Connectivity

Alliance Gateway 7.0

Functional Overview

March 2011

Table of Contents

1 Introduction

Alliance Gateway

Alliance Gateway is a software package that is installed on top of SWIFTNet Link. SWIFTNet Link provides the basic set of network connection services. Alliance Gateway enables application-to-application communication and facilitates connectivity to the SWIFT secure IP network.

Alliance Gateway can also act as a concentrator of SWIFTNet message flow, whereby multiple business users connect through Alliance Gateway to SWIFTNet. This is achieved by means of GUI applications deployed in Alliance Web Platform or service GUIs in Alliance WebStation designed to use the InterAct, FileAct, and Browse messaging services.

Alliance Gateway manages connectivity between customer applications and the SWIFT secure IP network by means of host adapters. Customers can use Alliance Gateway to concentrate the flow of messages between SWIFTNet and remote financial applications over Internet Protocol (IP) using the Remote API Host Adapter (RAHA), or by means of the MQ Host Adapter (MQHA).

Web-service applications can also connect to Alliance Gateway with the Web Services (SOAP) Host Adapter (WSHA), to exchange SOAP messages with other applications over SWIFTNet.

Web-service applications designed for use with SWIFTNet services using the https protocol can connect using the SOAP proxy.

Purpose of this document

The purpose of this document is to provide a description of the main functional enhancements for Alliance Gateway 7.0 as well as any functionality removed in this release.

2 Enhancements and Features

2.1 Alignment with SWIFTNet 7.0

Alliance Gateway 7.0 is aligned with SWIFTNet 7.0 and supports the following features:

- Message and file copy
- Message and file distribution
- Support for dynamic copy destinations
- Enhanced store-and-forward delivery options
- Session History Report
- Support for routing management using shared BIC operations
- Human password expiry enforcement
- Back-office support for delivery notification as system messages
- Enhanced HSM resilience and security
  - Support for additional boxes per cluster (maximum four)
  - Allow use of HSM certificates concurrently over multiple SWIFTNet Link instances
  - Avoid application certificate lock-out due to bad logins
  - Enable identification of HSM with two digits (e.g. HSM24)

Note The File Transfer Interface of Alliance Gateway 7.0 does not support the following SWIFTNet 7.0 features:
- Application Service Profile (ASP)
- Relationship Management Application (RMA)

For more information, see the *SWIFTNet 7.0 Release Overview.*

2.2 Backward Compatibility

Business applications developed to run with SWIFTNet Link 6.x can run with Alliance Gateway 7.0 by using the Remote API 6.0, 6.1 or 6.3.

Note Although Alliance Gateway 7.0 supports applications developed for SWIFTNet Link 6.0, you must nevertheless install SWIFTNet Link 7.0 before installing Alliance Gateway 7.0.

2.3 Silent Installation

Alliance Gateway 7.0 offers silent installation to ease the installation or upgrade process of Alliance Gateway. Using this feature significantly reduces the time required to perform the installation or upgrade of Alliance Gateway while reducing operational risks, in particular for customers with a large number of Alliance Gateway instances.

In addition to the existing GUI-based installation framework, Alliance Gateway provides the ability to perform a command-line installation based on a response file prepared in advance for easy execution. This approach allows unattended installations of multiple instances, avoids manual error and removes the need to open firewall ports for X-terminal usage.

Once executed, it is possible to find out through the exit code whether installation was successful. The details are logged in the installation.log file.

Furthermore, the use of a response file avoids any user interaction during the silent installation process: operations managers will be able to prepare the response files for different Alliance Gateway instances in advance, so that the actual software installation can be scripted or carried out potentially by other parts of the organisation. This supports segregation of duties (for example, when the operations managers do not have the required permissions to perform the installation).

Future Alliance Gateway 7.x patches will also support silent installation for easier patch deployment and will no longer mandate root permissions unless it is impossible to do otherwise (for example, upgrade of embedded third-party software).

2.4 Non-root Installation

For UNIX, Alliance Gateway 7.0 makes it possible for a non-root user to perform an installation or upgrade using the GUI or a silent process, provided that the root user performed some preliminary tasks. To complete the installation, the root user must perform some post-installation tasks.

