Password Management

Version: 8.2

Revised: June 2021

Copyright and Trademark Notices

Copyright © 2021 SailPoint Technologies, Inc. All Rights Reserved.

Contents

Introduction to Password Management **1**

Application Password Management **2**

Enabling Password Management in IdentityIQ 2

Business Process for Password Management 2

Optional Configuration Settings for Managing Passwords 3

Determining Who Can Manage Passwords 3

Defining Special Characters Available For Password Use 3

Configuring Password Policies for an Application 4

Configuring Applications for Password Management 4

Defining a Password Policy 4

Password Dictionary 6

Policy Re-Use 6

Password Validation Process 7

Application Change Password Provisioning Policy 7

Requesting a Password Change 7

Self-Service Requests 7

Requests for Others 8

LCM Manage Passwords Workflow 9

Passwords on New Account Requests 10

Troubleshooting Password Management with Provisioning Plan Debugging 10

IdentityIQ Password Management **12**

IdentityIQ Password Configuration 12

IdentityIQ Password Policy 12

Defining Special Characters Available For Password Use 13

Resetting IdentityIQ Internal Passwords 14

Self-Service Password Reset 14

Password Resets for Others 14

Password Expiration Resets 15
Password Management with Pass-Through Authentication 15
Defining the Security Questions 16
Configuring the Security Question Settings 16
Security Questions Tab 16
Recording Security Answers 16
Requiring Security Answers 16
Independently Providing or Editing Security Answers 17
Application-Specific Password Management Requirements 18
Active Directory and ADAM: SSL 18
SSL Configuration for the Direct Connector 18
Windows Local and Active Directory: IQService Agent 19
Windows Desktop Password Reset Utility 19

Introduction to Password Management

IdentityIQ supports multiple login configurations, including single sign-on, pass-through authentication, and validation against IdentityIQ's internally stored passwords. Pass-through authentication and internal passwords can be managed through the IdentityIQ user interface.

IdentityIQ's internal set of passwords are governed by the IdentityIQ password policy. These internal passwords are always available as a fallback login validation for IdentityIQ, even when other authentication methods are used; either the user or an administrator can reset an internal password through IdentityIQ's change password options.

When pass-through authentication is used, IdentityIQ enables the specification of challenge questions that can enable users to reset their own forgotten passwords, once they authenticate to IdentityIQ by correctly answering those questions. New passwords entered through this forgot password feature are validated against the pass-through authentication application's password policy and are reset on that application directly.

This section includes:

- Application Password Management
- IdentityIQ Password Management
- Application-Specific Password Management Requirements

Application Password Management

IdentityIQ can use the Lifecycle Manager product to manage passwords across many of the applications with which it is associated. It can enforce password policies specified for the applications, which can include requirements for length, complexity, unique history, and mandatory reset.

To manage passwords across application, you must configure both IdentityIQ and the applications on which you are going to manage passwords. Password management is further governed by the capabilities of the connector in use for each application and some applications have specific configurations requirements that go beyond the basic password management requirements.

This section contains:

- Enabling Password Management in IdentityIQ
- Configuring Password Policies for an Application
- Configuring Applications for Password Management
- Application Change Password Provisioning Policy
- Requesting a Password Change
- Passwords on New Account Requests
- Troubleshooting Password Management with Provisioning Plan Debugging

Enabling Password Management in IdentityIQ

The ability to manage passwords in other applications through IdentityIQ is controlled by a combination of settings:

- a business process that manages provisioning of password changes and password resets for application passwords
- some optional configuration settings that refine the behavior of your organization's password management processes
- Quicklink Populations that determine who can manage passwords, and which other users they can manage passwords for

Business Process for Password Management

IdentityIQ provides a standard business process (workflow) for password management: LCM Manage Passwords. You can substitute a custom workflow of your own if your business needs require it.

To set the workflow for password management:

1. Click **gear > Lifecycle Manager**.
2. Click the **Business Processes** tab.
3. In the **Manage Passwords** field, select the business process to use for password management.
4. **Save** your changes.

For more information about this business processes, see LCM Manage Passwords Workflow.

Optional Configuration Settings for Managing Passwords

In the Lifecycle Manager configuration, you can also set options for managing the auto-generation of passwords when requesting them for others, and password validation rules.

1. Click **gear > Lifecycle Manager.**
2. Click the **Configure** tab.
3. To enable auto-generation of passwords, check the **Enable password auto-generation when requesting for others** option.
4. To specify a rule to use for validating passwords, choose a rule from the **Password Validation Rule** drop-down. The validation rule is used in forms generated from provisioning policies during account creation.
5. **Save** your changes.

Determining Who Can Manage Passwords

Quicklink Populations control which populations of users can change account passwords for themselves or others. This is done by enabling and configuring the Manage Passwords Quicklink for a population.

