Security

There are several parameters that can be configured to optimize security in **Setup > System > Security**. Configure each setting as needed to provide optimal security for your system.

General Tab

The General tab has most of the security options necessary to secure your system. You might use some or all of these features in various combinations to suit your needs.

Restrict Standard Login / Password based access to Agiloft users authenticated by SSO

This option determines whether to restrict standard login/password-based access to only those users who have been authenticated by SSO. With this set to Yes, users who log in with a valid login and password must still be authenticated by SSO in order to access the system.

SSO Endpoint

SSO Endpoint allows an encrypted email hotlink to connect to a custom web SSO application. If you enter an endpoint value here, hotlinks included in emails do not include the login and password for authentication. Instead, hotlinks redirect to the specified endpoint and allow the user to be authenticated and logged in.

Security: Trusted Zones

Use the Trusted Zones option to limit external net resources to a specified list of source addresses. For example, if you add trusted zones here, users are only able to add hyperlinks and embedded images that point to locations inside these trusted zones. You can use this to help protect user data from malicious attacks, such as XSS or XSRF attacks. To use trusted zones, enter a comma- or CR character-separated list of addresses. HTML references outside these addresses aren't allowed.

If URLs outside the trusted zones are added in the system, they are displayed in gray to indicate they aren't clickable.

For optimal security, this global variable should generally be set to /, *.YOUR_COMPANY.COM.

Example Values:

Value	Behavior
*.agiloft.com , /	Users can refer to agiloft.com domain, its subdomains and the server host, without defining its name.
*, /	Users can refer to any domain in the net and the server host.
/	References to net resources are disabled.
NULL	Only references to the current host are enabled (e.g. /home.jsp).

⚠ This option restricts what URLs can be displayed within Agiloft. As such, the domain name or specific URLs that may be referenced as embedded URLs within the Home page should be added to the list.

Security: Allowed Referrers

This option restricts the host names that are allowed as referrers to your server. Enter a comma separated list of host names to use this feature. A value of “*” allows any host name to act as referrers to this server.

Security: Hotlink Master Password

This defines the master password used for checking cookies for those users who selected to save login credentials for generated hotlinks.

Allow use of Anonymous User

This allows anonymous users to use hotlinks without providing login credentials.

JavaScript Injections in UI

This determines whether JavaScript is allowed in the Look and Feel wizard options and in record form text headings. This can prevent malicious injections in interface objects. If you use JavaScript as part of your system design, set this to Yes.

Security: Permit Javascript in print templates

This determines whether JavaScript scripts are allowed in print templates. Select Yes to allow scripts.

Security: Allow scripts in dashboard widgets

This determines whether the system allows scripting in widgets on the dashboard. Select No to disable scripting and help protect users from malicious attacks (XSS, XSRF, etc). This ensures that only safe HTML is allowed.

Security: Allowed External Hosts

Use this option to restrict the host URLs the system is allowed to redirect to. This helps guard against XLS attacks. Specify as many hosts as necessary, delimited by spaces, commas, or semi-colons. To allow any host, enter *. This global variable should generally be set to a value such as *.YOUR_COMPANY_NAME.COM, *.SERVER_URL.COM. For example, *.widget.com, *.widget.enterprisewizard.com *.widget.agiloft.com.

⚠ This global variable restricts which values work as ExitURLs. If you use hotlinks that specify ExitURLs, add them to the list of values entered here.

Security: Re-generate cookie

This determines whether the system accepts cookies provided by the browser to re-enter a user session. For optimal security, this should be set to Yes, but you might decide to set it to No if your users frequently open Agiloft in multiple tabs. If this is set to Yes, users can open the system in only one tab at a time.

Security: Check client IP

Use this option if your installation blocks the use of cookies, which are necessary for the default session matching used by your system. If set to Yes, this checks that all system requests are made from the same IP address as the IP address used when the session first started. This helps prevent a hacker from seeing the URL or session ID in the browser and initiating a session on another machine. However, users whose ISP or gateway assigns a dynamically changing IP address are logged out when the IP changes.

Note that this method is not as secure as the default session matching behavior. Generally, this should be set to No so that the default session matching is used instead.

Security: Informative Password Messages

This determines whether diagnostic messages in password-related functions can contain the account name. If you set this to Yes, you can use the Security: Custom message for "Reset Password" error global variable to define a custom error message.

For optimal security, this variable should generally be set to No.

Security: Custom message for "Reset Password" error

If you set Informative Password Messages to Yes, use this field to define the custom message that appears when an error occurs during password reset. It's best to leave this variable unset or use a message that does not provide any security information, such as "Invalid login/password combination, please contact your administrator."

Security: Show Stack Trace on SoD

This determines whether the stack trace button appears on the SoD screen. Select No to prevent users from seeing the stack trace information. This feature is generally only used when testing a knowledgebase to troubleshoot errors.

Security: Web Services Anti SQL Injection

This determines whether anti SQL injection features are enabled. Select No to disable these features.

Security: Web Services Verbose Errors

This determines whether SOAP and REST calls produce more detailed error messages for debugging purposes. This feature is usually only set to Yes in testing environments, and should be set to No in production environments.

Security: Days to continue support of old key

This defines the number of days to continue the support of old keys. The default value is 31.

Security: JS Exceptions

This setting adds exceptions to the protections against cross-site scripting (XSS) attacks in setup wizards. The default value is Standard, which allows some common sense exceptions while still checking the contents of wizard values. You can select None to apply the highest level of protection to any text entered in a setup wizard, with no exceptions, or you can use All to use no extra protection for the setup wizard compared to the rest of Agiloft.

