Application / Source Onboarding Questionnaire

This questionnaire is designed to collect information that will determine how your source is connected for activities through IdentityNow.  Your answers will provide mission-critical information to empower your governance, risk, and compliance activities through the application.

Ideally, the following personnel in your organization should answer this questionnaire:

* Application Owner
* IT Custodian
* Audit Process Owner

This questionnaire should be answered in a collaborative fashion, as key pieces of the information may not be available to everyone. SailPoint suggests that each of the parties listed above work together to complete this document to enable a determination of how best to connect to and gather the information to derive the results you seek from IdentityNow.

**General**

This section deals with the general information required for each source being integrated into IdentityNow.

1. Please provide a brief description of the application and the types of users using the application. *e.g. Contractors, Temps, Employees, IT, HR, Finance, etc.*
2. Please provide the Application Owners' names and contact information so that we may contact them if questions arise during the onboarding process for the application.
3. Who in IT provides services to your application? Please provide us their name and contact information so that we may contact them if questions arise during the onboarding process for the application.

Application / Source Data

SailPoint will need to understand the application(s) being integrated into IdentityNow.  Your results with IdentityNow will be determined based on your input, as the data you require will be modeled based upon your answers to this questionnaire.

1. Can you provide a rough estimate of how many user accounts the application contains?
2. Where is the data for this application stored?  
   e.g. LDAP, database, Active Directory, etc.
3. Are there any technical interfaces, APIs, etc. which can be used to access application data in a supported way?
4. If there are no technical interfaces to provide this data, can a file be extracted in our generic file format?
5. What attribute is currently in use to uniquely identify each account? e.g. username, global user ID (GUID) or a distinguished name (DN)
6. Is there an attribute that ties (correlates) each account to the corporate directory or another authoritative data source? e.g. username matches email address
7. Which attributes in the application define the entitlements, access rights, groups, or permissions?  What is the authorization model for the application?
8. What different types of accounts exist in the system (System accounts, Disabled users, etc.) and how are they identified?

Password Change / Reset

The following section deals with the password reset processes within your organization. After considering your existing password reset processes and how you intend to improve those processes with IdentityNow, please answer the following questions:

1. What is the current password change/reset process for this application today?  How could it be improved?
2. Where and how are password changes and resets initiated from today?
3. Is this password change dependent alongside password resets to other applications or other data sources?  If so, please describe the password management flow and any dependencies.
4. Describe the current password policy for this application.

Provisioning

The following section deals with the provisioning and account setup processes within your organization. After considering your existing provisioning processes and how you intend to improve those processes with IdentityNow, please answer the following questions:

1. What is the current provisioning process to set up user accounts for this application today?
2. What is the current deprovisioning process to remove user accounts for this application today?
3. Who performs the account administration, user provisioning, and deprovisioning for this application?

e.g. Help Desk personnel, Security Operations administrators, IdentityIQ, other automated provisioning solutions, etc.

1. Describe any sort of provisioning logic needed to determine attribute values for different operations.

i.e. create, modify, delete, lock, unlock, enable, disable

1. To your knowledge, does this application offer any sort of API or technical interfaces to perform automated provisioning?  If so, what access rights are needed?

Access Review / Certification

The following section deals with the compliance certification processes within your organization. After considering your existing access review/certification processes and how you intend to improve those processes with IdentityNow, please answer the following questions:

1. How do you currently review users’ access to applications today and where do you obtain their access data from?
2. What is the level of granularity required for the certification process? Are they based solely on permissions (read, write, execute etc. on target), accounts, entitlements, or a combination thereof? What are the parameters you use to determine access certification?
3. What type of access review or certification process do you currently have in place? e.g. manager access review/certification, etc.
4. Could you provide a high-level description of the current process used to recertify access for the different types of users of this application?
5. How often do you perform access reviews/certifications?

Additional Application Detail

In order to ensure that we have all of the relevant details for your project is there anything we have missed asking you that would provide a successful deployment for IdentityNow? If so, please use this page for any additional information that may be relevant to the data aggregation, correlation, single sign-on, password management, or certification processes.