1. Click **gear > Global Settings > Quicklink Populations**.
2. Choose a population to configure. You can also use the **New** button to create a new population. See the **System Configuration** documentation for more information on creating Quicklink Populations.
3. On the **Quicklinks** tab for the population, check the **Manage Passwords** option.
4. To determine who members of this population can manage passwords for, click the **Configure** link on the line for **Manage Passwords**.
    - Choose **For Self** to restrict these users to managing only their own passwords.
    - Choose **For Others** if these users can manage passwords for themselves and for others, and select the **Single** option if you want to limit these users to managing passwords for one user at a time. The “others” these users can manage are determined by the **Who can members request for?** section on the Quicklinks **Configuration** tab.. See the **System Configuration** documentation for more information.
5. 5. **Save** your changes.

By default, IdentityIQ provides some standard populations that are able to manage passwords. You can modify this according to your business needs.

- The **Self Service** population is, by default, allowed to manage passwords for themselves only.
- The **Help Desk** and **Manager** populations are, by default, allowed to manage passwords for themselves and for others.

See also:

Defining Special Characters Available For Password Use

Defining Special Characters Available For Password Use

IdentityIQ enables you to define the special characters that can be used in passwords throughout your deployment of the product. A default set of special characters are included in the System Configuration object.

The special characters enabled for use in passwords are listed in the passwordSpecialCharacters key. To edit these items:

- Click the **Gear** icon in the navigation menu, go to the **Global Settings -> IdentityIQ Configuration -> Password tab -> Password Policy** area, and click **Define Character Type**.
  Or
- Go to the debug page of the IdentityIQ user interface and select object type Configuration from the drop-down menu. Select the SystemConfiguration object and edit the value for the passwordSpecialCharacters entry key. For example:

```
<entry key="passwordSpecialCharacters" value="~!@#$%^*_+-={}\\][:;?,."/>
```

Configuring Password Policies for an Application

Password policies specify the password requirements for an application. These can include minimum and maximum lengths for the password and requirements for its makeup, for example number of letters, digits, uppercase letters, lowercase letters, and special characters. The policies can also restrict password choice based on matches in password history, the password dictionary, the Identity's list of attributes, and the Identity's account attributes.

A separate password policy can be defined for each application in IdentityIQ. In fact, multiple policies can be defined for each application.

Configuring Applications for Password Management

Password management is further governed by the capabilities of the connector in use for each application. Passwords can be managed through IdentityIQ for any application using a read-write connector that has the PASSWORD feature enabled; this feature is enabled when the features String attribute on the application contain the word “PASSWORD”. The application definition, including its featuresString attribute, for each application is viewable in the XML representation of the Application object accessible from the debug pages or from the IdentityIQ console.

```
<Application connector=”sailpoint.connector.LDAPConnector” created=”1334252935835”
featuresString=”AUTHENTICATE, PROVISIONING, ENABLE, PASSWORD, MANAGER_LOOKUP, SEARCH, ACCOUNT_
ONLY_REQUEST" id="4028833636890f860136a7ac1a6c054f" modified="1335456303423" name="ADAM Direct"
profileClass=”“ type=”ADAM - Direct">
```

> Not all read-write connectors have the PASSWORD feature enabled. The Connector Registry entry for each connector includes all the valid features for that connector in its featuresString attribute. Specifying PASSWORD in the featuresString of an application to which the feature does not apply does not successfully enable password management for the application. To view the Connector Registry entries from the debug pages, select Configuration from the Objects list and click List. Then click ConnectorRegistry to view the connector registry XML.

See:

- Defining a Password Policy
- Policy Re-Use
- Password Validation Process

Defining a Password Policy

Complete these steps to define an application's password policy:

1. Open the application definition. From the navigation menu, go to **Applications -> Application Definition ->** select application from list or click **Add New Application** to create a new application.
2. Open the **Password Policy** tab.
3. Click **Create New Policy** to create a new password policy, click a policy name in the list to edit an existing policy, or click **Add Existing Policy** to select a predefined password policy from the drop-down list, see Policy Re-Use.
4. Name the policy (required) and provide a brief description. Specify any required password characteristics. Most of these characteristics are self-explanatory.

   These few are further explained here since they might be unclear:
   - **Password history length:** specifies number of previous passwords in password history to check against for uniqueness (prevents re-use of a password over the specified number of password changes); the current password is included in the count
   - **Validate passwords against the password dictionary**: compares password to an internally-stored, implementation-specific password dictionary, ensuring that the password is not, and does not contain, any word in that dictionary (see Password Dictionary below)
   - **Validate the password against the identities list of attributes**: ensures that values stored as Identity attributes (for example, last name, department, office number, region) are not used as the password
   - **Validate the password against the identity's account attributes**: prevents values stored on the application account from being used as the password

> The password history, if a Password history length value is specified, it is stored as a <PasswordHistory> element on the <Link> (account representation) within the Identity object. It is stored as a comma separated values list of encrypted passwords. The number of passwords stored is determined by the Password history length value specified. New passwords set for the account cannot match any password in the list.