Similar to silent installation, this capability allows segregation of duties between the root user and the person who installs the software for Alliance Gateway.

2.5 Upgrade on a New System

Alliance Gateway 7.0 allows during installation the prepared backup of an Alliance Gateway instance of a previous release level.

This is particularly useful for customers who want to use new systems when migrating to the next major release of Alliance Gateway.

This feature removes the need to re-install Alliance Gateway and manually reconfigure it as on the previous system.

Note This feature can only be used between two systems of the same operating systems (for example, only from Windows to Windows or from AIX to AIX).

2.6 Configuration Data Replication

Alliance Gateway 7.0 allows customers to replicate Alliance Gateway configuration data from one system to other similar Alliance Gateway instances.

To allow for easier management of configuration data, Alliance Gateway 7.0 provides command-line tools to support the export/import of selected configuration data into/from an external, user modifiable text file. This approach allows the following activities:

- Clone configuration data of an existing Alliance Gateway instance on an empty Alliance Gateway instance (for example, active/standby or multi active configuration)
- Merge the configuration data of an Alliance Gateway instance on another Alliance Gateway instance, which is already used for other applications
- Import the configuration data of an Alliance Gateway instance on another Alliance Gateway instance after manual modification of some configuration details (for example, to substitute a certificate's DN with those available on the target Alliance Gateway instance)
- Propagate configuration data changes from one active Alliance Gateway instance to Alliance Gateway instances on backup systems such as certificates and user passwords, message routing information, configuration parameters or event distribution.

Note Export/import commands require the installation of a Remote Adapter (RA) component. A local RA installation does not mandate the licensing of option 14: RA HOST ADAPTER while a remote RA installation does.

2.7 Integration of SWIFTNet Link Events into the Alliance Gateway Event Journal

Alliance Gateway 7.0 allows integration of SWIFTNet Link events (including HSM-related events introduced with SWIFTNet Link 7.0), within the Alliance Gateway Event Journal to offer a combined monitoring view of both SWIFTNet Link and Alliance Gateway applications.

Consequently, it is also possible to redirect SWIFTNet Link and HSM-related events through SNMP or log them in the system log.

2.8 Alliance Web Platform

Alliance Web Platform becomes the default user interface for Alliance Gateway. New features are implemented only for the Alliance Gateway Administration GUI on Alliance Web Platform while the SAG Admin GUI on Alliance WebStation remains available in maintenance mode (that is, no functional enhancements).

Several features introduced in the Alliance Gateway Administration GUI on Alliance Web Platform are therefore not available in the SAG Admin GUI on Alliance WebStation.

2.8.1 HSM Management GUI

The Alliance Gateway Administration GUI that runs on Alliance Web Platform includes the HSM Management GUI. Alliance Gateway 7.0 introduces this GUI to integrate the most frequently used HSM-related operational functions. Content previously in the Monitoring / Hardware Security Module of the Alliance Gateway Administration GUI is now part of the HSM Management GUI.

To use functions available in this GUI, you must upgrade the HSM firmware to software level 5.6.1 or above. An operating profile function **Show HSM Management GUI** is introduced to allow access to this GUI.

For more information about HSM firmware upgrade, see the *SWIFTNet Link 7.0 Installation Guide*.

Note This enhancement requires the availability of a Remote PED device and is available only in the Alliance Gateway Administration GUI of Alliance Web Platform. The HSM Management GUI is not supported through the SAG Admin GUI available with Alliance WebStation.

2.8.2 Alliance Gateway Re-licensing GUI

Alliance Gateway 7.0 allows the Alliance Gateway Administrator to update the Alliance Gateway licence through the Alliance Gateway Administration GUI within Alliance Web Platform.

As such, the licensing of optional features or BIC destinations no longer requires any intervention on the system itself. Furthermore, customers are able to remove licence options from an existing Alliance Gateway instance without having to physically access the system or be forced to reinstall the software. This may however requires some manual interventions to eliminate residual configuration data.

Thanks to the decoupling between the licensing and the installation framework, it is also possible to skip licensing activities during Alliance Gateway installation and perform them after installation using GUI-based re-licensing. This allows segregation of duties between system administrators and Security Officers.

