Axeda Platform - System Configuration properties (Platform settings)

This table lists and describes the properties shown in the Axeda® Administration application. These properties are defined and specified in the Platform by the Platform admistrator. (The property, **Custom Build Info,** is also set in the Platform but is derived from another property file.)

To help you find a description of a property quickly, the table lists the properties in alphabetical order.

Note: Some Platform properties are disabled (commented out) by default and therefore do not appear in the Administration application, System Configuration pages. If they aren't shown in this online help then they are set to not show by default in the Platform.

If you have any questions or concerns about how your server is configured with regard to its property settings, contact your Platform administrator.

System Configuration Properties

Property	Description
Access message timeout	The number of seconds the Access application waits between messages from Access Viewer or Access Remote. If the Access application does not receive any messages within this time period (for example, if there are network problems), the session is disconnected. The default is 40 seconds. In addition, this is the period of time within which the Access Viewer and Access Remote operators must connect to the shared session. If both Access Viewer and Remote do not connect to the session within this timeout period, the session will time out, and a new session must be requested.
Access session ID length	Length (in characters) of the Access Session ID. The default length is 6 characters.
Access session timeout	The number of minutes an inactive session stays open, waiting for activity, before it is removed. An inactive session is one that has not been used (no Access Viewer or Remote computers shared using this session ID). The default is 10 minutes (between contacts).
Access unattended session timeout	The number of minutes an inactive, unattended session stays open, waiting for activity, before it is removed. An inactive session is one that has not been used (no Access Viewer or Remote computers shared using this session ID). The default is 10 minutes (between contacts).
ActiveMQ Broker name	The name of the machine where the ActiveMQ Server (Broker) is running.
Additional Auditor types actively running in the system	Registers the types of auditors to use along with the JDBC Auditor when dispatching audit messages. Supported values of this property are as follows: AUDITOR_SYSLOG_SERVER (Note: Configuration properties for the syslog server such as host and port number, syslog facility id, and message format template can be specified in the log4j.appender.SYSLOG definition of the log4j.properties file.]
Administrator e-mail	The e-mail address of a user defined as a ServiceLink administrator.
Allow automatic creation of devices	True to allow automatic addition of assets to the database upon registration.

System Configuration Properties *(continued...)*

Property	Description
Allow automatic creation of models	True to allow automatic addition of models to the database upon registration.
Allow hosted sessions to be stopped. (Caution should be taken when setting to true.)	True to allow the Administrator to stop Global Access Server remote sessions hosted by this server (using the Administration application). By default, the administrator cannot stop host GAS remote sessions (False).
Allow remote sessions to be stopped	True (the default value to allow the Administrator to stop Global Access Server remote sessions (using the Administration application). If changed to false, administrator cannot stop GAS remote sessions.
Allow Remove of Tenant user	True (default) to enable users to remove Delegated Admin Units from the server. False to prevent Applications users from deleting Delegated Admin Units. Users also need the privilege, *Delegated Admin Unit - Remove,* to be able to remove Delegated Admin Units.
Allow the Admin to remove Remote Session Audit Information	Specifies whether or not the Administrator can remove Audit Session information: • False (default) to prevent the Admin from removing the Audit Session information • True to allow the Admin to remove the Audit Session information.
Allow unencrypted device data	True to allow the application to accept unencrypted messages from assets, or false to reject unencrypted messages.
Allow users to remove partner accounts	True to enable users to remove partners defined in the server from the server. False (default) to prevent Applications users from deleting partners. Users also need the privilege, *Partner Login - Remove Partner Account,* to be able to remove Partner Login accounts.
Allow users to remove remote Enterprise servers	True (the default value) to allow the Administrator to delete remote Enterprise servers (from the Administration application). If changed to false, the administrator cannot delete the remote Enterprise server.
AMQ JMX Domain	Identifies the ActiveMQ JMX domain that all objects names will use.
Application Bridge Server use SSL	True to enable SSL for the Application Bridge Server (ABS); false (default) to disable SSL for it.
Application Bridge Server web service	True to enable Web Services for the Application Bridge Server (ABS); false (default) to disable Web Services for it.
AQL query SLA target ms	The AQL SLA target. Need a little time for Groovy, WS, and network.
AQL SLA violation collection clear size	Size at which collection recording SLA violations clears to avoid excessive memory
AQL stats logging query count modulo	AQL stats logging query count modulo
ARemote minimum ping rate	Minimum ping rate for an Axeda Access Remote host. By default, this feature is off (property value is -1).

System Configuration Properties *(continued...)*

Property	Description
Audit Categories allowed for auditing (no value means all Audit Categories are allowed)	Registers the types of audit categories that will be dispatched to the auditors; audit messages of any other audit category type will not be dispatched. If the value of this property is empty, or if the property is omitted altogether, no filtering will be performed, Audit messages of any audit category type will be dispatched. Note: Currently, audit category filtering is activated for the Syslog Server auditor only. Supported values of this property are as follows: • dashboard • data-export • data-management • device-communication • file-upload • maintenance • network • notification • partner-access • report • scm-file-transfer • scm-package-management • transport-servicelink • update-window
Authenticator types assigned to the partner user store (comma-separated)	Supported Authenticator types for the Partner Login user store (if applicable to this server): • ActiveDirectoryAuthenticatorMBean • IPlanetAuthenticatorMBean • LDAPAuthenticatorMBean • NovellAuthenticatorMBean • OpenLDAPAuthenticatorMBean
Authenticator types assigned to the user store (comma-separated)	Supported Authenticator types for the Delegated Administration user store (if applicable to this server): • IPlanetAuthenticatorMBean • LDAPAuthenticatorMBean • NovellAuthenticatorMBean • OpenLDAPAuthenticatorMBean
Auto Refresh Rate	The default rate of refreshing tables is every 60 seconds.
AxedaDirect SSL connection port socket	The number of the SSL port that Remote Server can use to connect directly to the Enterprise Server. Defaults to 17002.
AxedaDirect standard connection port socket	The number of the port that Remote Server can use to connect directly to the Enterprise Server. Defaults to 17001.
Backup Agent model number	Name to identify the Backup Agent. Defaults to Backup if not specified. (Applies to Axeda Agents only, not to IDM Agents.)
Backup agent serial number separator	The character that separates the model number and serial number in the backup agent serial number. The default is @@.
Bad or Uncertain or Empty data item display value	The value that the system will display when the actual value for a data value is uncertain, bad, or empty data value. By default, the system displays a question mark, “?”, for data of this type.

System Configuration Properties *(continued...)*

Property	Description
Bind address for AWP file transfer TCP listener	Specifies where the AWP endpoint listens for file transfer data from AWP devices. Identifies which network interfaces are listened on if a host should have more than one Network interface card (NIC). The value 0.0.0.0, or no value at all, specifies all available network interfaces.
Bind address for AWP messaging TCP listener	Specifies where the AWP endpoint listens for incoming messages from AWP devices. Identifies which which network interfaces are listened on if a host should have more than one Network interface card (NIC). The value 0.0.0.0, or no value at all, specifies all available network interfaces.
Bind address for ASMP/ AWP file transferTCP listener	Specifies where the ASMP/AWP endpoint listens for incoming file transfer messages from ASMP/AWP devices. This address is the one that the listener actually binds to. Identifies which network interfaces are listened on if a host should have more than one Network interface card (NIC). The value 0.0.0.0, or no value at all, specifies all available network interfaces.
Bind address for ASMP/ AWP messaging TCP listener	Specifies where the ASMP/AWP endpoint listens for incoming messages from ASMP/ AWP devices. Identifies which which network interfaces are listened on if a host should have more than one Network interface card (NIC). The value 0.0.0.0, or no value at all, specifies all available network interfaces.
Bind address for Enfora UDP listener	Specifies where the Enfora endpoint listens for incoming messages from Enfora devices. Identifies which which network interfaces are listened on if a host should have more than one Network interface card (NIC). The value 0.0.0.0, or no value at all, specifies all available network interfaces.
Build Number	The version, and number, date and time of this ServiceLink build, which is set during the installation. Unless instructed to do so (for example, during an upgrade to a Service Pack), you do not need to modify this setting.You will need it when contacting Technical Support to help identify the version of software you are running.
Cache expiration frequency (seconds)	The number of seconds that the expiry invalidator waits between runs of its invalidator.
Case Number Prefix	A prefix for the system to use when creating Case Numbers.
Case Number Suffix	A suffix for the system to use when creating Case Numbers.
Configuration for hosting preparation folder path	The path to the user branding folder on the Axeda Enterprise server. The path should point to the “public” domain. For example: `com.axeda.drm.webapp.asset.device.module.public.folder.path = C:/ServiceLink/applications/servicelink.ear/public.war/styles/`
Configuration for specifying the ‘from address’ for Email Transport	The “from” address when sending an e-mail message (M2M).
Custom Build Information	Derived from the CustomConfigInfo.properties file (if it exists), displays information about the custom configuration.