5. Select an **Identity Filter** if this policy should only apply to certain sets of Identities. The default Identity filter is All, which means the policy applies to all Identities. Other options are:
   - **Match List**: specify Identity Attributes or Application Attributes/Permissions by which Identities can be matched for this policy to apply (for example, Identity Attribute: Department = Accounting)
   - **Filter**: specify a filter (as CompoundFilter XML) that can be used to identify Identities to which this policy applies
   - **Script**: specify a segment of beanshell that selects Identities that should use this policy
   - **Rule**: specify a rule (type: IdentitySelector) that returns a list of Identities to which this policy should apply
   - **Population**: apply this filter to the Identities in an existing IdentityIQ Population

> The first policy defined should be the default policy that applies to all users. This policy serves as the "fallback" policy if none of the more restrictive policy Identity Filters apply to the Identity whose password is being validated. If more than one policy is specified with Identity Filter = All, only the last one created is applied in any Identity password validation. This is further explained in the Password Validation Process section.

See, Password Dictionary

Password Dictionary

The password dictionary is a set of words (or character strings) that have been deemed impermissible as passwords or password contents for the specific IdentityIQ installation. It is populated by importing a Dictionary XML object through the iiq console or the Import from File option under System Setup. The XML looks like this, and the prohibited words in the password dictionary are included as <DictionaryTerm> elements:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE sailpoint PUBLIC "sailpoint.dtd" "sailpoint.dtd">

