Security and Global Variables

There are several parameters that can be configured to optimize security using the global variables in **Setup > Systems > Manage Global Variables**. They are explained below, together with their recommended values. For more information on how to configure global variables, see Global Variables.

Security:Allowed External Hosts

Name: Allowable_Redirection_Hosts

Description: Defines the host URLs to which the system allows redirects. This helps guard against XLS attacks. Multiple hosts may be specified, delimited by spaces, comma or semi-colons.

To allow any host enter a value of *.

Default Value: *

Recommended Values: 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.

Note that 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.

Location: Admin Console, Power-User Interface

Security:Check Session Match

Name: require_matching_cookie_and_seance

Description: Determines whether the system requires that the session ID matches the cookie associated with it. If you select Yes and the session ID does not match the cookie associated to that session when the user first logged in, the connection is rejected. This guards against a hacker who can see the user's browser from manually entering the URL.

Default Value: No

Recommended Values: For optimal security, this global variable should be set to All_Users. Note that some browser settings or firewalls may prevent cookies from being used. In that case, you can either set this global variable to No and enable the Security:Check client IP global variable or, if your Admin or Power Users are not affect by the issue, you can enter a value such as Admin_Users or Staff_Users for more security.

Location: Admin Console, Power User Interface

Security:Check client IP

Name: require_ip_check

Description: Determines whether the system checks that all requests are made from the same IP address as the IP address used when the session first started. This helps prevent a hacker who can see the URL/session ID on your PC from initiating a session on another machine.

Note that this feature causes 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.

Additionally, this method is not as secure as using Security:Check Session Match because if both PC's are accessing the server through the same NAT or Proxy servers, their IP addresses appear to be the same.

Default Value: No

Recommended Values: This variable should generally be set to No because stronger security is available using the Security:Check Session Match global variable. This option provides for those rare installations that block the use of cookies and, therefore, the use of the Security:Check Session Match global variable.

Location: Admin Console, Power User Interface

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:Informative Password Messages

Name: informative_password_messages

Description: Defines whether diagnostic messages in password-related functions contain the account name. If set to Yes, the relevant diagnostic messages may contain the account name. Additionally, if set to Yes, you can use the Security:Custom message for “Reset Password” error global variable to define a custom error message.

Default Value: No

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

Location: Power User Interface

Security:Custom message for "Reset Password" error

Name: ResetPasswordErrorMessage

Description: Defines the custom error message that appears when an error occurs during password reset if the Security:Informative Password Messages global variable set to Yes.

Default Value:

Recommended Values: This variable may be left unset, or set to some helpful message that does not provide any security information, such as "Invalid login/password combination, please contact your administrator."

Location: Power User Interface

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

Security:Show Stack Trace on SoD

Name: show_stack_trace_button_on_sod

Description: Determines whether the stack trace button appears on the SoD (bug report) screen. Select No to prevent users from seeing the stack trace information.

Default Value: No

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

Location: Admin Console, Power User Interface

Security: Trusted Zones

Name: trusted_zones

Description: Specifies a comma- or CR character-separated list of addresses for net resources (such as hyperlinks, images, embedded objects, etc.) from which HTML code in the system is allowed to refer. You can use this to help protect user data from malicious attacks, such as XSS or XSRF attacks.

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).

Note that 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.

Default Value: / *

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

Location: Power User Interface

Security:REST IP Whitelist

Name: rest_ip_whitelist

Description: Defines a comma-separated whitelist of IP addresses. 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, such as 10.168.6.102, 10.169.7.132-10.169.7.150.

Note that KB specific settings take precedence over server-wide settings.

Recommended Values: 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.

Location: Admin Console, Power User Interface

Security:REST IP Blacklist

Name: rest_ip_blacklist

Description: Defines a comma separated blacklist of IP addresses. Any IP address defined in this global variable is unable to access the system via the REST interface. You may enter IPv4, IPv6, and IP address ranges, such as 10.168.6.102, 10.169.7.132-10.169.7.150

Note that server-wide settings take precedence over specific KB settings.

Default Value:

Recommended Values: If values are set for the Security:REST IP Whitelist global variable, it is generally not necessary to set values for Security:REST IP Blacklist. However, Security:REST IP 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 want to block access from other ranges, such as those of foreign countries.

Location: Admin Console, Power User Interface

Security:SOAP IP Whitelist

Name: soap_ip_whitelist

Description: Defines a comma separated whitelist of IP addresses. 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, such as 10.168.6.102, 10.169.7.132-10.169.7.150.

Note that KB specific settings take precedence over server-wide settings.

Recommendation: 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.

Location: Admin Console, Power User Interface

Security:SOAP IP Blacklist

Name: soap_ip_blacklist

Description: Defines a comma separated blacklist of IP addresses. Any IP address defined in this global variable is unable to access the system via the SOAP interface. You may enter IPv4, IPv6, and IP address ranges, such as 10.168.6.102, 10.169.7.132-10.169.7.150

Note that server-wide settings take precedence over specific KB settings.

Recommended Values: If values are set for the Security:SOAP IP Whitelist global variable, it is generally not necessary to set values for Security:SOAP IP Blacklist. However, Security:SOAP IP 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 want to block access from other ranges, such as those of foreign countries.

Location: Admin Console, Power User Interface