Unit 20: Security
Questions Covered

• What forms of security are offered by Agiloft?
• How can you integrate Agiloft with Single Sign-On providers?
• What is Two-Factor Authentication and how is it used with Agiloft?
• How can user and field permissions be enforced to prevent unauthorized access to knowledgebases and records?
• Can you set up monitoring and reporting with detailed audit logs?
By default, Agiloft already complies with many of the best security practices in the industry.

- For example, each update contains compatibility improvements with current web security standards, making the system resistant to attack.

However, users should still take some time to determine the security requirements of a new system, and configure their knowledgebase to meet their business requirements.

Agiloft contains a large number of options for authenticating users, preventing malicious attacks, monitoring system activity, and restricting user access to sensitive data.

This security training unit will provide a brief introduction to some of the available methods for improving the level of security in your knowledgebases.
Security Unit Overview

- In this unit, we will be learning to add security to Agiloft in the following ways:
  - Passwords
  - Authentication methods
  - Hyperlinks
  - Global variables relating to security
  - User permissions including field permissions
  - Activity Logs
Passwords
Passwords

- Agiloft’s password options satisfy military grade security requirements, and can be made as strict, or as lenient, as you require.

- To change the password of an Agiloft user, log in as an admin and open the People table.

  Note that only admin users are permitted by default to change other users’ passwords.

  - Edit the relevant user and navigate to the Contact Information tab.
  - Change the password in the Password field and confirm the new password.

- Note that changing your own password is a different process that depends on the KB settings. Generally, a user can access their profile – their own user record – and click Change Password.
Reset a Lost Password

- On a custom login page, the **Lost Password** link lets users reset a forgotten password.

- This feature depends on group permission settings and requires that the user has an accurate email or cell phone number on file in their user record.

- The Text Message option uses an SMS service to send a reset code to the user who then enters it into a dialog on the login page.
The **Password** field wizard provides a number of options for restricting password entry options, and enforcing regular updates.

In the **Fields** tab of a table wizard, such as the Contacts table, select **New > Password** or edit the existing **Password** field, and select the **Options** tab.

Here you can configure the following options, among others:

- The maximum and minimum number of characters.
  - It is commonly recommended to use a minimum password length of 12 to 14 characters.

- Alphanumeric values and mixed case letters with a specific number of each kind.
  - It is generally recommended to include at least one uppercase, numeric, and symbolic character.

- Exclude dictionary words and prevent the password from matching the login name.
Password Field Wizard (continued)

- Options continued:
  - Password expiration time.
  - Whether the password is required.
  - Whether the account should be locked after a number of consecutive failures, indicating that there could be an attempted breach.
  - Whether users can reuse previous passwords.
  - Whether the old password must be entered when creating new passwords.
  - Whether passwords should be stored in an encrypted format in the database.
  - Whether the password field is required when creating a new record.
  - A default value for the password, before it is changed.
  - Whether the password and account should be locked after incorrect entries.
Subtables and Passwords

• Note that the Password field, like other field types, allows for different settings on different subtables.
• In our Training KB, the People table includes subtables for Employees and External Users.
• For instance, it is reasonable to make the Password field required on the Employees subtable but not the External Users table if only employees will be logging into the system.
• In other cases, you may want to require longer and stricter passwords for employees and let end users create passwords with fewer characters and requirements.
• Although this option provides useful flexibility, every unique password configuration requires additional future maintenance.
Configure Password Rules

• In this exercise, we will enforce a much stricter standard for password requirements than the Default test KB setup. See https://en.wikipedia.org/wiki/Password_strength for more information.

• Edit the Password field of the External Users table. Use the following settings in the Options tab:
  ▪ Minimum password length – 12.
  ▪ Require alpha-numeric values with at least 1 of Alphabetic values, Numeric values, and Symbols.
  ▪ Require mixed case letters – with at least 1 Uppercase letter.
  ▪ Exclude dictionary words – Yes
  ▪ Do not allow login and password to be the same.
  ▪ Expiration time – 1 month, and when a password has expired, Ask user to change it on next login.
Configure Password Rules (continued)

- Require user to change their password if it is reset.
- **Control reuse** – Yes
- **Require Confirmation** – Yes
- **Encrypt Password** – Yes
- **Make this a required field?** – Yes
- Click **Finish**.

