device, as well as to our database; and syslog can be integrated into Splunk just as any other syslog data can be, for analysis. Additionally, RapidIdentity Connect actions provide the ability to customize what data our actions send to our audit log database and other syslog/event logging systems. Configuration for syslog can be found within configuration, 'Audit Logging'-'Audit Types". Further Splunk-specific information pertaining to Syslog can be found in their documentation at http://docs.splunk.com/Documentation/Splunk/6.2.2/Data/SysgTCP

4. INFORMATION THAT IS LOGGED

Most event types, actions, and other data, including perpetrator, target, IP address, time stamp, and other action specific details can be logged directly to the audit database. Additionally, using RapidIdentity Connect, data of any type can be sent to various systems such as databases, SEIM solutions, event logs, text files, email, etc.

5. LOGSTASH

Audit logging can also be configured to audit to file (as with database and syslog). When the audit file is being utilized, Logstash and Kibana can be used for fast indexing and searching of centralized audit data. Information regarding basic configuration can be found in our documentation at: https://ri-doc-lts-html5.identitymgmt.net/en/logs.html

6. MFA CONTROLS FOR PRIVILEGED ACCOUNTS

Multi-factor authentication can be enabled based on any number of Authentication Policies, configured through the RapidIdentity Appliance interface. This option can be found under 'Home' - 'Edit Core Configuration' - 'Authentication Policies'. The policies may be applied based on LDAP filter (such that any valid search filter that yields administrative or privileged accounts can be selected), as well as providing configurable options for 'Time of Day', 'Day of Week', 'Source Network' and whether or not the browser is expected to present a Kerberos token. Supported authentication methods include Password, TOTP, SMS OTP, Kerberos, Biometrics (via mobile push), challenge response and social (Facebook, Twitter, LinkedIn).

7. RAPIDIDENTITY CLOUD

a. Identity Automation supports privately hosted solutions and offers multi-tenant as a service solutions utilizing Amazon Web Services.

b. **SEGREGATION OF TRAFFIC BETWEEN CUSTOMERS**

Customer data (and virtual environments) are completely segregated in our private RapidIdentity Cloud deployments through containerized encryption standards. Additionally, RapidIdentity databases reside on Relational Database Service instances, connected directly to their specific customer tenant. As such, each customer environment is separated from others. Additionally, Identity Automation provides a RapidIdentity Bridge service with the RapidIdentity Cloud tenant that provides a highly avail-

able endpoint for customers on-premises resources to communicate with securely. RapidIdentity Bridge replaces the need for a VPN between cloud, and on-premises resources.

The only external (outbound) access required for RapidIdentity Bridge to function securely is port 443 from the on-premises endpoint to the RapidIdentity Cloud. The only external facing components of RapidIdentity Cloud, beyond the Bridge endpoint, are the public facing web services for the RapidIdentity Portal and RapidIdentity Federation appliances, to allow third-party SAML integrations and off-site user access to the portal.

c. **ENCRYPTION FOR PRIVACY PROTECTION**

Data transmission (end user-to-appliance, appliance-to-appliance, appliance-to-remote systems) encryption is dependent upon the systems in use. The web interfaces to the appliances are secured via HTTPS (SSL) encryption, and the majority of traffic passed between any of the appliances (integrated cross-appliance functionality) occurs over the HTTPS as well. Other data transmission encryption (for instance between RapidConnect and connected systems) is dependent upon the security allowed and provided by those systems. RapidIdentity supports the following security protocols: FTPS, SSH, LDAPS and HTTPS.

d. **PREVENTION OF TAMPERING BY CLOUD SERVICE PROVIDERS**

Amazon maintains the ability to shutdown or deny access to services, should they find evidence of a security issue (they've been known to lockdown ACL's and/or disable hosts). If they find a security misconfiguration that causes problems; for example, if a host on their networks is participating in a Distributed Denial of Service (DDoS) attack, all access on the appliances is restricted to the VPC and any allowed Security group permissions -- while authentication to the appliances (local SSH for Linux or obtaining the Administrator password for Windows) requires Private keys.

e. **SLA CONTRACT AND UPTIME FOR RAPIDIDENTITY CLOUD CUSTOMERS**

In partnership with AWS, RapidIdentity Cloud adheres to a 99.9% uptime standard. The RapidIdentity Cloud product design and hosting options allow us to provide that standard, and we support high availability through the use of elastic computing, elastic load balancing, and other mechanisms within the AWS product offering. The terms and conditions for defining SLAs are customer-specific, and subject to contractual agreement.