System Configuration Properties *(continued...)*

Property	Description
Data source name	Axeda offers a stand-alone program called Adapter to gather the data and communicate with the Enterprise server through a TCP socket. The port and host properties tell the Enterprise system on which host and port the Adapter process is listening. For the port, type the number on which to access the remote data source. For the host, ONLY IF the remote data source is running on a separate node, un-comment the line and type the IP address of the node where the remote data source is running.
Database Product Name	Shows the database product configured for the system as “Oracle”.
Date format	A date format for the system to use, using Java date format strings. By default the data export uses the date format specified by the user’s locale. If the user has not specified a locale, the server’s default locale is used. For details on date format strings, refer to the JavaDoc for `java.text.SimpleDateFormat`
Days before alarms are acknowledged	The number of days after which all alarms will be acknowledged automatically. A number less than 1 (the default, -1) indicates that alarms are not to be acknowledged automatically.
Days to persist statuses in database	The number of days that the server should maintain asset command statuses in the database. Statuses older than this number of days will be deleted automatically from the database. The default number of days is 3.
Default Agent version	The version of the Axeda Agent to display in the Asset dashboard of the Applications UI. If the agent version value is not available in the Enterprise system, the server displays the agent version defined in this property. By default, the value is <blank>. In addition to being informational, this property also guides some server processes. This value is set based on the type of agents with which the server will communicate: • Firewall-Friendly agents - The set value is applied as the default version; for example, 6.5. • Wireless agents - This property should be left blank. • Both agent types - If the property is left blank, the system will work to distinguish the type of agents posting data. ***Important!*** *If this property is left blank, the server will apply the version “M2M” to any agent that does not supply a version.*
Default Audit filtering date range days	The number of days that the Audit filtering date range filters default to when the date range is not specified for a search. The default is 7 days.
Default chart	The chart that you want to display as the default chart for data. Other settings include: • Default Live Chart • Default History Comparison Chart • Default Bar Comparison Chart
Default e-mail encoding	Type of encoding to use as the default for e-mail messages. The default is UTF-8. Other possibilities include ASCII, UTF-16, ISO8859, and so on. A complete list is available in the Preferences page of the Axeda Applications. The type of encoding you select must be supported by your e-mail server and client applications.

System Configuration Properties *(continued...)*

Property	Description
Default gateway location and Organization inheritance	Defines the behavior for location and organization inheritance by managed devices of a Gateway. If true, the inheritance will be enabled by default, meaning Configuration application users will be able to select (via the “Set this organization and location for all managed devices” check box) that the managed devices of a Gateway inherit the location and organization of that Gateway upon registration. If false, the check box is disabled, preventing a Configuration application user from selecting it to enable inheritance for Gateways. By default this value is set to true.
Default missing device additional factor	The number of seconds to use in the equation for determining that assets are missing. The default is 10 seconds.
Default missing device ping multiplier	An integer to use in the equation that determines when the system should consider that assets are missing. The following equation is used to make this decision: missing = current-time > last-contact + ping-rate * ping-multiplier + additional factor
Default partner login session duration in minutes	The duration for this session, which is the number of minutes from when the session is created until it expires. During this period, no one else may log in to the server using the code created for this session. The default is 2880 minutes, or 48 hours (2 days).
Desktop Viewer download location on Linux client	Location on a Linux client where Quick Launch will download and run the version of Desktop Viewer required for a remote session with the Desktop Server running on a remote asset. By default, /opt/Axeda/Desktop/Viewers.
Desktop Viewer download location on Windows client	Location on a Windows client where Quick Launch will download and run the version of Desktop Viewer required for a remote session with the Desktop Server running on a remote asset. By default, c:\Program Files\Axeda\Desktop\Viewers.
Devcon cache synchronization delay	Number of seconds between synchronizations of the asset context cache with the database.
Device communication maintenance enable flag	If true, enables the maintenance ping manager; if false, disables the maintenance ping manager.
Device communication maintenance ping agent url	The URL where you want the agents to send their maintenance pings (when the Enterprise Server has placed them in maintenance mode).
Device communication maintenance ping delay	The number of minutes to wait between maintenance pings.
Device communication maintenance ping owner	The JNDI name of the data source as configured on the Enterprise Server to which agent maintenance pings are being redirected.
Device communication maintenance ping rate	The number of seconds to wait between sending maintenance pings (from the agent to the Enterprise Server).
Device communication maintenance ping re-direct ServiceLink url	The URL of the Enterprise Server to which the agent maintenance pings are being redirected.
Device communication notification display source	if true, notifications sent to the server administrator will identify the source of the errors (for example, an XML posting from a specific agent); if false (or blank), notifications will not show the source of the error. Default is true.
Device communication notification interval in minutes	The number of minutes to wait before sending an e-mail message to the server administrator. Leaving the parameter blank or specifying a negative number disables the property completely. The e-mail address used is that defined in `com.axeda.drm.administrator.email`

System Configuration Properties *(continued...)*

Property	Description
Device communication notification maximum e-mail length	The maximum number of bytes for an e-mail message. The default value (10000) limits the size of e-mail messages to 10K. To allow unlimited-length messages, use a setting of -1.
Device condition synchronization process setting	The process missing device task synchronizes the device condition with device missing status if the flag is true. The process does not synchronize the device condition with device missing status if the flag is false. The default is true.
Device update synchronization delay	Number of seconds between checks by the asset context cache for asset updates in the database.
Device Updates export root	The server directory to which the server saves the tar .gz file intended for export to a specified asset during an Axeda Transport - Export session. This file contains all queued server commands and eMessages, as well as any pending actions or download instructions for the asset. The file for export is stored in a new subdirectory named for the export session.
Device Updates import root	The server directory to which the server will save files imported from a specified asset during an Axeda Transport - Import session. The server store the imported file to a new subdirectory named for the import session.
Direct protocols allowed	True (default) for the server to accept direct protocol connections. (The agent uses the “direct connect” protocol in remote sessions.) False for the server to prohibit direct protocol connections from agents and ignore the following direct connect properties: *directConnectPort* and *directConnectSSLPort*.
Disable notification on device registration	True to include all newly registered assets in notifications for all users. False is the default setting, which means that all newly registered assets are excluded from notifications for all users.
Display Path	The path where displays created using Axeda Builder are stored for access from the Service application.
Duplicate data item value check	Indicates if the system inserts duplicate data items that have the same timestamp. If true, the system will process the duplicate data items that have the same timestamp. If false (the default), the system will not process the duplicate timestamp data item messages.
E-mail server	Name of e-mail server to use for sending e-mail messages. Specify the complete server path; for example, `usmail2.Axeda.com`.
eMessage persistent connection	Specifies whether or not to require a persistent HTTP connection: • False (default) to not require a persistent HTTP connection (HTTP 1.1 only) • True if you are using HTTP 1.1 and require a persistent HTTP connection.
eMessage timeout	The number of seconds that the Enterprise server waits before closing the connection to the asset, allowing enough time for a message being sent from the asset to the Enterprise server to complete.
eMessage will overwrite device time zone	True (default) for the eMessage from the asset (registration message) to overwrite the setting for the asset’s time zone (as stored in the Enterprise server database).
Enable alarm rules	True to enable the processing of alarm triggers (default), or false to disable processing. Note: If you are not going to need these triggers, set this to false to improve system performance.