- Edit an external user, for example the user with Full Name ‘Repair Customer.’ Set a new password that matches this standard – for instance, @GiL0ft.US3r
- You can try passwords that do not meet these standards to see the various error messages.

💡 Note that if you are following along in your Sample KB these settings will not be enabled.
Access and Authentication
Single Sign-On (SSO)

- While password management is a critical security resource for preventing unauthorized access, your company may prefer to use an external system to manage user authentication. In these cases, Agiloft offers integration with many Single Sign-On (SSO) methods and providers.

- SSO is a session/user authentication process that permits users to enter one name and password to access multiple applications.

- In Agiloft, SSO can be enabled to allow users to log into a knowledgebase (KB) from their SAML, LDAP, Google, or Microsoft accounts, with configuration options including trusted domains and IP address range.

- In this unit, we will introduce the various options and examine the configuration screens where possible. We will not fully configure single sign-on. We encourage you to practice further by following the more detailed instructions available in the help.
Configure Single Sign-On

- The first options we will examine can be found at **Setup > Access > Single Sign-On**.

- The first sign-on method is based on an LDAP profile and requires that Active X is enabled on the user machine.

- The Google SSO option lets users log in automatically via hyperlinks if they are already signed into Google. It finds a match in the Agiloft user table based on the user’s google mail address or login, i.e. john.doe@gmail.com or john.doe.
Configure Single Sign-On (continued)

- Enabling LDAP sign-on will log users in based on their Windows ID, and can be filtered through a domain name and IP address range if you wish to limit the logins to a specific organization. The Windows Active Directory Domain Controller can also be used to authenticate users.

- If Active X authentication is enabled, it is possible to login from a user’s desktop without entering a password. This may be considered a security risk for highly privileged users such as members of the admin group. The Excluded Groups selection list allows you to exclude members of such groups from using this feature.
Single Sign-On – LDAP and Active Directory

- LDAP (Lightweight Directory Access Protocol) is an open-source directory service standard that emails and other programs use to look up information from a server.

  - Select any excluded groups from LDAP login.
  - Select whether to use NTLM v2 or NTLM v1 authentication. For more information, see https://en.wikipedia.org/wiki/NT_LAN_Manager.
  - Select whether to use Windows Active Directory domain controller.

- Next, navigate to Setup > Access > LDAP/AD Authentication.

- This opens a pop-up dialog. After clicking Next, choose LDAP or Microsoft Active Directory.

- For more information on setting up LDAP in Agiloft, see the online help at https://wiki.agiloft.com/x/PwETAO
Single Sign-On – Google OAUTH 2.0

• Google OAUTH 2.0 is the authorization framework which enables single sign-on through a Google account.

• In order to enable OAUTH in Agiloft, Enable Google Single Sign-On must be selected in the Single Sign-On screen.

• Once enabled, Google OAUTH can be configured by clicking the Configure OAUTH 2.0 Profiles button in the Access screen.

• Click New to create a new profile.

• To do a complete integration with Google OAUTH, you will need to setup the Google Developer Console and obtain the required details, including the Redirect URI and the Client ID.

• For detailed setup instructions, see: https://wiki.agiloft.com/display/HELP/Google+OAUTH+2.0+SSO
Single Sign-On – SAML

- Security Assertion Markup Language 2.0 (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization between parties, in particular, between an identity provider and a service provider. See https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language for more details.

- Agiloft knowledgebases can be integrated with a SAML 2.0 Identity Provider (IdP) such as PingOne or Shibboleth. When using SAML 2.0 single sign-on, Agiloft acts as the Service Provider.
Single Sign-On – SAML (continued)

• Find the SAML configuration menu by navigating to **Setup > Access > Configure SAML Single Sign-On**.