For more information about AWS's SLAs, please visit: https://aws.amazon.com/ec2/sla/

f. **3RD PARTY ATTESTATIONS OR SECURITY CERTIFICATIONS (SOC 1/SSAE-16, SOC2, ISO,)**

RapidIdentity Cloud holds numerous certifications around data privacy that can be viewed in the RapidIdentity Cloud Reference Architecture: https://www.identityautomation.com/resources/rapididentity-cloud-reference-architecture/

8. DATA STORAGE AND TRANSFER

Aside from any audit data and job logs, the vast majority of data is stored only on the remote systems for which is intended. Audit logs are stored in a secured database, and job logs are stored in a compressed format on the RapidIdentity Connect appliance (or configured remote filestore, if clustered, etc), and are accessible (via appliance inter-

face) only to users who are granted RapidIdentity Connect administrator role(s). If stored on a remote file system, access permissions on that files system apply (e.g. stored on SMB share, Windows filesystem permissions apply to users of that storage server).

9. SECURITY CONTROLS OF SDLC

a. **Documentation of encryption strategy**
RapidIdentity uses the RSA algorithm to encrypt passwords when necessary. TLS 256-bit AES encryption is also used for storing sensitive items in the configuration database.

b. **Describe controls used to prevent cross-site scripting, SQL injection, etc.**
RapidIdentity uses the Hibernate platform for database access which has built in sql injection prevention, meaning we never construct SQL statements with string oncatenation. ESAPI for XSS is used for additional protection— escaping values used in javascript.

10. CUSTOMER TESTING OF THE UI USING NON-DESTRUCTIVE TECHNIQUES FOR VULNERABILITIES

a. **Access to admin console as privileged user**
As our appliances are considered 'managed', we do not provide the ability for customers to authenticate to the appliances with a privileged user (root) account. This is also to prevent the installation of 3rd party agents that can introduce vulnerabilities into the system.

For appliances within a local customer environment (non-SaaS / non-hosted), we discourage aggressive vulnerability testing without first contacting Identity Automation. Some operations of vulnerability scanners, when not directly applicable to a service, are known to overwhelm communications layers and cause a 'Denial of Service', etc, and could negatively impact proper daily operations of the appliances. Typically, these activities would not directly talk to our services, but as scans are usually done from within the local network, sometimes, they unnecssarily raise red flags; which could be avoided with proper pre-planning of a scan. As such, it is recommended that vulnerability scanning should be performed against development or test environments, only.

With regard to RapidIdentity Cloud customers (AWS), the customer is NOT permitted, in any way, to perform vulnerability scanning or penetration testing against our appliances. These activities are specifically restricted by AWS, and require us to schedule specific timeframes and get express permission in order to even test our own appliances, as well as still imposing limitations to prevent impact to the overall environment. Therefore, we do not allow customers to perform these activities against hosted servers.

b. **Load tests**
Load tests are discouraged against production environments, as they may cause an impact to the operation of the appliances or integrated systems.

c. **Reporting Security Vulnerabilities**
Vulnerability reporting should be done via contact with the Support Team at Identity Automation (support@idauto.net or 281-220-0021 option 4), who will engage the Information Security Team, as necessary, for analysis and review.

IDENTITY AUTOMATION

Identity Automation provides identity and access management (IAM) solutions for K-12 and higher education. Its flagship platform, RapidIdentity, safeguards learning environments, maximizes instructional time, and minimizes the load on Information and Instructional Technology teams. Technology leaders turn to RapidIdentity for its best-in-class security capabilities, time-saving automations, and flexible approach to managing digital identities. Headquartered in Houston, Texas, Identity Automation is trusted by Chicago Public Schools, Public Schools of North Carolina, University of Rochester, Houston Community College, and hundreds of other institutions. To learn more about partnering with Identity Automation, visit www.identityautomation.com.

RapidIdentity is the digital identity platform for education. Available on-premise or in the cloud with no sacrifices in functionality, features, or security, RapidIdentity offers:

- Identity Lifecycle Management- automates the full identity lifecycle of all users
- Authentication (MFA & SSO)- enables seamless user access, while protecting all entry points
- Rostering for K-12- automates integration and synchronization of student data with target applications
- Identity Governance- ensures proper identity and access controls are maintained and updated

IDENTITY AUTOMATION

+1 281.330.0021

Corporate Headquarters | 7102 N. Sam Houston Parkway, Suite 300 Houston, Texas 77064

www.identityautomation.com