System Configuration Properties *(continued...)*

Property	Description
Enable data rules	True to enable the processing of data triggers (default), or false to disable the processing. *Note: If you are not going to need these triggers, set this to false to improve system performance.*
Enable Cross-Site Scripting (XSS) Filter	If True (the default), the XSS filter servlet is enabled and will scan for cross-site scripting (XSS) exploits. The filter will use a RegEx-based approach to detect attempted exploits. When the filter is enabled, all requests must meet the following criteria or they will be prevented from accessing the server: • The URI must be present in the Whitelist (defined by the property “XSS white list file name”) • The request must be in the form POST executed during a valid WizardContext • The parameter being inspected must be one of a set of "known" URL constants, which are derived from the *QueryParameter* and MruKey classes. In the event that an exploit has been detected, the server will log the attempt and log out the related user. If False, Cross-Site Scripting filter is disabled.
Enable/Disable Extended UI Module Feature	True if the Platform supports Extended UI Modules; false if the Platform does not support Extended UI Modules. The default is true.
Extended UI Module load timeout	Specifies the number of seconds during which time the server will attempt to load an extended UI module before it times out. The default is 30 (seconds).
Enable forgot password feature	True (default) sets the reset password link as visible.
Enable registration rules	True to enable the processing of asset registration events as triggers (default), or false to disable the processing. Note: If you are not going to need these triggers, set this to false to improve system performance.
Enable schedule rules	True to enable schedule triggers; false to disable schedule triggers (default). Note: If you are not going to need these triggers, set this to false to improve system performance.
Enable SOAP status rules	True to enable the processing of SOAP status events as triggers (default), or false to disable the processing. *Note: If you are not going to need these triggers, set this to false to improve system performance.*
Enable Soundex Feature	False (default) to disable Soundex functionality for searching for and displaying data; True to enable the server to implement Soundex functionality when searching the database.
Enable the SFTP server funtionality	Enable the SFTP server functionality.
Enable writing data to file should processing fail	If true, data that could not be inserted in the database is saved to a backup file; if false, the data is not saved if the database insert fails. Default is false (data not saved to backup file).
Endpoint of the ActiveMQ instance, in URI form	The endpoint of the ActiveMQ instance, in the form of a URI. The default setting is tcp://localhost:61616.

System Configuration Properties *(continued...)*

Property	Description
Endpoint to connect to ActiveMQ JMX, in URI form	The endpoint to connect to ActiveMQ JMX, in URI form. The default setting is `service:jmx:rmi:///jndi/rmi://localhost:1099/jmxrmi`. If the machine running ActiveMQ is not the same as the machine running the Enterprise server, replace `localhost` with the name of the machine where ActiveMQ is running. Otherwise, keep this setting as is.
Enterprise Server host name	The name of the cluster that this Axeda Enterprise server belongs to. This name does not need to correspond to a machine name. All Axeda Enterprise servers that communicate with the same database (that is, are in the same cluster) must have the same name. Each cluster must have a unique name. Note that the pound sign (#) is a reserved character and should not be used in the name. The name specified here does not have to correspond to a machine name. ***Important!*** *This value must be set for the server to start up. On start up, the server now ensures that critical properties are set (currently, there are only two - this one and the com.axeda.drm.db.dataSource property). If they are not, the server will not start.*
ESS default protocol URI	The default URI for the ESS protocol.
ESS JMS message TTL in milliseconds	The number of milliseconds that a JMS message is allowed to remain alive. The default value is 20 minutes.
Event subscription Queue Cleanup thread frequency in seconds	The number of minutes that the Reaper thread waits between each check for subscriptions that have expired. Each time it finds expired subsriptions, it deletes them. The default value is 1800 seconds (30 minutes).
Event subscription Queue Time-To-Live in seconds	The number of minutes that a subscription is allowed to remain alive. The default value is 1200 seconds (20 minutes).
Exclude default group from notifications	True to exclude all users from asset group security-based notifications who belong to default asset group only, for a specific model. False to include all users show are defined only in default asset group for particular model. True is the default setting, which means if a user is included in the default asset group for a model and in no other asset group settings for that mode, that user will not receive notifications for the related asset.
Extended UI Module load timeout	Specifies the number of seconds during which time the Platform will attempt to load an extended UI module before it times out. The default is 30 (seconds).
Extension of the file used to store data should an insert fail	If the server is set to save data to a backup file when it can't insert that data in the database, it will save that data to a file of this type, and create that file if needed. For example. *csv* or *txt*. Make sure `com.axeda.drm.data.failed_insert.enable` is set to `true`.
File download base directory	The path to the download directory for the Enterprise server.
File upload base directory	The path to the upload directory for the Enterprise server. Be sure to use forward slashes in the path, no matter which operating system is hosting your Enterprise Server.
Filter non-ascii characters from device data	True to enable the filtering of non-ASCII characters or false to disable filtering.
Filter substitute character	The character that replaces non-ASCII characters when filtering is enabled.

System Configuration Properties *(continued...)*

Property	Description
Forced ping interval	The maximum amount of time allowed for a managed asset to be silent (that is, not sending messages to the Axeda Enterprise server). Normally, when a managed asset has no data to send, the Axeda Agent managing that asset sends a brief ping message based on a configured ping rate. However, if a managed asset is deleted on the Enterprise server and the agent sends no data for that asset, the asset becomes hidden such that it exists, from the agent's perspective, but is not visible in the Enterprise server. Note: To make a hidden asset reappear, the agent must send an explicit message (a forced ping) on behalf of the asset, so that the Enterprise server can re-register it.
Frequency threads for poll for updates in milliseconds	Default is 500 milliseconds.
Global Access Server activity monitor cleanup period	The number of hours that the Activity Monitor will wait before cleaning out inactive sessions. Identifies how frequently the activity monitor runs and cleans up (removes) unused or abandoned sessions. The default is every 720 (seconds).
Global Access Server agent serial	The serial number of the Agent that has been deployed on the Remote Server.
Global Access Server auto register	True to allow remote servers to register themselves with the Axeda Enterprise server; false to require that someone register them manually.
Global Access Server determined by the user's time zone	True to use the user's time zone to determine which Global Access Server (GAS) to use; false (default) to find the GAS using the default algorithm. The default algorithm uses the time zone offset value of the GAS and the asset to determine their geographical location. The algorithm then uses the geographical location, the current load, and maximum supported load to determine the GAS to use.
Global Access Server DNS name (IP) usable by all users	An IP address that all users can access for Remote Sessions.
Global Access Server external address	An IP address that can be used for Remote Sessions from machines that are not running Axeda Agents.
Global Access Server hostname that the user connects to	True (default) to allow the remote server user connect url to be visible.
Global Access Server internal name	A user-friendly name to display for the server. The default value is "Internal".
Global Access Server log path	The path in which to store Terminal audit sessions. If this path is empty of invalid, the audit sessions are not stored. Example: `/usr/local/servicelink/sessionlogs`
Global Access Server max. sessions	The maximum number of sessions to allow on this server. To specify an unlimited number of sessions, type 0 here. The default is 10.
Global Access Server name of host to be used exclusively for all remote sessions	The IP address of the host that will be used exclusively for Remote Sessions.
Global Access Server proxy name	IP address or the host name of the proxy server that the Global Access Server will use to access the Axeda Enterprise server.

System Configuration Properties *(continued...)*

Property	Description
Global Access Server proxy port	The number of the port on the proxy server that the Global Access Server will use when accessing the Axeda Enterprise server.
Global Access Server uses SSL	True to enable SSL for the Global Access Server (GAS); false (default) to disable SSL for it.
Global Access Server web service name	True to enable Web Services for the Global Application Server (GAS); false (default) to disable Web Services for it.
Google API Key	Defines the Google Map Key. (Google Maps are used in the Map module of an Asset dashboard.) If this key is not present, you will not be able to use the Map module.
Google client ID for Premier Service	Client ID needed to use Google Premier Service.
Ignore eMessage Duration	Number of minutes after startup during which time the Enterprise server ignores messages from agents. The default is 0 (no messages are ignored).
Inactivity period for ABS monitoring task	The number of minutes that the Enterprise server waits without communication from the Application Bridge Server (ABS) before setting the status of the ABS to Offline.
Inactivity period for GAS monitoring task	The number of minutes that the Enterprise server waits without communication from the Global Access Server (GAS) before setting the status of the GAS to Offline.
Instantiator start-up file	Name of the XML configuration file for the Scheduler. The Instantiator reads this file for the Scheduler.
Integration Queue Message TTL, 0=indefinite	Specifies the messaging TTL for the integration queue. The default setting is 60 minutes, meaning a message will remain in the queue for 60 minutes; after which, that message will be removed from the queue. Any positive value is supported.
Integration Queue Message DeliveryMode 1=non-persistent, 2=persistent	Identifies whether or not queued messages are persisted upon server or AMQ restarts. The supported values are: 1 - the queue delivery mode is not persistent 2 - the queue delivery mode is persistent. By default, the integration queue persists messages (1). *Tip: If you plan a server maintenance period that will result in a long downtime for the server and you want message persistence, you should consider bumping this value so that persisted messages will be available when the maintenance is complete.*
Internal Global Access Server description	A user-friendly description to display for the server. The default value is “Internal Access Server”.
Is Expression Rules Monitor enabled?	Whether to enable or disable the monitoring of Expression Rules for recursion. The monitor tracks the executions of Expression Rules to determine which rules are recursive. The default value is “true,” which enables the monitor. If you do not want to use this monitor, set this property to “false.”
JSP page to use for Remote Application sessions	The path to the JSP page that you want to use for Remote Application sessions. The default is launch/application.jsp, and should not be changed.
JSP page to use for RemoteTerminal sessions	The path to the JSP page that you want to use for Remote Terminal sessions. The default is launch/terminal.jsp. If you create your own JSP page, be sure to store it in the launch directory and put its name here.
Key to use when encrypting an external credential	This property should be set to a unique 16-character string. This feature does NOT impact the local credentials that provide access to this Platform. External Credentials are accessed via Custom Objects for use with external systems.