• In the SAML Configuration wizard, enter the details of the SAML authenticated user mapping in the respective tabs.

• In the **Identity Provider Details** tab, you can enter XML metadata details that are provided by your IdP.
Two-Factor Authentication

- Two-factor authentication (2FA), or two step verification, adds an extra level of security requirements beyond the standard login details.
- Agiloft supports two-factor authentication through SMS text message or through Google Authenticator.
- To enable 2FA in Agiloft, navigate to Setup > Access > Two Factor Authentication.
- In the Two Factor Authentication screen, select Require two factor authentication.
- Select the groups and users for which two factor authentication is excluded.
- Configure the login and renewal requirements for 2FA.
- To use SMS authentication, you must first set up an SMS account through Twilio at https://www.twilio.com
- For more information on SMS setup, see https://wiki.agiloft.com/x/DIdZAQ
- Select Text message (SMS) as the authentication method and define the message including the $code variable, then select the SMS account from the drop-down.
Two-Factor Authentication (continued)

- To use **Google Authenticator 2FA**, your users will be required to install the Google Authenticator app on their smartphones. The app can be downloaded from the iOS and Android app stores.
- You can choose whether they receive confirmation codes via SMS or email, and select the SMS account to use.
- You can also choose whether 2FA is required on every login, or just the first one.
- Now when a user attempts to log into Agiloft, they will be prompted to send a secret key to the mobile number in their profile.
- When this key is pasted into **Google Authenticator**, it will establish the user account and provide an initial key.
- Now whenever the user logs into the KB, they will be required to enter a new Authenticator code which can be found by opening the app.
Configure Two-Factor Authentication

• For the purpose of this and several other exercises in this training, you will create a test user for testing the security restrictions that you implement.

• In addition, you will need a smart device running Android (2.3.3 and up), or iOS (7.0 or later).
  ▪ Go to the People table and create a new employee user in the adminimport group,
  ▪ **Make sure** to update the user with an email address that you can access!
  ▪ In a separate browser window or tab, log in as that user and leave the window open while you set up 2FA.

  ▪ Follow the steps given at [https://support.google.com/accounts/answer/1066447?hl=en](https://support.google.com/accounts/answer/1066447?hl=en) for help configuring Google Authenticator on your phone.
Configure Two-Factor Authentication (cont.)

- In the Test KB, go to Setup > Access > Two-Factor Authentication and select Require two-factor authentication.

- Choose the following options:
  - Exclude the admin group – This enables you to log back in as the admin user if the 2FA fails to work.
  - Require authentication for the first login from a particular device.
  - Authentication Method – Google Authenticator.
  - Send initial secret code by Email.
  - Click Finish.

- In your inbox, copy the key. In Google Authenticator, click + to create a new account, enter an account name, and paste the secret key. Click ADD.

- The new account will show a 6-digit code. In Agiloft, enter the code and click Submit.

- You will be logged in as the user.
Hyperlinks

- Hyperlinks allow external users to access a system or a specific record by clicking a link, which can be embedded in emails and generated at runtime, or manually.

- Hyperlinks can be used to execute complex functions, such as logging in to a specific table and view or running a saved search.

- For example, the following hyperlink would log a user into https://example.agiloft.com/gui2 in the Banana Stand project with Username/Password login details:
  https://example.agiloft.com/gui2/login.jsp?KeyId=0&state=Main&project=Banana%20Stand&user=Username&passwd=Password.

- The formula to construct hyperlinks allows you to specify parameters such as expiration time and table access, and is discussed further in Hyperlink Formula.
Hyperlinks (continued)

• Hyperlinks sent from within Agiloft messages are automatically encrypted, so it is not possible to use them to obtain user login details; however, a malicious user could still access the system through the link.