 <sailpoint>
    <ImportAction name='merge'>
      <Dictionary name="PasswordDictionary">
       <Terms>
         <DictionaryTerm value="password"/>
         <DictionaryTerm value="identity"/>
       </Terms>
      </Dictionary>
    </ImportAction>
 </sailpoint>
```

Include the <ImportAction name='merge'> element to add new terms to the dictionary without overwriting the existing dictionary entries. Omit this element to overwrite the dictionary with a new set of terms.

If removing terms or replacing the entire dictionary, then delete the dictionary object first using the console or debug pages. The terminator will handle removing both the Dictionary and the dictionaryTerms.

> Terms included in this dictionary are prohibited even as any part of a password when password dictionary validation is enforced. For example, if the term “rock” were included in the password dictionary, these passwords would all be prohibited: rocketlauncher, sprocket, Sh@mrock125. Additionally, validation against the password dictionary is case insensitive, so RocKeTTe would also be prohibited in this case.

Policy Re-Use

Previously created policies (for example, ones created for one application but applicable to more than one application) can be added to an application instead of recreating the same policy over and over. For example, if super-user accounts on all applications have the same password requirements, the super-user policy could be created once and copied to all applications.

To copy an existing policy from one application to another:

1. On the **Password Policy** tab for the target application, click **Add Existing Policy.**
2. Select the desired password policy by name. The password policy characteristics are displayed for review.
3. Configure the **Identity Filter** to apply the policy to the appropriate set of Identities for this application. Filters might differ from one application to another (for example, different application attributes or permissions or different Identities attributes can designate a super-user on one application but not on another), so they do not carry over between applications in this policy sharing feature.
4. Click **Save** to save the filter on this application.

The policy now appears in the application's **Password Policies** list with a warning icon. Hovering over this icon displays the message “Be careful editing this policy, it is also used by another application.” Changes made to the requirements in a shared policy affect all applications using that policy. Changes made to the Identity Filter on these shared policies only affect the individual application's use of the policy.

Password Validation Process

In many cases, the password policy for an application applies to all users, so there is only one password policy per application. Sometimes, more than one policy is created for a single application to specify different password requirements for different levels or types of user access. In the password management process, when a user's password is being changed, the policy checker scans all of the policies that apply to the identity and creates one super-policy that covers all of the restrictions for that user.

If no password policy is defined for the application, no password policy is enforced and any password entered for a password change is accepted by IdentityIQ and passed to the application to be set as the account's new password.

Application Change Password Provisioning Policy

Some applications support more than one password type. For example, Lotus Notes has three different types of passwords that need to be managed, a vault password, a file password, and an internet password. IdentityIQ can be used to configure those applications so that all password types can be managed through a change password provisioning policy.

The change password provisioning policy template is loaded when a change password request is created through Lifecycle Manager. This template is only loaded for change password. The other password management requests are not affected.

The Change Password provision policy is configured on the Provisioning Policy tab of the Application Configuration page.

Requesting a Password Change

Password changes, self-service or for others, are requested through the Manage Access QuickLink for Lifecycle Manager. When the request is submitted, it is immediately processed through a workflow, by default, the LCM Manage Passwords workflow.

By default, application password requests (forgot, expired, or change), either self-service or for others, invoke the LCM Manage Passwords workflow. This workflow's default configuration requires no application-owner or manager approvals on a password change. It creates and processes a provisioning plan that contains the requested password changes and then notifies the user by email when the change is complete.

If the change request is for an account whose application is configured with a Change Password provisioning policy, additional information is required before the change occurs. See Application Change Password Provisioning Policy.

See:

- Self-Service Requests
- Requests for Others
- LCM Manage Passwords Workflow

Self-Service Requests

When a user wants to, and is authorized to, change their own password on an application, they must complete these steps in IdentityIQ:

1. From the **Manage Access Quicklink**, click **Change Passwords** and select **For Me**.
2. Select the application account or accounts for which the password is being changed.

> Hover over the help text icon () by the application name to review its password policy requirements.

3. Enter the **Current Password** for each account being updated. Enter the new password twice: once in **New Password** and once in **Confirm Password**.

If more than one application's password is being changed at a time and the new passwords should all be identical, select **Synchronize passwords for selected accounts**. Each of the selected accounts is then prompt for the **Current Password** for that account but the New Password and **Confirm Password** boxes are displayed only once at the top of the window and apply to all applications whose passwords are being changed.

4. Click **Submit** at the bottom of the window to submit all password changes.

> If the entered passwords do not match or if the password does not meet the requirements of all of the application's password policies, an error message is displayed on this window and the password values must be re-entered before the requested changes are successfully submitted.

5. A summary of the requested changes is displayed on the next window. Review this summary and click **Submit** (or click **Cancel** or **Make Additional Changes** if the changes noted in the summary do not match the desired changes). Individual request line items can be deleted from this window by clicking the **x** icon on any row. Comments can be added to any of the change records by clicking the icon in the **Add Comments** column. These comments are stored on the IdentityRequest object, which can be accessed later through the **My Work** > **Access Requests** menu option.