System Configuration Properties *(continued...)*

Property	Description
LDAP Admin group name	Identifies the name of the LDAP group in which LDAP administrators are defined. Only users defined in this group can edit LDAP settings (for Sun ONE servers only).
Lightweight Ping servlet enabled	True (the default) to enable the Lightweight ping V1 servlet; False to disable the ping servlet
Lightweight Ping servlet host	The IP address or hostname of the Lightweight ping V1 servlet. If unspecified, the Agents use the same IP/hostname defined for the main message servlet.
Lightweight Ping servlet port	The port number of the Lightweight ping V1 servlet. If unspecified, the Agents use the port defined for the main message servlet.
Lightweight Ping servlet port path	The path of the Lightweight ping V1 servlet on the server. The default is /lwPing.
Lightweight Ping servlet uses HTTPS	True to make the Lightweight ping V1 servlet accessible through HTTPS. False to use HTTP. If unspecified, the Agents use the communication protocol defined for the main message servlet (eMessage).

System Configuration Properties *(continued...)*

Property	Description
List of package deployment error codes that should trigger a retry of the package deployment.	Identifies which agent package deployment statuses will cause the Platform to retry package deployments. These are the possible errors codes that may be sent from an asset when package deployment for that asset has failed. Multiple error codes (identified by number in a comma-separated list) can be defined to trigger package retries. Possible values are from 0 to 27, as follows: 0 : failed 1 : version 2 : bad-format 3 : unknown-soap-method 4 : unsupported-function 5 : dataitem-not-found 6 : registry-name-not-found 7 : registry-file-read-error 8 : invalid-dependency-expression 9 : no-files-found 10 : some-files-not-found 11 : download-execution-failure 12 : archive-error 13 : read-error 14 : http-status-error 15 : checksum-error 16 : connection-failure 17 : socks-failure 18 : http-failure 19 : ssl-failure 20 : agent-shutdown 21 : download-checksum-error 22 : partial-file-missing 23 : invalid-directory 24 : restart-of-gateway-device 25 : soap-function-error 27 : multifile-uncompressed The default error codes for retries are *14,15,16,17,18,19,21* (Http Status Error, Checksum error, Connection failure, Socks failure, Http failure, SSL failure, Download Checksum error)
Listen port for AWP file transfer TCP listener	Specifies the port on which the AWP endpoint listens forincoming file transfer messages from AWP devices.
Listen port for AWP messaging TCP listener	Specifies the port on which the AWP endpoint listens for incoming messages from AWP devices.
Listen port for ASMP/AWP file transfer TCP listener	Specifies the port on which the ASMP/AWP endpoint listens forincoming file transfer data from ASMP/AWP devices. NOTE: This value must match the value of the property, “Server port that gets reported to ASMP/AWP devices in SCM package upload/ download instructions“ (`com.axeda.drm.scm.asmp.awp.file-transfer.server-port`).
Listen port for ASMP/AWP messaging TCP listener	Specifies the port on which the ASMP/AWP endpoint listens for incoming messages from ASMP/AWP devices.

System Configuration Properties *(continued...)*

Property	Description
Listen port for Enfora UDP listener	Specifies the port on which the Enfora endpoint listens for file transfer data from UDP devices.
Maximum allowed AWP message size in bytes	Specifies the largest size of an AWP message, in bytes. The default value is 102400 bytes.
Maximum concurrent deployments per asset	The maximum number of deployments that can be in progress for a given asset at one time. The default is 2 deployments. When setting this property, note that Axeda Agents can only process a certain number of downloads at the same time. Set this property to a value lower than the agent's set download processing limit to ensure that download "slots" remain available for other agents. If this value is set higher than the agent's set download processing limit, a larger number of deployments may end up "in-progress", but still have to wait for the agent to complete the installation when the agent restarts."
Maximum delay between alarm inserts in seconds	Maximum number of seconds between alarm inserts.
Maximum delay between data inserts in seconds	Maximum number of seconds between data inserts.
Maximum delay between event inserts in seconds	Maximum number of seconds between event inserts.
Maximum delay between gateway managed asset map inserts in seconds	The maximum number of seconds between managed gateway device map and device offline updates in the temporary database tables. The default is 1 (second).
Maximum delay between last contact update inserts in seconds	Maximum number of seconds to allow between contact updates.
Maximum delay between location inserts in seconds	Maximum number of seconds between location inserts.
Maximum delay between package status inserts in seconds	Maximum number of seconds between package status message inserts.
Maximum delay between script inserts in seconds	Maximum number of seconds between script message inserts.
Maximum delay between state inserts in seconds	The maximum number of seconds between asset state inserts (in seconds). The default value is 1800 seconds.
Maximum delay between upload chunk updates in seconds	Maximum number of seconds between upload chunk updates.
Maximum delay to clear user group security after deleting usergroup in authentication server in hours	Maximum number of hours to delay clearing user group security after deleting usergroup in the authentication server. Set this value to 0 if the user group security is never removed from the system after deleting usergroup in the authentication server.
Maximum depth of the custom object call stack	This property places a limit on the number of nested custom object invocations. The default is 10.
Maximum file size of user uploaded SWF application.	The maximum size to allow for an uploaded SWF file, in bytes. The default size is 25MB.

System Configuration Properties *(continued...)*

Property	Description
Maximum number of concurrent event subscriptions	The maximum number of concurrent subscriptions. The default value is 1000. If the number of concurrent queues (subscriptions) exceeds this value, then an error is returned to the client application stating that no subscriptions can be created because the maximum number of concurrent subscriptions has been exceeded.
Maximum number of devices per event subscription	The maximum number of devices that a subscription can monitor. The default value is 100. If the number of devices requested exceeds this value, then an error is returned to the client application, stating that the maximum number of devices for the subscription has been exceeded.
Maximum number of rule monitors tracked at a time	The maximum number of rule monitors (recursion detection) that the Enterprise server can track at the same time in the LRU Expression Rule Monitor cache. The default value is 2000, which means that the Monitor can track up to 2000 expression rules at a time.
Maximum number of search results	Maximum number of rows for a set of search results to display on an application page (for a database search).
Maximum number of subfolders that can be created in the SCM uploads folder	The maximum number of subfolders that can be created in the scm/uploads folder. The default value is 30000. New scm/uploads folders are created based on a simple division calculation. The system divides the value of the DeviceID by the value of this property. (The DeviceID is assigned by the system the first time it registers.) It then appends the quotient to the newly created scm/uploads folder. For example, suppose only the scm/uploads folder has been needed. The subfolder limit is set to the default value, 30000, and files are uploaded by an asset whose DeviceID is 90000. At this point, the Enterprise server creates a new scm/uploads folder and the number that is created for that folder, based on the calculation, is 3. The new folder is scm/uploads3. This folder will contain another folder that is named for the DeviceID. That folder contains the actual uploaded file.
Maximum number of times to re-evaluate events	Maximum number of times to re-evaluate a Triggerable Event. This applies to the Reevaluate() function, available for configuration in Expression rules. The default, 10, ensures the does not run reevaluate more than 10 times. When the maximum limit is reached, a warning message is entered in the audit log.
Maximum queue size for inserting alarms	Maximum number of alarms that can be placed in the queue before the system starts discarding the oldest alarms.
Maximum queue size for inserting data items	Maximum number of data items that can be placed in the queue before the system starts discarding the oldest data items.
Maximum queue size for inserting events	Maximum number of events that can be placed in the queue before the system starts discarding the oldest events.
Maximum queue size for inserting gateway managed asset map in temporary table	The maximum number of gateway and managed asset mappings and offline/online messages that can be placed in the temp tables queue. The default is 10000.
Maximum queue size for inserting last contact updates	Maximum number of updates the queue can hold before the system starts discarding the oldest updates.
Maximum queue size for inserting locations	Maximum number of events that can be placed in the queue before the system starts discarding the oldest locations.