• For that reason, when sending links from Agiloft in emails or other messages, you can enforce authentication and restrictions when users click through into the system, generally in one of two ways:
  ▪ First, the Configure Hotlinks screen at Setup > Access > Configure Hotlinks contains the settings for requirements for user authentication via hotlink.
  ▪ Hyperlinks can be set to always require authentication, or to only require authentication the first time they are clicked.
  ▪ Second, the Automatic Login Hotlinks screen at Setup > Access > Automatic Login Hotlinks enables you to encrypt any hyperlink which you manually constructed. The encrypted link can then be shared with users, or embedded in a web page, for example to create a self-registration link.
Encrypted Hyperlinks

• To create an encrypted hotlink in this screen:
  ▪ Enter the hotlink into the Encrypt Hotlink field.
  ▪ Select any excluded groups who will not be able to use the encrypted link.
  ▪ Set an expiration time.

• To add further security, you can generate an encryption/decryption key pair which can be shared to ensure that the link will only be decrypted from their location.

Generate encryption keys
Hyperlink Formula

• An Agiloft hyperlink consists of three main components:
  ▪ $URL\_address\_of\_Agiloft$? — This is the address for the server where the Agiloft instance is installed. For example, https://<server>gui2/login.jsp
  ▪ KeyID=0 — Strictly speaking, this is just another keyword/parameter pair, but it is always the same and is required in all hyperlinks.
  ▪ Keyword/Parameter pairs — With the syntax &keyword1=value1&keyword2=value2 – for instance, user=admin&password=Ag1L0FT!tR@iN^ng.

• For a detailed description of the parameters that can be used to construct a hyperlink, see Hyperlink Keywords and Examples.

• In addition, to add security to the standard URL format, the urlEncode(url) function treats the URL as a hotlink, retrieves the keys, and encrypts the output as a secured hotlink.

• For example, urlEncode("http://localhost:8080/gui2/login.jsp?keyID=0&KB=a&user=admin&passwd=qwer
ty&state=Main") will be parsed as: http://localhost:8080/gui2/login.jsp?p=a&genhotlink=Aj3ze1xUTq4FziVPB9W5INENQy1xxpLju4lsfbPOxwlXRB/MPL8VHo+m72uJJmGvL9mh6Qm+vhPCU41hVmkMfVVj/YGTEbLzsAobYYfHpv6Y.
Configure Hyperlinks

- Let’s test some hyperlinks with the user you created in the Configure Two-Factor Authentication practice exercise. In the examples below, replace the variables in <BRACKETS> with your server, KB name and user login details. For instance:
  - <SERVER> - ew-132.saas.enterprisewizard.com
    <KBNAME> - Your%20Name%201483%20Training

- First, let’s create a hyperlink that logs the test user into the Contacts table of the test KB:

  https://<TESTSERVER>.com/gui2/login.jsp?keyID=0&kb=<KBNAME>&user=<USER>&passwd=<PASSWORD>&State=Main&table=contacts

- Open a new Support Case without allowing the user to view the rest of the Agiloft GUI:

  https://<SERVER>.com/gui2/login.jsp?keyID=0&kb=<KBNAME>&user=<USER>&passwd=<PASSWORD>&State=New:task&gui=no
Configure Hyperlinks (continued)

- Open a record in the Approvals table in edit mode. Note that in this case the record ID is 613, but you should ensure that this exists in the KB, or use an ID that does exist.

  https://<SERVER>.com/gui2/login.jsp?keyID=0&amp;kb=<KBNAME>&amp;user=<USER>&amp;passwd=<PASSWORD>&amp;State=Edit:Approval&amp;table=Approval&amp;record=613&amp;record_access=edit

- Encrypt the hyperlink above:
  - Go to **Setup > Access > Automatic Login Hotlinks**.
  - In the **Encrypt Hotlink** field, paste the hotlink.
  - Set the **Expiration** time for 10 minutes, and click **Encrypt**.
  - Copy the encrypted hotlink that appears. Paste it into your browser’s address bar to test it.
Global Variables
Global Variables in Security

- **Global Variables** are a store of values in predefined formats that can be customized by the user and will be applied throughout the knowledgebase wherever the variable appears. For more information, see Training Unit 17.