> The password reset only occurs if all requested changes can be made successfully. If the password reset fails, an error message is displayed at the top of the page indicating the failure.

Requests for Others

As described in Enabling Password Management in IdentityIQ, the sets of Identities for which a user can make requests, as well as the types of requests available to each user, depend on the Lifecycle Manager Configuration settings that apply to that Identity. The rest of this section assumes that the logged-in user is authorized to make password requests for the Identity needing a password change.

Complete these steps to reset another user's password on an external application through IdentityIQ:

1. From the **Manage Access Quicklink**, click **Change Passwords** and select **For Others**.
2. Select the Identity for whom the password change is required.
3. Specify the password change method:
    - **Set passwords for the selected accounts**: enter new passwords manually on this window
    - **Synchronize passwords for selected accounts**: apply a single manually entered password to all of the selected accounts (rather than entering a separate new password for each selected account)
    - **Generate passwords for the selected accounts**: allow system to generate new passwords

When passwords are reset for another user, the system automatically sets a flag that tells the external application to require a password reset upon initial login by the user, so whether the password is manually set or generated, the user is prompted to change it when they first sign in to the target application.

The Generate passwords for the selected accounts option can be turned on or off from the Lifecycle Manager Configuration window, Additional Options tab. Select or clear the Enable password auto-generation when requesting for others box in the Manage Password Options section.

4. Select the application account or accounts for which the password is being changed.
5. Enter the new password twice - once in **New Password** and once in **Confirm Password** - if prompted.
    - If **Generate passwords for the selected accounts** is selected, the system does not prompt for a new password.
    - If **Synchronize passwords for the selected accounts** is selected, the password prompting occurs one time at the top of the window above the accounts list.
    - Otherwise, each selected application account has a set of password prompt boxes.
6. Click **Submit** at the bottom of the window to submit all password changes.

If the entered passwords do not match or if the password does not meet the requirements of the application's password policy, an error message is displayed on this window and the password values must be reentered before the requested changes can be successfully be submitted.

7. A summary of the requested changes is displayed on the next window. If the password is a generated password, the password is displayed in the **Password** column. If it was manually entered, it is represented with ***** in that column. Review this summary and click **Submit** (or click **Cancel** or **Make Additional Changes** if the changes noted in the summary do not match the desired changes). Individual line items can be deleted from this window by clicking the icon on any row. Comments can be added to any of the change records by clicking the icon in the **Add Comments** column. These comments are stored on the IdentityRequest object, which can be accessed later through the access request pages.

The password reset only occurs if all requested changes can be made successfully. If the password reset fails, an error message is displayed at the top of the page indicating the failure.

LCM Manage Passwords Workflow

By default, application password requests (forgot, expired, or change), either self-service or for others, invoke the LCM Manage Passwords workflow. This workflow's default configuration requires no application-owner or manager approvals on a password change. It creates and processes a provisioning plan that contains the requested password changes and then notifies the user by email when the change is complete.

If the change request is for an account whose application is configured with a Change Password provisioning policy, additional information is required before the change occurs.

The default email template for password change notification sends a summary of the change request. This includes the requester, some representation of the new password, and any comments entered on the request (from the **Summary of Requests** window). If the password was system generated, that password is included in the email body. If it

was a manually entered password, it is displayed in the email body as ******; in the case of request-for-others password resets, the new password value must be verbally, or otherwise, communicated to the user by the person who made the change.

To direct IdentityIQ to use a different, custom workflow for password management, create a workflow of type LCMProvisioning and select it as the Manage Passwords business process on the **Lifecycle Manager Configuration** window's **Business Processes** tab.

Passwords on New Account Requests

New account requests often contain password values. If you want to use default account-creation passwords that are different from the standard password policy for that application, IdentityIQ uses a configuration setting to govern the enforcement of password policies on account creation.

To enforce password policies on account creation, complete these steps:

- On the **Lifecycle Manager Configuration** page located under the gear icon menu, **Additional Options** tab, select the Check Password Policy rule as the **Password Validation Rule**. Check Password Policy is a rule that is supplied with Lifecycle Manager that validates the password field on an application's provisioning policy against the application's password policy. To write a custom rule, click the button to the right of that box.
- Define a Create provisioning policy for the application that includes a **password** field. This field name must end with password, must be of type **Secret**, and must not have its own validation rule specified for the Password Validation Rule to be applied. The connector maps this password provisioning policy field to the application's password field as the account is created.

When the provisioning policy form is presented for completion, by default to the application owner, the value entered in the **Password** field on the form is validated against the application's provisioning policy.

Troubleshooting Password Management with Provisioning Plan Debugging

Password changes are managed as provisioning activities, creating a provisioning plan that reflects the password change as an account modification request. Problems encountered with password management during the early set-up phases can be more easily diagnosed by turning on logging of the provisioning plan for individual applications as a debugging tool. The provisioning plan shows the actions IdentityIQ intends to perform on the account.

To turn on logging, add this XML block to the desired application's XML through the IdentityIQ Debug pages.