Note The re-licensing GUI is provided onlyfor the Alliance Gateway Administration GUI within Alliance Web Platform. A local GUI-based utility remains available after Alliance Gateway installation and no longer requires the Alliance Gateway DVD.

2.8.3 Certificate Status

Alliance Gateway 7.0 includes a status for each certificate used. This status helps identify possible certificate-related issues or configuration not in line with general recommendations.

Note The certificate status is displayed only when using the Alliance Gateway Administration GUI in Alliance Web Platform.

In addition, whenever Alliance Gateway has to choose a certificate amongst a set of potential candidates (for example, equivalent certificates) it will prefer a certificate that is known as being valid based on the certificate status.

The introduction of certificate status also can be used to ease the development of applications in relaxed mode with regard to resiliency aspects. An application can provide a starting node (e.g. self-or-descendant (o=<bic8>,o=swift)) instead of referring to an explicit certificate and then Alliance Gateway selects the closest match which is operational based on the certificate status.

Note When a certificate is used for either relaxed mode purpose or for defining virtual SWIFTNet Users, it must be of policy type "Application" and not "Human". To enforce this policy, a new configuration parameter can be activated to prohibit configurations that do not respect this policy rule. In any case where the policy rule is not respected, the certificate status will be "Unexpected Certificate Policy". See section 2.14.1 for more details.

2.8.4 Supportability Enhancement

Alliance Gateway 7.0 provides system and integrity checks in the Alliance Gateway Administration GUI package on Alliance Web Platform to rapidly assess the Alliance Gateway environment:

The system check quickly determines if the operating system configuration is compliant with the SWIFT configuration requirements for Alliance Gateway. The system check page displays the actual configuration values found and the expected values. If the requirements are not met, then the information provided enables you to coordinate with your system administrator and take the actions required to make the alignments during scheduled maintenance.

The software integrity check verifies the integrity of the files for the installed Alliance Gateway software. The result of the check indicates whether any software files were added, removed, or updated.

The database integrity check verifies the integrity of the Alliance Gateway database. The result of the check indicates any problem detected. You can view entity-specific details for any check that failed.

Note that the online access to these commands is in addition to the existing command-line tools. Running software integrity and database integrity check use the existing operating profile function Run Integrity Check while there is the new Run System Check for the other one.

2.9 Enhanced End-user Certification Process

Alliance Gateway 7.0 offers a way to create or recover a SWIFTNet certificate by allowing the end user (that is, the certificate owner) to trigger the certification or recovery process and specify a password when logging in the first time, similar to what is done for virtual SWIFTNet users.

This approach still allows the Alliance Gateway Administrator to decide what the certificate name will be as well as its (HSM) location.

The certification process as available in previous Alliance Gateway releases also remains available for Alliance Gateway 7.0.

2.10 Approval for Certificate and Virtual SWIFTNet User Configuration

Alliance Gateway 7.0 allows segregation of tasks between Alliance Gateway operators who configure Alliance Gateway for use with certificates and the actual use of these certificates as approved by their owners. The approval of the configuration mandates the knowledge of the password.

This enhancement primarily concerns the following cases:

- Setting the relaxed SNL protocol for a real SWIFTNet user. This feature allows authorised applications to use the corresponding certificate for business purposes without the need to know the password of this certificate.
- Mapping a virtual SWIFTNet user with a certificate. This feature (also called “concentration of the PKI profiles”) allows a virtual SWIFTNet user to use this certificate for business purpose. It can also be seen as a mapping between virtual SWIFTNet users and real SWIFTNet users.
- Resetting the password of a virtual SWIFTNet user.

Note The approval feature is supported only through the Alliance Gateway Administration GUI on Alliance Web Platform. The existing mechanism of configuring and approving in a single operation remains available.

2.11 Configuration Parameters for Virtual SWIFTNet User Password Policy

Alliance Gateway 7.0 introduces configuration parameters to manage password policy settings for virtual SWIFTNet users. In past releases, the password policy settings applied equally to operators and virtual SWIFTNet users. Beginning with this release, a separate set of configuration parameters exists to allow defining values for password policy settings for virtual SWIFTNet users that are different from the values established for operators.