Enable CORS for REST Service

Enable cross-origin resource sharing (CORS) for the REST API, which allows requests from one origin to another origin. This is most useful in cases where you are using a separate website or web app that is hosted in your own domain, such as mycompany.com, but you want to call the Agiloft REST API.

If you set this to Yes, make sure to specify the REST Service Allowed Origins.

REST Service Allowed Origins

If Enable CORS for REST Service is set to Yes, use this field to specify the origin domains that are permitted to make requests. Make sure to include https:// and exclude the slash (/) at the end of the URL.

Enable AppSource for ACA

This setting controls whether you can use AppSource to install the Word and Outlook apps directly in Word and Outlook. By default, this is set to Yes to make it easier to install and set up these apps. In most cases, this setting does not need to be changed.

AppSource ACA Domain List

This list specifies the domains that are used by AppSource to make the Word and Outlook apps available for connection to Agiloft. By default, the list includes domains for both apps. In most cases, this list does not need to be altered.

Web Services Tab

This tab contains settings related specifically to web services.

SOAP Groups

Select the groups whose users are allowed to use SOAP.

Security: SOAP IP Blacklist

Any IP address defined in this global variable is unable to access the system via the SOAP interface. If a blacklist is defined, IP addresses on the blacklist are not accepted, and IP addresses outside the blacklist are subject to any other relevant security checks. You may enter IPv4, IPv6, and IP address ranges in a comma-delimited list, such as 10.168.6.102, 10.169.7.132-10.169.7.150. Server-wide settings take precedence over specific KB settings.

If you use the SOAP IP Whitelist, it is generally not necessary to set values in the Blacklist as well. However, the Blacklist is useful if you allow API access from a constantly changing set of IP addresses that do not live within well-defined ranges, but you also want to block access from certain ranges, such as those of foreign countries.

Security: SOAP IP Whitelist

The system allows any IP addresses defined in this global variable to access the system via the SOAP interface. If a whitelist is defined, all other IP addresses are automatically blocked. You may enter IPv4, IPv6, and IP address ranges in a comma-delimited list, such as 10.168.6.102, 10.169.7.132-10.169.7.150. KB-specific settings take precedence over server-wide settings.

For optimal security, set this global variable to the value of the machines from which your SOAP scripts are running. You may also enter 127.0.0.1 to block external access entirely.

REST Groups

Select the groups whose users are allowed to use REST.

Security: REST IP Blacklist

Any IP address defined in this global variable is unable to access the system via the REST interface. If a blacklist is defined, IP addresses on the blacklist are not accepted, and IP addresses outside the blacklist are subject to any other relevant security checks. You may enter IPv4, IPv6, and IP address ranges in a comma-delimited list, such as 10.168.6.102, 10.169.7.132-10.169.7.150. Server-wide settings take precedence over specific KB settings.

If you use the REST IP Whitelist, it is generally not necessary to set values in the Blacklist as well. However, the Blacklist is useful if you allow API access from a constantly changing set of IP addresses that do not live within well-defined ranges, but you also want to block access from certain ranges, such as those of foreign countries.

Security: REST IP Whitelist

The system allows any IP address defined in this global variable to access the system via the REST interface. If a whitelist is defined, all other IP's are automatically blocked. You may enter IPv4, IPv6, and IP address ranges in a comma-delimited list, such as 10.168.6.102, 10.169.7.132-10.169.7.150. KB-specific settings take precedence over server-wide settings.

For optimal security, set this global variable to the value of the machines from which your REST scripts are running. You may also enter 127.0.0.1 to block external access entirely. Be careful when configuring this variable. You can potentially lock yourself entirely out of a knowledgebase if it's configured improperly.

WDC Editor Groups

Users who are part of a group selected in this field have permission to set a saved search to be available in Tableau . This generates a WDC URL that can be used as a Web Data Connector in Tableau.

IP Restrictions Tab

This tab allows general IP restrictions for system access. These settings work together to determine whether a user can successfully access the system, so choose your configuration carefully. These settings are useful if some groups should only have access to the system when they are at a specific location or using a specific workstation or network.

1. In the Groups to be Restricted field, select the groups whose access you want to limit based on IP.

2. In the Whitelisted IP Ranges field, enter the IP ranges you expect from these users when accessing the system. Users in the groups you selected above will only be granted system access if they log in from a whitelisted IP address. You can enter IPv4, IPv6, and IP address ranges in a comma-delimited list.
3. In the Whitelisted Users field, you can select individual users who might be part of a restricted group, but who should always have access to the system, regardless of IP address.

Additional Security Global Variables

In addition to the settings in the Security wizard, there are a few security-related global variables you might want to set. For details on how to access and set global variables, see Global Variables.

Security: Check iframe origin

Name: check_iframe_origin

Description: Determines whether the system requires that KB usage occurs only in an iframe, or an embedded web page, that has the same origin as the KB. If this global variable is set to No, any origin is allowed. If you are using a third-party or external API that displays information in the End User Interface, this variable should be set to Yes.

Default Value: No

Recommended Values:

Location: Admin Console

Security: Collect System Data on Error

Name: collect_system_information_on_sod

Description: Determines whether to collect and include system information, such as the OS version and IP address, in the data that appears on the automatic bug report screen (SoD). Select Yes to collect and include this information.

Default Value: No

Recommended Values: For optimum security, the recommended value is No.

Location: Admin Console

Security: Show KB Names

Name: show_kb_names

Description: Determines whether the generic login page shows a drop-down list of KB names. If set to No, the KB list on the /gui2 login page is hidden, and users need to manually enter the desired KB name.

Default Value: No

Recommended Values: For optimal security, this variable should generally be set to No.

Location: Admin Console