- Global variables can be configured within a knowledgebase by navigating to **Setup > System > Manage Global Variables**.

- While many of the available system variables do not have a security impact, there are several parameters that we suggest configuring to optimize security in a KB. The following slides define some of the most important security-related variables.
Security Related Variables

• Security: Check client IP
  ▪ **Description:** Check that requests are coming from the same IP where the session was started. If set to Yes, the system checks that all requests originate from the same IP from which the session was initiated. This helps prevent hackers who can see the URL/session ID on your PC from initiating a session on another machine. It is not as secure as Security: Check Session Match because if both computers are accessing the server through the same NAT or Proxy servers, their IPs will seem to be the same. Please note that this feature will cause the user to be logged out if they access the system from an ISP or through a gateway that assigns a dynamically changing IP address.

  ▪ **Recommendation:** This variable should generally be set to No because stronger security is provided by the Check Session Match variable. It is provided for those rare installations that block the use of cookies.

• Security: Allowed External Hosts
  ▪ **Description:** If the constant is set, the system will only allow redirection to URLs at one of the specified hosts in order to guard against XLS attacks. Multiple hosts may be specified, delimited by spaces, comma or semi-colons. To allow any host, set the constant to *.
Security Related Variables (continued)

- **Recommendation**: This variable should generally be set to a value such as YOUR_COMPANY_NAME.COM, SERVER_URL.COM.

- **Security: Check Session Match**
  - **Description**: Require matching session and passed cookie. If the session ID does not match the cookie associated with that session when the user first logs in, the connection will be rejected. This prevents hacker who are able to see the user's browser from manually entering the URL.
  - **Recommendation**: This variable should generally be set to All_Users.

- **Security: Informative Password Messages**
  - **Description**: If set to YES, diagnostic messages in password related functions may contain account name.
  - **Recommendation**: This method is less secure and the variable should generally be set to No.
Security Related Variables (continued)

- Security: Show Stack Trace on SoD
  - **Description**: Show stack trace button on SoD screen. For added security, this should be set to **No** to prevent users from seeing the stack trace information.
  - **Recommendation**: This variable should generally be set to **No**.

- Security: Trusted Zones
  - **Description**: In order to protect user data from malicious attacks (XSS, XSRF, etc.) you can specify addresses of net resources on which HTML codes in the system can refer - hyperlinks, images, embedded objects, etc. Please separate multiple values with comma or CR character.
  - **Recommendation**: This variable should generally be set to */, *.YOUR_COMPANY.COM

- Security: REST IP Whitelist
  - **Description**: Whitelist of IP Addresses applicable to access via REST interface. Project settings take precedence over the server-wide settings. If a whitelist is set, all other IPs are automatically blocked. IPv4 and IPv6 comma separated IPs and IP ranges may be entered.
  - **Recommendation**: Set to the value of the machines from which your REST scripts are running or set to 127.0.0.1 to block external access.
Permissions and Auditing
Permissions and User Access

- Group permissions enable you to protect sensitive tables, records or fields from being viewed and edited. For more information, see https://wiki.agiloft.com/display/HELP/Groups

- In the Group Permissions Wizard, located at Setup > Access > Manage Groups > Edit any group, table and general permissions can be set for a user group.

- The Table Permission wizard, located by editing a table in the Tables tab of the Group Permissions Wizard, contains very fine-grained permissions for:
  - Menus, such as saved searches, templates and reports.
  - Records, including create, edit, mass edit and view permissions.
  - Fields in the table.

- For more information on permissions, please review Unit 14: Group Permissions.
Permissions and Least Privilege

- In information security, the principle of least privilege* stipulates that a user should only be able to access the information and resources that are necessary for them to carry out their legitimate purpose.