2.12 File Transfer Interface Enhancements

File Transfer Adapter (FTA) and File Transfer Integrated (FTI) support the following SWIFTNet 7.0 functionality:

- FileAct full copy: In addition to FileAct header copy, FTA and FTI can be used at the emission and reception ends of the FileAct copy flows, or as a central institution for Y-copy, as well as a third party for T-copy.
- SWIFTNet file distribution: FTA and FTI can be used to send a file (over store-and-forward) to a user-specified list of receivers.
- Dynamic copy destination: FTA and FTI allow including a user-specified list of values to identify alternative third parties to exchange files for services that use T-copy or Y-copy, as permitted by a service.
- Store-and-forward system recovery: In the exceptional case of a central disaster fallback, FTA and FTI will generate an Alliance Gateway event. FTA will prepare a store-and-forward recovery report for use by a business application (for potential files that need to be resent with a Possible Duplicate Emission indicator).

Note FTA and FTI are not enhanced in release 7.0 to support Relationship Management Application (RMA) and Application Service Profile (ASP). Also, there are no plans to further evolve FTA and FTI beyond release 7.0: they go into maintenance mode as of now.
In the mean time, customers who upgrade to release 7.0 can continue to use FTA/FTI for FileAct services that do not require RMA filtering. If you need to access FileAct services for which RMA is mandated, then we recommend you to migrate to Alliance Access.

Additionally, when acting as a Y-copy server (as in the case of a central institution), FTA and FTI do not automate resending of xsys.001.* messages and files submitted after the last replication status. As FTA and FTI do not comply with this new SWIFTNet 7.0 mandatory qualification test for messaging interfaces, FTA/FTI can no longer be used by Y-copy servers.

Alliance Access/Entry 7.0 as SWIFT's prime messaging interface supports all SWIFTNet 7.0 features and is a qualified FileAct messaging interface for SWIFTNet 7.0.

2.13 Licence Control

When a customer purchases Alliance Gateway, charges are determined in part by the extent to which Alliance Gateway is used within an organisation. Two factors, specified during installation by selecting the appropriate licence options, reflect such aspects:

- The maximum allowed number of concurrent users that may be connected to Alliance Gateway at a given moment.
- The number of messages per day that pass through Alliance Gateway. This does not include SNL API traffic from applications that are local to the Alliance Gateway host or traffic not intended to a production service.

To ensure that customers comply with the contractual obligations based on the Alliance Gateway licence options they purchased, Alliance Gateway 6.0 introduced checks for compliance in the following ways:

- Alliance Gateway 6.0 prohibited a user from connecting if the maximum concurrent user limit is exceeded. Alliance Gateway 6.0 counted Alliance Gateway operators and SWIFTNet users when calcuating the number of concurrent users. Alliance Gateway 6.0 also counted the number of Alliance WebStations connected to an Alliance Gateway instance.
- A reporting tool (the **sag_system -- statistics** command) was included to provide traffic statistics, which could be compared with the licensed traffic band.

In Alliance Gateway 7.0, the above mentioned capabilities have been reviewed for alignment with 7.0 licensing rules. In particular, note the following:

- Alliance Gateway 7.0 ensures that the control on the maximum number of concurrent users takes into account different users connecting through the Alliance Web Platform as well as any users who connect through individual WebStations. Also, Alliance Gateway operators are now excluded from the counting. The count of concurrent users considers only business users (real or virtual SWIFTNet users). The **sag_system -- concurrentusers** command provides information about the SWIFTNet users currently logged in to Alliance Gateway.
- In addition, the configuration parameter **ConcurrentUsersWarningLimit** can be used to log an event if the number of concurrent users that can still log in is equal to or less than this defined value. The maximum number of concurrent users that can connect to an Alliance Gateway instance is still determined by the value of the **MaxConcurrentWebStations** configuration parameter.
- In a production environment, the reporting tool only reports traffic intended to live services and excludes some SWIFTNet protocol-related messages.

2.14 Other Functional Enhancements

2.14.1 Enforced Use of Application-type Passwords

With Alliance Gateway 7.0, the use of application passwords can be enforced for virtual SWIFTNet users or certificates configured in relaxed mode.