```
<!-- Inserting a provisioning configuration to support dumping the
     provisioning plan out to the log file during every execution. -->
<!-- The deleteToDisable flag prevents account deletion activities, changing them
     to disable account requests instead of delete  -->
<ProvisioningConfig deleteToDisable="true">
  <PlanInitializerScript>
    <Source>
       System.out.println("DEBUG: ProvisioningPlan: \n" + plan.toXml());
    </Source>
  </PlanInitializerScript>
</ProvisioningConfig>
```

This writes the provisioning plan to standard out (appearing as shown below). Note that the password is written in the provisioning plan in plain text, so this ProvisioningConfig should not be left in the Application XML in a production environment.

```
DEBUG: ProvisioningPlan:
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE ProvisioningPlan PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<ProvisioningPlan targetIntegration="ADAM">
  <AccountRequest application="ADAM" nativeIdentity="CN=Adam.Kennedy,DC=sailpoint,DC=com"
op="Modify">
    <AttributeRequest name="password" op="Set" value="test123">
      <Attributes>
        <Map>
          <entry key="preExpire">
            <value>
              <Boolean>true</Boolean>
            </value>
          </entry>
        </Map>
      </Attributes>
    </AttributeRequest>
  </AccountRequest>
  <Attributes>
    <Map>
      <entry key="identityRequestId" value="0000000028"/>
      <entry key="requester" value="admin"/>
      <entry key="source" value="LCM"/>
    </Map>
  </Attributes>
  <Requesters>
    <Reference class="sailpoint.object.Identity" id="2c901c1e34aa96a70134aa96e40200ba"
name="admin"/>
  </Requesters>
</ProvisioningPlan>
```

IdentityIQ Password Management

IdentityIQ supports multiple login configurations, including single sign-on, pass-through authentication, and validation against IdentityIQ's internally stored passwords. Pass-through authentication and internal passwords can be managed through the IdentityIQ user interface.

IdentityIQ's internal set of passwords are governed by the IdentityIQ password policy. These internal passwords are always available as a fallback login validation for IdentityIQ, even when other authentication methods are used. A user or an administrator can reset an internal password through IdentityIQ's change password options.

When pass-through authentication is used, IdentityIQ enables the specification of challenge questions that can enable users to reset their own forgotten passwords, once they authenticate to IdentityIQ by correctly answering those questions. New passwords entered through this forgot password feature are validated against the pass-through authentication application's password policy and are reset on that application directly.

This section contains:

- IdentityIQ Password Configuration
- IdentityIQ Password Policy
- Defining Special Characters Available For Password Use
- Resetting IdentityIQ Internal Passwords
- Password Management with Pass-Through Authentication

IdentityIQ Password Configuration

IdentityIQ supports one-way hashing for following identity secrets:

- IdentityIQ password
- IdentityIQ password history
- IdentityIQ security question answers
- Application password history for external applications, such as Active Directory.

> Hashing support for application password history is enabled even if an application does not have a password policy.

To enable one-way hashing of secret values, click the **Gear** icon and select **Global Settings -> IdentityIQ Configuration -> Passwords** tab **-> Configuration**.

IdentityIQ Password Policy

The password policy for the IdentityIQ internally stored passwords is set in the System Setup configuration pages. Click the **Gear** icon and select **Global Settings > IdentityIQ Configuration > Passwords** tab **> Password Policy**.

Most of the setting options are the same as the password policy options for application passwords.

Unique settings available only for the IdentityIQ password policy are:

- **Define Character Types**: used to define allowable character types: Digits, Uppercase Characters, Lowercase or Non-English Characters, Special Characters. All characters are allowed if these fields are empty.
- **Days until expiration for manually set passwords**: used when a user resets their own password through the Edit Preferences window. This option sets the password expiration date by adding the specified number of days to the current date. The user is required to reset their password the first time they log into IdentityIQ on or after that expiration date.
- **Days until expiration for generated passwords**: used when an administrator resets a user's password through the Identity Cube's Attributes page. This option sets the password expiration date by adding the specified number of days to the current date. The user is required to reset their password the first time they log into IdentityIQ on or after that expiration date.
- **Minimum Hours between password changes**: specifies the amount of time (in hours) that must elapse before a user can reset their own IdentityIQ login password after they have reset it once. This does not prevent an administrator from resetting the user's password and does not prevent the user from resetting the password again immediately after it was reset by an administrator.
- **Require users to enter their current password when setting a new password**: enables a user to change their IdentityIQ password only if they enter the correct current password for the account.

Additional password policy options:

- **Password history length**: specifies number of previous passwords in password history to check against for uniqueness (prevents re-use of a password over the specified number of password changes)
- **Validate passwords against the password dictionary**: validates new IdentityIQ passwords against the password dictionary (see Defining a Password Policy for information on the password dictionary).
- **Validate password against the identity's list of attributes**: ensures that values stored as Identity attributes (last name, department, office number, region, etc.) are not used as the password

The **Validate passwords against the Identity's account attributes** option found on the application password policies does not apply to the IdentityIQ password policy. Those attributes are specific to each application and present a security risk when used in the login credentials for that specific application, but they do not pose the same risk for the IdentityIQ login.

> The password history, if a Password history length value is specified, is stored as a <PasswordHistory> element on the Identity object. It is stored as a comma separated values list of encrypted passwords. The number of passwords stored is determined by the value set for the Password history length. IdentityIQ prevents the setting of a new IdentityIQ password for the user that matches any password in the list.

Defining Special Characters Available For Password Use

IdentityIQ enables you to define the special characters that can be used in passwords throughout your deployment of the product. A default set of special characters are included in the System Configuration object.

The special characters enabled for use in passwords are listed in the passwordSpecialCharacters key. To edit these items:

- Click the **Gear** icon in the navigation menu, go to the **Global Settings -> IdentityIQ Configuration -> Password tab -> Password Policy** area, and click **Define Character Type**.
  Or

- Go to the debug page of the IdentityIQ user interface and select object type Configuration from the drop-down menu. Select the SystemConfiguration object and edit the value for the passwordSpecialCharacters entry key. For example:

```
<entry key="passwordSpecialCharacters" value="~!@#$%^*_+-={}\\][:;?,."/>
```

Resetting IdentityIQ Internal Passwords

Each user's internally-stored password in IdentityIQ can be updated by that user on the Edit Preferences window. A user with rights to edit Identities' passwords (Password Administrator, Identity Administrator, etc.) can change passwords for other users as well through the Identity Cube.

> Passwords set through these options are the internally stored passwords for IdentityIQ. They are used as the primary authentication resource when the default login configuration is used. If pass-through authentication is enabled, the internal password (if one exists) is used to authenticate a user to IdentityIQ if authentication against the pass-through authentication resource fails. This password reset is not pushed out to any external resource.

See:

- Self-Service Password Reset
- Password Resets for Others
- Password Expiration Resets

Self-Service Password Reset

To change your own IdentityIQ password:

1. From the navigation menu bar, click the user name and select **Preferences**.
2. Click the **Password** tab to display the section in which the new password can be entered.
3. If the IdentityIQ password policy requires that the current password be entered, the **Current Password** box appears, and that value must be entered for the password change to be allowed.
4. Enter the new password twice, once in **New Password** and once in **Confirm New Password**. The password must meet the requirements of the IdentityIQ password policy.
5. Click **Save** at the bottom of the window to save the password changes.

Password Resets for Others

> To use this feature, you must have authority to reset passwords for other users.

To change an IdentityIQ password for another user:

1. From the navigation menu bar, click **Identities > Identity Warehouse ->** [select Identity name]. Then click **Change Password** to display the password reset fields.
2. Enter the new password twice (once in **Password** and once in **Confirm Password**). The password must meet the requirements of the IdentityIQ password policy.

3. If this is a temporary password that the user should be prompted to reset, select **Require the user to change their password the next time that they log in**.
4. Click **Save** to save the password change. Password changes for others do not require the user to enter the current password even if that requirement exists for self-service password changes.

Password Expiration Resets

When a password expiration date is set for the IdentityIQ password, the system forces the user to change their password the first time they try to sign in, on or after the specified date.

First the user is informed that the password has expired. Click **Close** to acknowledge and dismiss this message.

Then the user is prompted to enter a new IdentityIQ password. Enter the new password in both **New Password** and **Confirm Password** and click **Change**.

Password Management with Pass-Through Authentication

> This feature is available when pass-through authentication is in use and can only be used to reset the password for a pass-through-authentication application.

When IdentityIQ is configured for pass-through authentication, the Forgot Password option can be turned on to enable a user to reset their password in the authenticating application. A user can then authenticate to IdentityIQ through security questions when they are unable to remember their password.

To enable this feature, from the Navigation bar, go to the **Gear** icon **> Global Settings > Login Configuration > User Reset** tab and select **Enable Forgot Password**.

This feature causes the **Forgot Password?** link to appear on the IdentityIQ login window. When a user clicks this link, they are prompted to answer one or more security questions that enable IdentityIQ to verify their identity. After a user successfully answers the security questions, the user is prompted for a new password. The pass-through application is then updated with that new password.

Pass-Through Authentication Requirements

Though the setup of pass-through authentication is not the focus of this document, there are a few configurations that are required for Pass-Through Authentication to work. If these configurations are not properly completed, authentication features related to Pass-Through Authentication can be prevented from working.

The **Authentication Search Attributes** field for the application must contain the names of the application account schema attribute(s) that contain the Username entered during sign-on. This field tells IdentityIQ which application fields to search to locate the matching application account. One or more attribute names can be specified in this field.

See:

- Defining the Security Questions
- Configuring the Security Question Settings
- Security Questions Tab
- Recording Security Answers

Defining the Security Questions

To specify the security questions, from the Navigation bar, go to the **Gear** icon **-> Global Settings -> Login Configuration -> User Reset** tab **-> Security Question Configuration -> Questions** area. A default set of security questions is provided. Any of these can be removed from the list by clicking the icon next to the question to be deleted. Custom questions can be defined as needed by clicking the icon next to the last question in the list and entering a new question in the box that appears.

Configuring the Security Question Settings

To configure security questions, from the Navigation bar, go to the **Gear** icon **-> Global Settings -> Login Configuration -> User Reset** tab **-> Security Question Configuration -> Settings** area.

Security Questions Tab

The Security Questions tab allows users to change security questions and answers, should the user need assistance when the password has been forgotten. The Security Questions tab is only displayed when Forgot Password and Security Question is enabled from the **Login Configuration -> User Reset** page.

Select the desired questions from the three drop-downs and provide the answers in the Answer field.

Click **Save**.

Security question settings:

- **Number of questions asked to authenticate an identity** — Specifies the number of correct answers to the security questions the user has to provide to be authenticated by these questions.
- **Number of authentication answers a user must have defined in IdentityIQ** — Specifies the number questions for which the user must provide answers in advance so they can be authenticated using these questions; questions without known answers cannot be used for authentication because there is no “correct” answer to be matched.
- **Prompt users for answers to unanswered security questions upon successful login** — Causes IdentityIQ to check (during login) whether the user has the required number of authentication answers provided already and, if not, prompt the user for those answers.
- **Maximum number of unsuccessful authentication attempts before IdentityIQ lockout** — Locks the IdentityIQ account when a user enters invalid authentication answers this number of times.