- Agiloft permits a very high level of granularity when setting access privileges, and system administrators should be careful not to permit their user groups to have greater permissions than their role strictly requires. This prevents users from unintentionally accessing sensitive information and from inadvertently changing records that should be restricted.

- When setting up a knowledgebase, there should always be some consideration of the level of access that is needed for each type of user in relation to activities such as:
  - Record conversion
  - Record creation
  - Field viewing
  - Field editing
  - Table viewing

Field Permissions

- In a complex system with many tables and rules, setting field permissions for security purposes is particularly challenging because it is not always obvious what permissions are needed for automation functionality to work properly.

- Below are some considerations and options when setting up field permissions in a table:

- **Background tables** – When a background table provides the data that a user must select in another table, the user’s group must have some basic permissions related to the background table.
Background Table Permissions

For example, the Contract Type is a background table for Contracts. To choose a **Contract Type**, users must have the following permissions:

- Access to the table Contract Type table, or else the **Contract Type** field in Contracts will show null values.

- **View Own** and **View Other** record-level permissions for Contract Types, as well as **View Own** and View Other field-level permissions for the field used in contracts to select a Contract Type. Otherwise, the **Contract Type** field selector in contracts will not show any records to select, or will show --null-- values.

Now, when the user selects the **Contract Type** in a Contract, any other fields included in the linked set can be viewed by the user, whether or not they can view those fields in the source Contract Types table. In other words, once the source record is selected, the Contract table permissions supersede the permissions for the source fields in Contract Types.
Special Field Permissions

- **Record Conversions** — When conversion mapping is set up, users do not need to have view permissions for either end of the transaction. However, if they are performing a record conversion for a linked field, they will need **Create** permissions for the linked field in the target table that is being used to link back to the original record.

- **Conditional Editability** — **Edit** permissions can be restricted by adding conditions to the field for selected groups in the **Options** tab of the Field wizard. Fields that are restricted from editing will still be visible, but displayed as plain text.

- **Conditional Visibility** — Standard view permissions are set on the **Permissions** tab of the Field wizard. However, sometimes you may want to limit a field from view unless a condition is met. In the **Display** tab, select **Add Condition** under **Make the visibility of this field conditional**. For instance, if a Contract status changes, you may hide sensitive data fields from view.
Field Permissions (continued)

• Note that if the visibility conditions are met, users are still able to see and potentially edit sensitive data. For this reason, view restrictions are primarily used for optimizing the record layout by hiding irrelevant fields.

• **Action Buttons** – Giving users *view* access to an action button allows them to execute that action on any record they can *edit*. Action buttons run with global system permissions, so the user pressing the button typically does not need permission to edit the specific fields or linked records updated by the button’s actions.

• For these reasons, it is important to treat action buttons carefully to prevent people from using them when it is not appropriate.

• You can also add action buttons to the action bar, allowing users to run actions on multiple records. When a user runs an action this way, without opening the record, the system checks if they have permission to edit the record. If not, the user receives an error message that the action could not complete.
Related Table Permissions

- **Related Tables** – There are several different ways to prevent unauthorized access to records in a related table. For instance, consider a related table of Support Cases contained in the Company record. Typically such a related table includes controls to look up additional records to link or unlink a record from the related table. Below are some options for situations where you do not want certain users to change the Support Cases related table in a company record:

  - In the Field wizard for a related table, the **Permissions** tab includes an option to **Allow users to unlink records**. If the user does not have the permission, they can’t remove records from the related table.
  - You can customize the action bar for a related table to hide the lookup and unlink options.
  - If a user doesn’t have edit permissions for the fields in the set of linked fields in the source related table – meaning those fields in the Support Case table which link to the Company table – then the lookup and unlink action bar items will not work, but the user will not receive a warning or error.
Field Permissions Practice