The **EnforceApplicationPasswords** configuration parameter is introduced to control this behaviour and is set to Yes by default.

2.14.2 Enhanced Restore

With Alliance Gateway 7.0, the restore operation is enhanced to offer a choice whether to restore instance-specific configuration files (such as RA and WSHA configuration files, WSHA keystores, LDAP certificates on UNIX…) in addition to configuration data.

The command syntax for **sag_restore** includes an optional argument to allow restoring such files: `sag_restore <file_path_name> [-cfgfiles]`

This eases the default restore operations where the Alliance Gateway backup is restored on the same host when no environment settings have changed in between (e.g. IP or directory structure). If the restore occurs on a different system, some additional manual changes may be required, for example, to update network-related details.

2.14.3 Flexible Configuration of Entities

Alliance Gateway 7.0 configuration for message partners is more flexible than in previuos releases by allowing users to configure them independently of the status of related or unrelated subsystems (which was not always possible before).

For example, when MQHA is disabled or down, it is now possible to create or update a message partner that uses WebSphere MQ.

2.14.4 WSHA Integration

Alliance Gateway 7.0 includes Web services related functionality (19:WS HOST ADAPTER and 18:SOAP PROXY licence options) as part of the product installation. Such functionality is no longer provided as a separate add-on feature with separate distribution media.

For more information on Web services related functionality, see the *Alliance Gateway Web Services Host Adapter Configuration Guide*.

The functionality available in Alliance Gateway 7.0 is equivalent to the WSHA 6.1.60 delivery.

2.14.5 WSHA Keystore Re-initialisation

Alliance Gateway 7.0 introduces the **-reset** argument for the **sag_ws_keytool** command, which allows re-initialisation of the WSHA keystore.

This command is useful if, for example, you have lost the WSHA keystore password. Note in that case all the application certicates stored in the keystores are removed and must be reintroduced manually.

2.14.6 New sag_configmq Tool

When the MQ Host Adapter option is licensed post-installation or the directory location of the WebSphere MQ software changes, the **sag_configmq** tool can be used to provide necessary configuration details.

2.14.7 Software Upgrade Archives Completed File Transfers

Information related to completed file transfers is automatically archived as part of the upgrade to Alliance Gateway 7.0. You do not need to archive file transfers manually before the upgrade.

2.14.8 Enhancement to the sag_logreorganize Tool

As of Alliance Gateway 7.0, the **sag_logreorganize** tool includes the **-rebuildindex** parameter. Use of this parameter reorganises the database table space for indexes of the Event Journal.

It is recommended to always add this parameter when using this command, typically after a forced archive of the Event Journal.

2.14.9 Additional Default Message Partners and Endpoints

Alliance Gateway 7.0 installation or upgrade provides additional message partners and endpoints (fin_relaxed and sni_relaxed). These entities are created to ease the configuration of a messaging application designed in relaxed mode, such as Alliance Access.

2.14.10 SNL Events to Replace HSM Polling Status

As mentioned above ("Integration of SWIFTNet Link Events into the Alliance Gateway Event Journal" on page 6), Alliance Gateway can log SWIFTNet Link events. SWIFTNet Link 7.0 includes events related to monitoring HSMs and detecting failure. These SWIFTNet Link events will progressively replace the existing Alliance Gateway events related to HSM polling status. The difference with the existing Alliance Gateway events resides in the fact that they are logged when systematically calling the HSM to get its status, while the SWIFTNet Link events are triggered only when relevant.

To allow for a smooth transition period of HSM monitoring, the existing **HSMStatusPollingPeriod** configuration parameter of Alliance Gateway remains active and allows for an additional possible value which is -1. This value has a specific behaviour and is the default value for a new installation. When the configuration parameter is set to -1 and the HSM is a Luna box, Alliance Gateway will send Sw:SMAGetStatus to monitor HSMs every 60 minutes, while the HSMs of type Token are monitored at intervals of 10 minutes.

The other values of the **HSMStatusPollingPeriod** configuration parameter remain as in the previous releases of Alliance Gateway; for example the value 0 (zero) can be used to switch off the polling mechanism if needed.