System Configuration Properties *(continued...)*

Property	Description
Maximum queue size for inserting package status messages	Maximum number of package status messages that can be placed in the queue before the system starts discarding the oldest package status messages.
Maximum queue size for inserting scripts	Maximum number of script messages that can be placed in the queue before the system starts discarding the oldest script messages.
Maximum queue size for inserting states	The maximum number of asset states that can be placed in the queue before the system starts discarding the oldest asset state.
Maximum queue size for upload chunk updates	Maximum number of upload chunk updates that can be placed in the queue before the system starts discarding the oldest upload chunk updates
Maximum rows from the Asset Event table to process at a time	This advanced configuration parameter sets the maximum number of elements that will be read from the asset event table during each run of the eligibility evaluation tasks. The default value is 1000.
Maximum rows from the Deployment Event table to process at a time	This advanced configuration parameter sets the maximum number of elements that will be read from the deployment event table during each run of the eligibility evaluation task. The default value is 10000.
Maximum rule result sequence length to be tracked	The maximum length of a sequence of rule evaluation results for recursion detection. For example, when a rule triggered, the results show which expression was run, the THEN expression or the ELSE expression. The default value is 5, which means that up to five rule results can be in the same sequence.
Minimum number of times a rule pattern needs to occur before it is considered to be recursive	The maximum number of times that a rule pattern needs to coccur before it is considered to be recursive. The default value is 5 times. When enabled, the Expression Rules Monitor keeps track of the evaluations of Expression Rules. A rule pattern is a sequence of rule results, describing which rules and expressions were triggered and in what sequence. In this context “recursive” means that the rule evaluation is repeating continuously, potentially in an infinite loop. .
Minimum ServiceLink User's password length	The minimum length of a user’s password
Missing device update frequency	The number of seconds to wait between checks for assets that are missing (offline) and returned (back online after having been missing). The default is 30 seconds.
Model profiles file system location	The file system location for any model profiles supported by the server. Profiles will be saved to this location, under a directory name that matches the name of the model profile. This value is specified during installation. The default location for this “model_profiles” directory is under the ServiceLink installation (for example, *C:\ServiceLink\model_profiles*). You can direct the server to access the model profiles from any location to which the server has access.
MRU maximum lines	The maximum number of lines to display when a select list is in enhanced mode.
MRU popup threshold	The number of lines at which the system will shorten the list to the value specified for max-lines-displayed. When the number of items in the select list is greater than or equal to this value, the system shortens the list and uses enhanced mode.
MRU size	The number of items to store in an MRU list. Because of the way popup windows work, 9 is the recommended value.
Name of the authenticator for partner logins	The name of the WebLogic Authenticator configured for the Partner Login store. For example, *IPlanetLDAPAuthenticator.* This is the name of the security realm set up in WebLogic. The default value is defined by the installer when Partner Login is configured.

System Configuration Properties *(continued...)*

Property	Description
Name of the file that holds the white list entries for web services	The name of the white list xml file.
Name of the file used to store data should a database insert fail	If the server is set to save data to a backup file when it can't insert that data in the database, it will save that data to a file of this name, and create that file if needed. Make sure `com.axeda.drm.data.failed_insert.enable` is set to `true`.
Name of the integration queue for this instance, in the form com.axeda.integration.<*customername*>.queue	The name of the integration queue for this instance, in the form, com.axeda.integration.<*customername*>.queue, where <*customername*> should be replaced with the name of the customer or client that will use the queue.
Name of the Key Management Algorithm	The name of the SSL algorithm for KeyStore and TrustManager. In keeping with the default selection of the BEA WebLogic Server, the default SSL algorithm select is SunX509. The IBMX509 algorithm for WebSphere is commented out. If you are using WebSphere, move the comment symbol (#) from the IBMX509 line to the SunX509 line to change the selection.
Name of the SSL Protocol used	The version of SSL protocol to use for SSL negotiation.
New thread for schedule rules	True to spawn a new thread to process each trigger (default); false to use same thread for each trigger. Keep in mind that the number of threads is related to system performance. You may need to tune this setting.
Notification tone files location	The location of tone files on the machine running the Axeda Enterprise server.
Notify administrator about partner login requests	True (default value) for the server to send e-mail requesting a session to the Enterprise server administrator e-mail address. False for the Enterprise server administrator to not receive these e-mails.
Number of device messages per last contact update	The number of asset messages that will cause the server to update an asset's last contact time. For example, if set to 10, the server updates an asset's last contact time when processing every 10th message from the asset. By default this value is 1, which causes the server to update the last contact time with each message received from an asset. Although increasing the value of this parameter helps improve the server's scalability, it also lengthens the amount of time required to detect that the asset is missing.
Number of minutes to track a sequence for recursion	The number of minutes to track a sequence of rules for recursion. The default value is 60 minutes (1 hour), which means that the Enterprise server will track a squence of expression rules for an hour to determine if the sequence is recursive.
Partner Login notification message	Identifies the message body for the e-mail message to send to the partner for a new case. Default is "Please visit: {0} and use the login code: {1} to access case number: {2} com.axeda.drm.partner.supportmessage=Partner Login information with login code {0}, was sent to {1}partner {2} for case number {3}.
Partner Login notification subject	Identifies the subject line for the e-mail message to send to the partner for a new case. Default is "Axeda ServiceLink Case {2} Access Support Information", for which {2} is replaced with the Case Number for the case.

System Configuration Properties *(continued...)*

Property	Description
Partner Login return address	Identifies the e-mail address of the sender for the e-mail message to send to the designated support personnel for a new case. The default address is: support@axeda.com.
Partner Login support message	Identifies the message body for the e-mail message to send to the designated support personnel for a new case. Default is “Partner Login information with access code {0}, was sent to {1} partner {2} for case number {3}.” In this example, {0} is replaced with the access login code the server created for the case, {1} is replaced with the name of the partner assigned to this case, {2} is replaced with the e-mail address of the partner assigned to this case, and {3} is replaced with the Case Number for the case.
Partner store class name	The kind of LDAP used as a Partner Login store. By default, the Partner Login store is set to the Directory Server chosen for Partner Login during installation (set by the property `com.axeda.drm.userVendor.LdapUserStoreFactory)`.
Password with access to ActiveMQ JMX	The password for the system to present to the event subscription queues for read and write operations. Do NOT change this value.
Password with read/write access to the integration queue	The password for the system to present to the integration queue for read and write operations. Do NOT change this value.
Path of the file used to store data should an insert fail	If the server is set to save data to a backup file when it can’t insert that data in the database, it will save that data to the backup file in this path, and create that file if needed. Make sure `com.axeda.drm.data.failed_insert.enable` is set to `true`.
Path to store terminal audit sessions	The path in which you want to store Remote Terminal audit sessions. If this path is empty or invalid, audit sessions are not stored. The example shows how to specify a path on a Windows server.
Ping rate for Global Access Server to notify they are alive	The rate (in seconds) at which Remote Servers will notify the Enterprise Server that they are “alive.”
Process bad quality data	False (default) to reject bad or uncertain data, or true to accept bad or uncertain data.
Remote activity monitor	False (default) to disable the activity monitor for remote sessions. True to enable the monitor. The Activity Monitor tracks sessions that were created and cleans up sessions that it determines are abandoned. If true, the activity monitor for the GAS is enabled; if false, the activity monitor is disabled.
Remote activity monitor period	How frequently the activity monitor runs to track all remote sessions for this GAS. During this operation, the activity monitor is watching each session. If it seems that a session may be abandoned (based on the value of `com.axeda.ras.activity-monitor.min-data-threshold)`, the activity monitor does not remove the session until the number of cleanup periods has been reached (as defined in `com.axeda.ras.activity-monitor.num-periods-forcleanup)`. While monitoring a potentially abandoned session, the activity monitor will run at the frequency specified here. The default is every 60 (seconds).
Remote Application maximum data buffer size	The maximum amount of data (in KB) that can be buffered on the Enterprise Server before further data posts are rejected. The default setting of -1 disables buffering on the Enterprise server.
Remote application secure web port	The number of the SSL port (default is 443) for Remote Application sessions.