- **Number of minutes a user will remain locked out due to unsuccessful authentication**: Determines the duration of the lockout before the user can try again to sign in to IdentityIQ. During the lockout period, an administrator with the appropriate system capabilities can unlock the account by clicking **Unlock Identity** on the Identity Cube's **Attributes** tab.

Recording Security Answers

A user can only be authenticated through these questions if the answers are pre-recorded in IdentityIQ. Users can be required to provide these answers or they can choose to provide (or modify) their own answers.

Requiring Security Answers

Users can be forced to provide answers to these questions by selecting **Prompt users for answers to unanswered security questions upon successful login** in the Authentication Questions Settings. This causes the system to check whether each user has the required number of authentication answers recorded during the login process. If too few answers are recorded for a user, the **Answer Authentication Questions** window is display and the user is

required to answer these questions before they can gain access to IdentityIQ. The number of questions shown depends on the required number of answers in the Security Question Settings (**Number of authentication answers a user must have defined in** IdentityIQ). The user can select any of the configured questions from the question drop-down lists.

Users who have already provided the required number of answers are not prompted again; this window is bypassed in subsequent logins and they are taken directly to the normal IdentityIQ interface.

Independently Providing or Editing Security Answers

If users are not forced to provide authentication answers, users can choose to provide the answers through the Edit Preferences page. Users can also update their authentication answers on this window, including changing their answers or choosing different questions.

1. From the Navigation menu bar, click the user name and select **Preferences**.
2. Select the **Password** tab.
3. Select the desired questions from the question lists and provide the appropriate answer for each question. Click **Save** to save the changes.

Application-Specific Password Management Requirements

Some applications have specific configurations requirements that go beyond the basic password management requirements previously discussed in this document. This section explores some of those application-specific requirements.

This section contains:

- Active Directory and ADAM: SSL
- Windows Local and Active Directory: IQService Agent
- Windows Desktop Password Reset Utility

Active Directory and ADAM: SSL

Both AD and ADAM require a secure connection (SSL) for any password management activities. IdentityIQ offers two separate read-write connectors for each of these applications.

See:

SSL Configuration for the Direct Connector

SSL Configuration for the Direct Connector

Installations using the AD or ADAM Direct connector must generate and install an SSL certificate under AD/ADAM and then build a java key store for IdentityIQ that trusts the AD/ADAM SSL certificate.

These are the basic steps for building that java key store and configuring IdentityIQ to use it.

1. On a Domain Controller, log in as an administrator and open Internet Explorer. Navigate to **Tools** -> **Internet Options** -> **Content** and click **Certificates**.
2. Switch to the **Trusted Root Certificate Authorities Tab** and select the certificate issued by your Active Directory integrated Certificate Server. Click **Export**.
3. Choose **Base-64 encoded X.509(.CER)** as the **Export File Format**.
4. Specify file name for the exported certificate.
5. Finish the export and copy the exported.cer file to the Java client machine.
6. At the client machine run the following command from the jdk bin directory.

   keytool -import -alias [aliasname] -keystore [keystore filename] -file [fully qualified certificate filename]

   The key store (jks) file is created in the bin directory where the keytool command is found. The name of the file is the name you specified following the -keystore parameter, such as myCaCerts.jks.
7. Create the Application in IdentityIQ using the appropriate direct connector (Active Directory or LDAP - ADAM). Select **Use SSL** and provide all the required values. Save the application (do not click **Test Connection** yet).
8. Assuming that the keystore is created in /tomcat/apache-tomcat-7.0.47/, enter the following in catalina.sh:
   -Djavax.net.ssl.trustStore=/tomcat/apache-tomcat-7.0.47/myCaCerts.jks
   -Djavax.net.ssl.trustStorePassword=password
9. Restart the Tomcat server.
10. Return to the Application Definition in the UI and click **Test Connection** to verify that the SSL connection is properly configured.

Windows Local and Active Directory: IQService Agent

> AD and ADAM require a secure connection (SSL) for any password management activities.

The IQService is a native Windows service that enables IdentityIQ to participate in a Windows environment and access information only available through Win32 APIs. You must install and register an IQService before you can provision to Active Directory, aggregate Terminal Services attributes, collect information from the Windows Event Logs, or load local Windows users or groups through the Direct connectors. This includes provisioning of password changes.

IQService can be installed on an independent Windows computer or on a Windows machine that is a member of a domain. It listens for connections from an IdentityIQ instance and can be used to do one of several things, including:

- Aggregate access to the file shares on the server
- Aggregate local user and group definitions from the independent Windows machine
- Aggregate users and groups from the Active Directory or ADAM domain of which the machine is a member
- Change the passwords for a user who has rights to the independent Windows machine or the domain

The application definition for the Active Directory or Windows Local application must then be configured with the host and port where IQService is installed and listening.

Windows Desktop Password Reset Utility

Since a user would normally have to successfully log into their computer before accessing IdentityIQ (or any other application) through a web browser, enabling reset of a Windows Desktop password requires the installation of a utility application called IdentityIQ Lifecycle Manager Desktop Password Reset. This application adds a link or button to the Windows login screen that can be configured to connect users to IdentityIQ's Forgot Password feature (or any other web-based password management solution) in a restricted browser to change their password; this functionality bypasses the Windows login credential requirement for this specific and limited purpose.

> Users can only be authenticated and permitted to change the Windows Desktop password through the IdentityIQ Forgot Password functionality if they have previously configured challenge question answers that can be used for authentication.

This utility is available to any customer who has licensed the Lifecycle Manager product.

When this application is installed, the **Forgot Password?** button, tile, or link appears on the login windows.

If configured to point to the IdentityIQ Forgot Password functionality, the restricted browser window displays the IdentityIQ's challenge question authentication windows.