The following event templates in Alliance Gateway are provided for the SNL events:

- Sag:SN-I 5603 HSM cluster(s) down
  Description: SECSRV003; at least one HSM cluster is down
  Details: HSM cluster(s) %1 is/are down. Detected by the monitoring.
  Content of %1 is the HSM cluster name(s)
- Sag:SN-I 5611 HSM box down
  Description: SECSRV011; HSM box detected down
  Details: HSM box %1 from cluster %2 is detected down.
  Content of %1 is IP address of the HSM box; content of %2 is cluster name

3 Obsolete Functionality

The following functionality is removed from or suppressed in this release of Alliance Gateway.

3.1 Alliance Starter Set

As a consequence of Alliance Gateway pricing model changes introduced for January 2011, the Alliance Starter Set ceases to exist in favor of a migration to Alliance Gateway 7.0. Except for the removal of dial-up access, all functionality generally remains available.

When Alliance Starter Set changes to Alliance Gateway, the Starter Set Administrator operator remains and becomes like any Alliance Gateway operator. The Starter_Set_Admin operating profile becomes visible and is treated like any user-defined operating profile. That operating profile no longer automatically receives operating profile functions added in subsequent releases.

The **sag_switchconnectiontype** tool is removed as a consequence of changing Alliance Starter Set to Alliance Gateway. The following configuration parameters are no longer present:

- **DialupDisconnect**
- **DialupIdleTimeOut**

3.2 Backup/Restore on Another Host

The introduction of this capability in Alliance Gateway 6.1.15 was to allow restoring an Alliance Gateway database backup on one operating system to a different operating system.

The introduction of the export / import configuration data with Alliance Gateway 7.0 provides a standard way to perform such operations and makes the functionality introduced in 6.1.15 as an interim solution obsolete.

3.3 Removal of Message Partner sabmp50

The WebStationmp message partner introduced with Alliance Gateway 6.0 replaces sabmp50.

The sabmp50 message partner was deprecated in Alliance Gateway 6.x. It is removed in Alliance Gateway 7.0.

3.4 Removal of Sag:SN-I:LogSNLResponseHeader Configuration Parameter

In Alliance Gateway 6.0, several event templates were enhanced so that they log only the important fields inside a received or sent SNL primitive thereby avoiding the truncation of the events when too long. As a consequence of this change, the **Sag:SN-I:LogSNLResponseHeader** configuration parameter is no longer meaningful.

The **Sag:SN-I:LogSNLResponseHeader** configuration parameter was deprecated in Alliance Gateway 6.0. It is removed in Alliance Gateway 7.0.

3.5 Removal of Sag:System:LoggingMode Configuration Parameter

Alliance Gateway 6.0 introduced performance improvement in event template caching. As a consequence of this change, the **Sag:System:LoggingMode** configuration parameter is no longer relevant.

The S**ag:System:LoggingMode** configuration parameter was deprecated in Alliance Gateway 6.0. It is removed in Alliance Gateway 7.0.

3.6 Replacement of sag_switchlogmode

Alliance Gateway 7.0 includes the **sag_configeventlog tool**, which provides a parameter **-switchlogmode**.

The **sag_switchlogmode** tool is removed in Alliance Gateway 7.0.

3.7 Obsolete GUI Features

In addition to moving the Monitoring / Hardware Security Module to the HSM Management GUI, the following features are also oboslete for the Alliance Gateway Administration GUI.

The Alliance WebStation node is removed. The configuration parameters Maximum Number of Concurrent Alliance WebStations and Alliance WebStation Disconnect Timeout are no longer present. These configuration parameters are renamed Maximum Number of Concurrent SWIFTNet Users and SWIFTNet User Disconnect Timeout, respectively, and are visible in the User Management / SWIFTNet Users node.

The nodes User Management / Local Security and User Management / SWIFTNet Users are no longer present. Instead, nodes are added for User Management / Operators and User Management / SWIFTNet Users. This change accommodates the introduction of configuration parameters specifically for virtual SWIFTNet user password policy management, in addition to the existing password policy configuration parameters that are now for operators only.

Legal Notices