System Configuration Properties *(continued...)*

Property	Description
Remote Application timeout	The number of seconds that an Agent getData request pauses to wait for data. If the time period is reached before data is received, the getData request is returned with a NO DATA value specified. This amount needs to be less than any proxy or bridge timeouts for HTTP GET requests (usually 40 to 45 seconds).
Remote Application user timeout	The number of seconds that a User getData request pauses to wait for data. If the time period is reached before data is received, the getData request is returned with a NO DATA value specified. This amount needs to be less than any proxy or bridge timeouts for HTTP GET requests (usually 40 to 45 seconds). Set this to a small value.
Remote data source Port	The remote.port and remote.host parameters support the import of non-ServiceLink data, such as external databases and @aGlance data servers. These parameters apply to a ServiceLink installation that is integrating such external data sources only; otherwise, they are ignored.
Remote session inactive timeout in seconds	The number of seconds before closing a session that is inactive (either from user or asset).
Remote session merge allowed	True (default) to allow remote sessions to merge or false to prevent remote sessions from merging.

System Configuration Properties *(continued...)*

Property	Description
Remote session start-up timeout in seconds	The number of seconds before a session that has not started is closed. This timeout must be greater than the asset Ping rate.
Remote Terminal request timeout	The number of seconds to wait for data from a user for an asset. If the time period is reached before data is received for the asset, the GET request is returned to the asset with a NO DATA specified. This amount needs to be less than any proxy or bridge timeouts for HTTP GET requests (usually 40-45 seconds).
Remote Terminal User request timeout	The number of seconds to wait for data from the asset, for the user. If the time period is reached before data is received for the user, the GET request is returned to the asset with a NO DATA specified. This amount needs to be less than any proxy or bridge timeouts for HTTP GET requests (usually 40-45 seconds). It is advised that you set this to a small value.
RemoteTerminal maximum data buffer size	The maximum amount of data (in KB) that can be buffered on the Enterprise Server before further data posts are rejected. The default setting of -1 disables buffering on the Enterprise server.
Root folder for Data Accumulator Bulk Data API. Please set this to a valid folder that can be reached by each node in your cluster. You will want to back up regularly.	The server will create the write-once files containing the accumulated device information to this folder. When requested (via Axeda API), the accumulated device information will be streamed from this folder. When the system receives a command to stream the data (for example, to an external FTP server), it will first merge the files in this location according to their individual timestamps and then provide the caller with a stream object for the accumulated data. It is recommended that you schedule this folder for backups. If you do not specify a root folder, the system default is to create the folder in a temp directory.
Schedule rules delay	The delay (in minutes) that the schedule thread waits between database queries for execution.
Schedule rules owners	Do not change. This setting retrieves the appropriate domain name and JDBC data source from the config.xml file.
Scheduler check pooled frequency	Number of milliseconds that the Scheduler waits between attempts to connect to the JDBC connection pool.
Scheduler maximum threads	Maximum number of threads for the Scheduler to use.
Scheduler retry frequency	Number of milliseconds that the Scheduler waits between attempts to connect to the Oracle database.
Scheduler uses JMS	When JMS is enabled, create a com.axeda.drm.scheduler, SchedulerTopic in WebLogic Server. By default this property is set to false (JMS disabled).
Scripting timeout	A number by which to multiply the ping rate in order for the server to determine when SOAP messages to an asset have timed out and the status of the script or timer should be changed. What the status is changed to depends upon which operation timed out. For example, an asset has a ping rate of one minute, and the default timeout factor of 5 is used. You attempt to register a timer on the asset, but the asset is offline. After 5 minutes, the timer will go from “waiting to register” to “register error”.
Seconds to wait for idle AWP clients before closing connection	30 seconds is the default number of seconds that the Enterprise server waits before closing a connection with an AWP client. If the value is 0, the server waits indefinitely.
Seconds to wait for idle AWP file transfer clients before closing connection	30 seconds is the default number of seconds that the Enterprise server waits before cloaing a connection with an AWP file transfer client. If the value is 0, the server waits indefinitely.

System Configuration Properties *(continued...)*

Property	Description
Seconds to wait for idle ASMP/AWP clients before closing connection	30 seconds is the default number of seconds that the Enterprise server waits before closing a connection with an ASMP/AWP client. If the value is 0, the server waits indefinitely.
Seconds to wait for idle ASMP/AWP file transfer clients before closing connection	30 seconds is the default number of seconds that the Enterprise server waits before cloaing a connection with an ASMP/AWP file transfer client. If the value is 0, the server waits indefinitely.
Server hostname that gets reported to AWP devices in SCM package upload/ download instructions	The name of the server host for SCM package uploads and downloads for AWP devices. This name is used in the SCM upload and download instructions. Typically this server is the same as the file transfer listener bind address, unless a load balancer is being used.
Server hostname that gets reported to ASMP/AWP devices in SCM package upload/download instructions	Tthe name of the server host for SCM package uploads and downloads for ASMP/AWP devices. This name is used in the SCM upload and download instructions. Typically this server is the same as the ASMP/AWP file transfer listener bind address, unless a load balancer is being used.
Server port for remote session communications	The number of the port on the Enterprise Server machine to use for Remote Session communications.
Server port for secure remote session communications	The number of the port on the Enterprise Server machine use when SSL encryption is required for Remote Sessions.
Server port that gets reported to AWP devices in SCM package upload/ download instructions	The server port of the server host for SCM package uploads and downloads for AWP devices. This port is used in the SCM upload and download instructions.
Server running in redundant-gateways mode	Redundant Gateway Functionality - multiple gateways can manage one device. If true, multiple gateways can manage one device; if false, one gateway manages one device.
Server port that gets reported to ASMP/AWP devices in SCM package upload/download instructions	The server port of the server host for SCM package uploads and downloads for ASMP/ AWP devices. This port is used in the SCM upload and download instructions. NOTE: This value must match the value of `com.axeda.drm.listeners.asmp.awp.file-transfer.listen-port.`.
Server to Server post rate	The rate, in seconds, at which to send out the queue of messages to the parent server. This defines how often the child server takes the list of messages that have queued up and sends them up using HTTP to the parent server.
Server to Server validate SSL certificate	If true, this Enterprise Server strictly validates all SSL certificates; if false, the server accepts any certificates.
Server to Server verify host name	If true, this Enterprise Server rejects certificates if the hostname in the certificate doesn't match the parent server name; if false, certificates are not checked against the hostname.
Service Application date navigation amount	An integer to set the number of steps backward in time that each click of the single arrow will take. The default setting is 1, so that the arrow moves back one step with each click. Thus, if data is updated once per minute, the setting of 1 here means that clicking the arrow results in the display of data going back 1 minute. If data is updated every 30 seconds, clicking the arrow results in the display of the last update.

System Configuration Properties *(continued...)*

Property	Description
Service Application date navigation big amount	An integer to set the number steps backward in time that each click of the double arrow will take. The default setting is 10, so if data is updated once every minute, clicking the double arrow results in the display of data going back 10 minutes. If data is updated every 30 seconds, clicking the arrow results in the display of data going back 5 minutes.
Service Application Device dashboard note display length	The number of lines for notes about assets in the Service application home page.
ServiceLink user's password expiration warning will be shown in (days)	By default, the Axeda Enterprise system warns users 5 days before their passwords are due to expire. If this property is set to -1, Axeda Enterprise does not check passwords for expiration.
ServiceLink user's passwords are expiring in (days)	By default, the user's password expires in 30 days. If you set this property to -1, the password expiration attribute will not be set.
Skinny Ping servlet enabled	True (the default) to enable the Enhanced ping servlet; False to disable the Enhanced ping servlet
Skinny Ping servlet host	True to make the Enhanced ping servlet accessible through HTTPS. False to use HTTP. If unspecified, the Agents use the communication protocol defined for the main emessage servlet.
Skinny Ping servlet port	The IP address or hostname of the Enhanced ping servlet. If unspecified, the Agents use the same IP/hostname defined for the main emessage servlet.
Skinny Ping servlet port path	The port number of the Enhanced ping servlet. If unspecified, the Agents use the port defined for the main emessage servlet.
Skinny Ping servlet uses HTTPS	The path of the Enhanced ping servlet on the server. The default is /\lwPingV2.
SLDAP SSL enabled	Directory Server setting for SSL, defines whether SSL is enabled for an LDAP directory server (com.axeda.drm.directory-server.ssl property)
Smart Suggest Interval	The interval at which the server searches the database using the currently specified search values. As the user types characters, the server updates the list of returned strings at a frequency defined by this setting. The default value, 1000 milliseconds, causes the server to query the database every 1000 milliseconds (1 second) using the currently specified search characters.
Smart Suggest max list size	The number of records that the server shows in the list of returned strings. The default value is 10 records.
Snapshot status 0 Snapshot status 1 Snapshot status 2 Snapshot status 3	The string in the snapshot XML file that will identify the level. The following levels are defined in the file: • name_0 = ok • name_1= info • name_2 = warning • name_3 = error

