Security for Integrating with Other Systems - Best Practices

https://campus.barracuda.com/doc/91980494/

Barracuda recommends creating dedicated service accounts when integrating Barracuda products with external systems and services – such as LDAP servers, backup servers, or your email server. Then, give these accounts the least amount of privileges possible. Avoid using personal credentials for integration points – especially if you are a domain administrator or other privileged user. Along with minimizing the impact in the event of exposure of the credentials, using a service account eliminates the likelihood of the integration's breaking when you change your password.

Service Accounts with Minimal Privileges

When integrating Barracuda products with other systems, remember these two key points:

- **Use service accounts rather than personal user accounts.**
  Create special accounts for integration points, rather than using your personal account. If you are an administrator and you provide your personal credentials, an attacker who gains access to the credentials could use them throughout your environment. A service account created for the purpose of integration with a Barracuda appliance should not be useful for any other purpose.
- **Assign these service accounts the minimum permissions required.**
  Follow the *principle of least privilege* and use the absolute minimum credentials needed to get the job done. For example, determine whether a certain integration requires both read and write privileges or just reading privileges. Use the minimum required permissions for any integration. This guideline pertains to all integrations within your environment, not just Barracuda products. In general, use permissions sparingly to increase your security.

Part of an Overall Security Policy

Service Account Inventory

You should have a formal account management process that tracks accounts in use. The tracking mechanism simplifies the process of rotating credentials and providing access to other employees. The tracking process should include the following properties:

- Active?
- Service Account Email
- Where Used
- Integration Point
- Account Permissions

- Creation Date

Password Management Policy

Your entire organization benefits from having a secure password management policy. Service accounts you create for integration points should also follow your password management policy.

A password management policy should include things like:

- Choose strong passwords. Refer to the Password Complexity Policies for Barracuda Cloud Control.
- Do not reuse passwords.
- Do not use the same password for an integration point that you use to log into the main system.
- Follow best practices for password security. You can find many of these online.

Multi-Factor Authentication and Integration Points

Multi-Factor Authentication, or MFA, increases security by requiring both a password and something the user possesses, like a security token. This is not, however, an option with integration points. MFA requires human interaction and one of the purposes of an integration point is to remove the need for a human touch. Your service accounts for integration points do not have the added security of MFA, so limit what those credentials can access.

Rotating Credentials

Rotating credentials improves security by limiting the length of time that a lost credential is valid. It protects against an undetected exposure or loss of those credentials. When a user leaves your organization, rotating credentials ensures that they can no longer access system using that account. Have a plan for rotating credentials within your various products and integration points.