• Let’s say we want to make a Task description non-editable once it has been completed, for all but admin-level users:
  ▪ Go to the Tasks table of your Training KB as the admin user and edit the Task Description field.
  ▪ In the Options tab, under Make the ability to edit this field conditional, select the Prevent users in the checkbox and then select all groups apart from the admin user.
  ▪ In the groups from editing this field if drop-down, select Status.
  ▪ In contains one of these values, select Done.
  ▪ Click Finish.
Field Permissions Practice (continued)

- Edit a Task in the table and change the Status to Done, then Save it.
- Edit the Task again. The Description field will still be editable.
- In a separate tab, log in as the user you created in the Configure Two-Factor Authentication practice.
- Edit the Task. The Description field will be displayed as plain text.
Auditing with Activity Logs

- Activity logs maintain a record of any specified statistics of system usage, which can assist with auditing behavior that might compromise your security.
- To view your activity logs go to the Activity Log table and view a record.

- Click **Setup > System > Configure Activity Log** to set up the auditing rules which define what system usage statistics to keep and how long to retain them.

Click Configure Activity Log to define what statistics are kept of system usage and for how long they are retained.
Auditing with Activity Logs (continued)

- The Audit Rules wizard allows you to define system events, and create saved searches for logging user actions.
- Any of the events selected will trigger a notification in the activity logs.
- In addition, rules can be created from events in the Activity Log table. This can be used to notify you when, for instance, a user record is changed or if someone changes a rule or a workflow, and this creates a record in the Activity Log.
- It can be very useful to set up reports for activities that pose a security concern. For instance, you could create a report for failed logins that would alert you if there had been an attempt to breach the login screen.
Create an Activity Log Report

• Click **Setup > System > Configure Activity Log**, then click **New** to create a new audit rule.

• Enter the name ‘Failed Logins’, select the **Login Failed** checkbox.

• Change the default retention schedule from 1 Day to 1 Month and click **Finish**.

• It is possible that the Activity Log table is not activated. In that case go to **Setup > Tables**, select **Activity Log** and click **Unhide**.

• Go to **Activity Log Charts/Reports** and create a new report titled Login Failures.

• For the **Output format**, select **HTML**.

• Click **Next** twice to reach the **Filter** tab, then under **Relative dates**: select a Start Date of **Date of Earliest Activity Log**, and an End Date of **Today**.
Create an Activity Log Report (continued)

- At the bottom of the Filter tab, let’s create a saved search to find Failed Logins over the last 30 days.
  - In the search dialog, choose a Simple filter that finds “Action = Value Login Failed”, and a Time filter where “Date is less than 30 Days old.”
  - In the Options tab, name the saved search “Login failures for last 30 days”.
  - Make the search accessible and active for the Creator and Admin group users. Click Finish to close the search wizard.
- In the Grouping/Summary tab, select these options:
  - Add Summary Information using “the number of Activity Log”.
  - Show records? using the Personal view, and show not more than 100 records in each grouping.
  - Group data by: in the dialog, choose User Name, then click Finish.
- In the report wizard, select the Preview tab and then click Finish to save the report.
Test the Audit Rule

- Now we can test the audit rule and the report we just created.
- Log out of the knowledgebase, then attempt to log in with an incorrect password to provoke a failed login.
- Now do a few successive failed login attempts using the wrong user/password combination.
- Log back in (successfully) as the admin user and view the Activity Log table to see the records created.
- Next, view the report.
Security Unit Summary

• In this unit we have learned about many of the options available for increasing the security of an Agiloft system.
• Single Sign-on methods include LDAP, Active Directory, SAML and Google OAuth, among others.
• Two-factor authentication uses either SMS or Google Authenticator to require an additional step for users to login.
• Hyperlinks can be used to allow external users to access the system, with a high level of specificity for the level of access they provide.
• Global variables can restrict system behavior and access by default.
• User and field permissions can control the information users are allowed to access and change within a system, and should be carefully managed to prevent undesirable access when using linked fields and related tables.
• User passwords can be configured to be as strict or lenient as required.
• Activity logs provide reporting capabilities for monitoring system activities.