System Configuration Properties *(continued...)*

Property	Description
Snapshot status image 0 Snapshot status image 1 Snapshot status image 2 Snapshot status image 3	The image to display when an entry has the level specified by the name. The following images are defined in the file: • image_0 = snapshot_status_ok.gif • image_1 = snapshot_status_info.gif • image_2 = snapshot_status_warning.gif • image_3 = snapshot_status_error.gif
Snapshot status levels	The number of status levels to configure. Each status is identified by four values, followed by a number. The priority of the level is identified by the number at the end of the tag (0 is lowest priority). If a snapshot entry has no status, it is assigned the status identified by level 0 (the default).
Software Management agent initiated uploads require throttling	Indicates that the Platform should throttle agent initiated uploads (default).
Software Management Completion e-mail sender	E-mail address of the sender of notifications that a package deployment completed. By default, the value of this property is AxedaServiceLink. See also “Software Management Error e-mail sender.”
Software Management download chunk delay	Number of milliseconds for the Agent to wait before requesting the next chunk of a file.
Software Management download chunk delay for AWP devices	Number of milliseconds for an AWP agent to wait before requesting the next chunk of a file. If not set, the value of the “Software Management download chunk delay” property is used for AWP agents.
Software Management download chunk size	Number of bytes from a portion of a file to include in a single request.
Software Management download chunk size for AWP devices	Number of bytes from a portion of a file to include in a single request. If not set, the value of the “Software Management download chunk size” property is used for AWP agents.
Software Management download retry count	Maximum number of times that an Axeda Agent should try the download operation.
Software Management download retry count for AWP devices	Maximum number of times that an AWP agent should try the download operation. If not set, the value of the “Software Management download retry count” property is used for AWP agents.
Software Management download retry maximum delay	Maximum amount of time (in milliseconds) that the Agent should wait before retrying a download.
Software Management download retry maximum delay for AWP devices	Maximum amount of time (in milliseconds) that an AWP agent should wait before retrying a download. If not set, the value of the “Software Management download retry maximum delay” property is used for AWP agents.
Software Management download retry minimum delay	Minimum amount of time (in milliseconds) that the Agent should wait before retrying a download.
Software Management download retry minimum delay for AWP devices	Minimum amount of time (in milliseconds) that an AWP agent should wait before retrying a download. If not set, the value of the “Software Management download retry minimum delay” property is used for AWP agents.

System Configuration Properties *(continued...)*

Property	Description
Software Management download session length	Number of seconds that a file should be available for download.
Software Management download URL	URL for the directory in which you want to store files downloaded from the server to an Agent.
Software Management Error e-mail sender	E-mail address of the sender of notifications that a package deployment failed. By default, the value of this property is AxedaServiceLink. See also “Software Management Completion email sender.”
Software Management high compression threshold for downloads	The size of a file (in bytes) to be downloaded that will result in content compression being disabled automatically. The default setting is 2 GB. You cannot specify a value larger than 2GB. This setting overrides the file transfer options selected for a Software Management package.
Software Management high compression threshold for uploads	The size of a file (in bytes) to be uploaded that will result in content compression being disabled automatically. The default setting is 2 GB. You cannot specify a value larger than 2GB. This setting overrides the file transfer options selected for a Software Management package or in an upload action configured in the Agent project when the file to be transferred exceeds this threshold.
Software Management named instruction file root directory	The location where files that the user has uploaded to the server to be part of a named instruction set should be stored. This directory must exist before you start the server or use the Software Management application.
Software Management package root directory	The location where package files that the user has uploaded to the server to be part of a package should be stored. This directory must exist before you start the server or use the Software Management application.
Software Management retry count	Number of times that an Axeda Agent should try the upload operation.
Software Management retry timed out uploads	True to enable the retryUploadTimeouts or false to disable it (default). Disable retryUploadTimeouts if you find that Upload instructions are resulting in a continuous loop. The retryUploadTimeouts keeps track of the number of retries for each upload for each device and everytime it retries the upload, it checks the retry count. Use this property in conjunction with the retry count to limit the number of times an upload is retried.
Software Management temporary directory	The path to temporary space in which the Software Management application can store files. This directory must exist before you start the server or use the Software Management application.
Software Management timeout ping multiplier	Number of ping intervals the server waits before removing a deployed package that stays in the Pending state (that is, still on the Enterprise server, not deployed to the asset) from the deployment queue. The expectation is that, if an asset is missing and you deploy a package to it, you do *not* want that package be sent when the asset comes back online a day later. For example, if an asset pings the server every hour, and the timeout ping multiplier is 4, then a package will be timed out if it remains pending for four hours.
Software Management upload chunk delay	Number of milliseconds for the Agents to wait before sending the next chunk of a file.
Software Management upload chunk delay for AWP devices	Number of milliseconds for the AWP agents to wait before sending the next chunk of a file. If not set, the value of the “Software Management upload chunk delay” property is used for AWP agents.

System Configuration Properties *(continued...)*

Property	Description
Software Management upload chunk size	Number of bytes from a portion of a file to include in a single request.
Software Management upload chunk size for AWP devices	Number of bytes from a portion of a file to include in a single request. If not set, the value of the “Software Management upload chunk size” property is used for AWP agents.
Software Management upload chunk timeout threshold (seconds)	The time elapsed, in seconds, since last upload chunk after which associated package will be marked as timed out.
Software Management upload chunk timeout threshold for canceling paused transfers (seconds)	Time elapsed in minutes since last upload chunk after which associated paused package will be canceled (seconds).
Software Management upload keeping history	True to keep old copies of the files or false to overwrite the existing copies.

Software Management upload keeping history override	A comma-separated list of file hints that are exceptions to the keep-history rule set with the keep-history parameter.
	For example, if keep-history is true, then this list determines files that will NOT be kept when a file of the same name arrives. To keep all copies of all files except for the dependency files from the agents, you would set these parameters as follows:
	`upload.keep-history = true`
	`upload.keep-history.override = DependencyRegistry, MyCustomHint`

Software Management upload requires overall MD5 checksum	If true, MD5 checksum generation (and verification on client) is enabled for file uploads. If false (the default), MD5 checksum generation is disabled.
Software Management upload retry count	Maximum amount of time (in milliseconds) that the Agents should wait before retrying an upload.
Software Management upload retry count for AWP devices	Maximum amount of time (in milliseconds) that AWP agents should wait before retrying an upload. If not set, the value of the “Software Management upload retry count” property is used for AWP agents.
Software Management upload retry maximum delay	Maximum amount of time (in milliseconds) that the Agents should wait before retrying an upload.
Software Management upload retry maximum delay for AWP devices	Maximum amount of time (in milliseconds) that AWP Agents should wait before retrying an upload. If not set, the value of the “Software Management upload retry maximum delay” property is used for AWP agents.
Software Management upload retry minimum delay	Minimum amount of time (in milliseconds) that the Agents should wait before retrying an upload.

System Configuration Properties *(continued...)*

Property	Description
Software Management upload retry minimum delay for AWP devices	Minimum amount of time (in milliseconds) that AWP agents should wait before retrying an upload. If not set, the value of the “Software Management upload retry minimum delay” property is used for AWP agents.
Software Management upload root directory	The root directory for the files that will be uploaded by assets. The files are stored in subdirectories by asset ID. This directory must exist before you start the server or use the Software Management application.
Software Management upload session length	Number of seconds that a file should be available for upload.
Software Management Upload URL	URL at which the Enterprise Server accepts files uploaded by the Axeda Agents.
Software Management User’s Deployment security	True (default) to enable Software Management User’s Deployment security
Software Management validate IP	True to validate the IP addresses of assets when transferring files, or false to transfer files without validating the IP addresses.
Software Management default stall duration (in seconds) for non-polling assets	This is the default stall time delay for non-polling assets. Stall duration is primarily retrieved from the Model’s Model Profile, but if there is no stall duration defined for the model, then this property is used as the default stall duration. The default value for this property is 60 seconds.
Software Management delay (in hours) for marking deployment as Timeout	The amount of time that deployments may remain marked with the status of Stalled, Pending Ask, Agent Scheduled, or Preempted before being marked as Timeout. The default is 168 hours (1week).
Status of Event Subscription Queue cleanup thread	False to disable the Reaper thread (so that subscriptions are not destroyed automatically when they expire), or True (the default setting) to enable the Reaper thread, so that subscriptions are automatically removed periodically when they have expired.
Support Duplicate State for Alarms	True to enable the Duplicate state for Alarms. A “duplicate” alarm is defined as another instance of a current alarm (that is, an alarm that is in one of the following states: Started, Acknowledged, or Escalated); to be a duplicate, the alarm name and the asset that sent the alarm must be the same, When the Duplicate state is enabled, the existing “current” alarm remains, while the new instance is moved directly to Historical Alarms, with the state set to Duplicate. Duplicate alarms do NOT trigger expression rules, nor are they available for evaluation or processing in any business rule. False to disable the Duplicate state. When another instance of an alarm is detected by the Axeda Enterprise server, the “current” alarm is moved to Historical alarms, and the new instance becomes the “current” alarm. No changes are made to the original or new “current” alarms. The new instance of the alarm will
Support e-mail	By default, the e-mail address of Axeda’s Technical Support group. After installation, system administrators need to change this value to the e-mail address for your company’s technical support or services group.
Tenant Authenticator	The name of the WebLogicJBoss Authenticator configured for the Delegated Administration login store. For example, Delegated AdministrationIPlanet. This is the name of the security realm set up in WebLogicJBoss. The default value is defined by the installer when Delegated Administration LDAP is configured.

System Configuration Properties *(continued...)*

Property	Description
Tenant directory server	The IP address or hostname of the machine running your Delegated Administration directory server. This value is entered during the installation process. Example: Delegated AdministrationServer_1.axeda.com.
Tenant directory server admin search	Search information for locating administrators in the database of the Delegated Administration directory server.
Tenant directory server group search	Search information for locating groups in the database of the Delegated Administration directory server. This value is entered during the installation process.

System Configuration Properties *(continued...)*

Property	Description
Tenant directory server people search	Search information for locating users in the Delegated Administration directory server database. This value is entered during the installation process.
Tenant directory server port	The number of the port on the Delegated Administration LDAP directory server to use for Enteprise server communications. The standard port for LDAP directory servers is 389. This value is entered during the server installation process. NOTE: If you want to use SSL with your LDAP Sun ONE Directory Server, refer to *"Enabling SSL Encryption for Sun ONE/iPlanet Servers"* on page 48.
Tenant User store class name	The location of user information for Delegated Administraion. Do NOT change this setting.
The maximum amount of time in milliseconds that an event can take to process before the next item from the same group is processed	Identifies how frequently the server's queue clean-up task runs in the background to clear any events that may have been left in the filter. For example, if an event does not make a callback to the queue that event will be left in the queue.
The maximum length of array elements used while performing SCM related bulk SQL operations	Sets the maximum length for the array elements used during Platform operations related to Software Management. The default value is 25000 (maximum number of elements in the array).
The maximum number of application sessions allowed on this server	The maximum number of sessions to allow on this server. Zero (0) implies no limit.
The maximum number of eligibility chunk events that will be processed synchronously	This advanced configuration parameter sets the maximum number of distributed eligibility evaluation chunks that the eligibility evaluation task will run synchronously. This parameter is only valid when Eligibility Evaluation Mode is enabled. The default value is 1.
The maximum number of terminal sessions allowed on this server	The maximum number of sessions to allow on this server. Zero (0) implies no limit.
The maximum weight that can be processed in a single eligibility chunk event	This advanced configuration parameter sets the maximum amount of work that can get done in each chunk of the distributed eligibility evaluation. The default value is 2000.
The partner login support URL	The ServiceLink support URL used by the Partner Login sessions. This value is defined during the server installation process. Specify the complete ServiceLink server address; for example, `http://support.acme.com:1001`. This value is entered during server installation. *Note: Partners will need to access this URL; therefore, this address must be accessible outside the corporate firewall.*

System Configuration Properties *(continued...)*

Property	Description
The number of seconds a sequence of events that all originate from the same incoming message, is allowed to process across multiple threads before it is automatically terminated.	The number of seconds a sequence of events (processing on multiple threads) originating from a single event will run before the system terminates it. The default value is 300 seconds (5 minutes). A single event can create multiple downstream events. For example, a single data item message may cause 2 rules to run, each rule running 3 actions which create multiple objects whose values cause more rules to run, and so on. If this processing reaches the timeout value defined here, the server will not create any additional events. The server will create an audit message (to the Administration application - Audit log) indicating processing for the event terminated due to this execution policy violation (time violation). Also, the system will send notifications to the server administrator and to the user who last modified the rule.
The number of seconds an event is allowed to process on a single thread before it is automatically terminated.	The number of seconds a single event (processing on a single thread) will run before the system terminates it. The default value is 300 seconds (5 minutes). If the processing for a single event (such as a rule) takes longer to finish than the time alloted by this property, the system will stop processing the event which it reaches this this time limit. The server will create an audit message (to the Administration application - Audit log) indicating processing for the event terminated due to this execution policy violation (time violation). Also, the system will send notifications to the server administrator and to the user who last modified the rule.
The partner login support URL	http://localhost:7001
Time in seconds to await graceful thread-pool shutdown before interrupting	The default is 5 seconds.
Time Zone Offset for the internal access server	Used to set the timezone offset if the Global Access Server is in a different timezone from the Enterprise server. The Offset is defined as a number of hours ahead of or behind GMT. For example, -6:00 sets the time zone offset to six hours behind GMT (Central Standard Time).
Top logo on-click link page	Enables the company logo (displayed at the top of each Applications page) to link, typically to the Release Notes for the current release.
Truncate trailing zeroes for Numeric Data	True to truncate trailing zeroes after the decimal point for numeric data or false to preserve all trailing zeroes for numeric data.
Use primary authenticator for partner store (not recommended for production)	True for the primary authenticator for the Enterprise server to be used also for the partner store. Set this to “true” only when testing partner authentication in a development/staging environment. *Note: You MUST set this value to false for a production server.*
User alerts refresh rate	Time, in milliseconds (ms), between refreshes of notifications (user alerts). The default is 1200000 ms (20 minutes).
User connects to a different hostname of the Global Access Server than the agent	True (default) to allow the remote server user connect url to be visible.
User Login/Logout triggers enabled	True (default) means that when users log in or out, the resulting events will trigger configured expression rules. False means that these events will NOT trigger expression rules.

System Configuration Properties *(continued...)*

Property	Description
Username with read/write access to the integration queue	The user name that enables the Enterprise server to read and write to the integration queue (ActiveMQ) and the event subscription queues. Do NOT change this value.
User store administration enabled	Leave this setting at true to ensure the use of your directory server for ServiceLink access control.
User store administrator group name	For the system to recognize users as administrators, they must belong directly to the group specified by the `userStore.group.administrators` setting. For the system to allow access to users, they must belong to a group that belongs to the groups specified by the `userStore.group.users` setting. Note that since groups may contain sub-groups, the users must belong to a group that has DRMUsers (to use the default user group name) as an ancestor
User store class name	Change this setting ONLY if you are storing user information somewhere other than LDAP and have implemented your own UserStore and UserStoreFactory. For example, if you are using Microsoft Active Directory and you have implemented a UserStore and UserStoreFactory.
User store synchronization	True (default) to enable user store synchronization.
User store synchronization enabled at server startup	Enable (true) or disable (false) synchronization with the directory server on startup of the Enterprise Server.
User store user group name	The groups you have created within LDAP (or your custom user store) for the ServiceLink System.
User SWF Applications upload directory	The user name that enables the Enterprise server to read and write to the integration queue (ActiveMQ) and the event subscription queues. Do NOT change this value.
Username with access to ActiveMQ JMX	The user name that enables the Enterprise server to read and write to the integration queue (ActiveMQ) and the event subscription queues. Do NOT change this value.
WebServer factory class name	Identifies the Web Application Server Factory Class Name for the WAS you are using (BEA WebLogic Server or JBoss).
Web Resource root directory	The root directory where staging directories are created. This directory also stores Web Resource artifacts in the local repository. This directory must be an absolute path.
Web Resource socket connect read (in seconds)	Defines the read connection timeout (in seconds) used for WSDL downloads and Web Resource client web services requests. The default is 10 seconds.
Web Resource socket connect timeout (in seconds)	Defines the socket connect timeout (in seconds) used for WSDL downloads and Web Resource client web services requests. The default is 10 seconds.
Web service white list file name	Identifies the name of the web service white list file, which holds the white list entries for web services. Groovy scripts will be able to acess only the web services identified in this “white list”. If no white list file is defined here (or the file is defined but the contents of the actual file are inaccurate or formatted badly, etc.) then Groovy scripts will be able to access ALL Web services, without restriction.
XSS white list file name	Identifies the name of the white (permitted) list. This file contains the list of URIs and request parameters which are not to be inspected for exploits. To determine if the server checks for cross-site scripting exploits, see the property “Enable Cross-Site Scripting (XSS) Filter”.