GiAM System Security Data Feed Specification

ITID Identity & Access Management (ITID IAM)

27 January 2017

Version 7.10

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Status | Prepared by | **Comments** |
| 21-Oct-2011 | 3.0 | Draft | Manoj Sudarshan | **Milestone Version:** As part of the GAMD Onboarding initiative, this document has been standardized to support the needs of all GAMD initiatives. The major changes: Glossary Specification and SofD Rules Specification Sections added and aligned with requirements from GAMD initiatives. Replaced all references to GRMR tool with Access Governance tool. |
| 10-Nov-2011 | 4.0 | Draft | R. Kumar Rajah | Detail Reviewed and Updated. |
| 26-Nov-2011 | 5.0 | Draft | R. Kumar Rajah | Updated SofD Rule File Changes |
| 05-Dec-2011 | 5.1 | Draft | R. Kumar Rajah | Updated Orphan Accounts section with alternate correlation attributes |
| 07-Dec-2011 | 5.2 | Draft | R. Kumar Rajah | Extracted SofD Rule Specification sections out from this document |
| 11-Dec-2011 | 5.3 | Draft | Jared P Little | Updated Entitlement File with Account Source on Underlying Platform or Database |
| 13-Dec-2011 | 5.4 | Draft | R. Kumar Rajah | Updated Glossary section |
| 13-Dec-2011 | 6.0 | Draft | Manoj Sudarshan | Removed Section – 4.3.2: Entitlement File with Account Source on Underlying Platform or Database following discussion with Solutions. Baselined version. |
| 07-Feb-2012 | 7.0 | Baselined version | Manoj Sudarshan | Multiple updates. Added Appendix D for AD/ADAM based data feeds. Updated naming convention for Glossary file and added SBT # field to Glossary file schema to accommodate SofD requirement. |
| 08-Mar-2013 | 7.1 | Draft | Manoj Sudarshan | Multiple updates. Updated AD/AD LDS appendix section and moved into Section 6. Removed AD/Non-AD dual feed appendix based on feedback. Moved header file formats from Appendix A into Section 4. Removed note about support for limited HTML format for glossary. Updated note in Section 3.5 on removal of whitespaces in CSV files. |
| 21-Feb-2014 | 7.2 | Final | Jessica M Scott | Updates to Doc and Sample links and updates to section 6. |
| 24-Mar-2014 | 7.3 | Final | Jessica M Scott | Updated header row details – added note that double quotes are no longer required however system will accept both formats. |
| 15-May-2014 | 7.4 | Final | Jessica M Scott | Added Alternate ID info to Person ID field in section 4.1 accounts. |
| 18-Mar-2015 | 7.5 | Updated | Jessica M Scott | Updated link to guides. |
| 29-Sept-2015 | 7.6 | Updated | Jessica M Scott | Updated section 5.1.1 Glossary Feed Transmission to comply with updated policies and standards – stating updates are needed at least yearly. |
| 08-April-2016 | 7.7 | Updated | Jessica M Scott | Updated for SCPA |
| 13 April 2016 | 7.8 | Updated | Kendra L Troster | Updated section 6.0 to include note regarding nested groups. |
| 2 Sept 2016 | 7.9 | Updated | Paul Dawson | Added approvers; updated link to other docs |
| 27 Jan 2017 | 7.10 | Updated | Jessica M Scott | Updated Glossary section |

Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | E-mail | Date approved |
| Owner | Paul Dawson | pauldawson@hsbc.com | N/A |
| Preparer | Various | n/a | N/A |
| Approver | IT Security | rebecca.roberts@hsbcib.com |  |
| Approver | IT ID | andyhollingum@hsbc.com | 06-Sept-2016 |

**Table of Contents**

[1 Purpose 6](#_Toc447899502)

[2 Scope 6](#_Toc447899503)

[3 System Security Data Feed Overview 6](#_Toc447899504)

[3.1 System Security Data Feed 6](#_Toc447899505)

[3.2 Feed Transmission 7](#_Toc447899506)

[3.3 Header Record 7](#_Toc447899507)

[3.4 Trailer Record 8](#_Toc447899508)

[3.4.1 Trailer sample 8](#_Toc447899509)

[3.5 CSV Format 8](#_Toc447899510)

[4 Feed Files Schema 9](#_Toc447899511)

[4.1 Accounts 9](#_Toc447899512)

[4.1.1 Orphan Accounts 10](#_Toc447899513)

[4.2 Account Status Translation 11](#_Toc447899514)

[4.2.1 Active Accounts 11](#_Toc447899515)

[4.2.2 Disabled Accounts 11](#_Toc447899516)

[4.2.3 Account Status Mapping Examples 11](#_Toc447899517)

[4.2.4 Account File Sample: 12](#_Toc447899518)

[4.3 Entitlements 12](#_Toc447899519)

[4.3.1 Entitlement Collections 13](#_Toc447899520)

[4.3.2 Entitlement File Sample 13](#_Toc447899521)

[4.4 Security Model 14](#_Toc447899522)

[4.4.1 System Profile Hierarchy 14](#_Toc447899523)

[4.4.2 Security Model File Sample 15](#_Toc447899524)

[5 Glossary Data Feed Overview 15](#_Toc447899525)

[5.1 Glossary Data Feed Specification 15](#_Toc447899526)

[5.1.1 Glossary File Maintenance 16](#_Toc447899527)

[5.2 Glossary File Schema 16](#_Toc447899528)

[5.3 Glossary File Sample 17](#_Toc447899529)

[6 Data Feeds for Active Directory/AD LDS Application Entitlements 18](#_Toc447899530)

[6.1 Sample AD Glossary File 19](#_Toc447899531)

# Purpose

The purpose of this document is to provide the engineering specifications for the different access data loaded into the Global Identity and Access Management (GiAM) Tool which includes System Security Data Feed and Glossary (a.k.a Risk) files. This document contains consolidated data feed requirements from the following Identity & Access Management initiatives:

* Access Recertification
* Segregation of Duties (SofD)
* Transfers
* Application Leavers

# Scope

The scope of this document is limited to defining the specification of the System Security Data Feed and Glossary files for the GiAM tool.

# System Security Data Feed Overview

## System Security Data Feed

The System Security Data Feed contains text files that capture system security information for loading into the GiAM tool. The term “system” includes applications, platforms and databases. For a single system data feed, the security information is stored in three distinct files:

Figure 1: Files required in a System Security Data Feed

|  |  |
| --- | --- |
| **File** | **Description** |
| 🗋 Accounts | Defines account related information, such as login ID and account status. |
| 🗋 Entitlements | Defines the access granted to each account in the system, such as entitlements, roles or profiles. |
| 🗋 Security Model | Defines entitlement collections, such as application profiles and roles, which may be referenced in the Entitlements file. |

Within a System Security Data Feed, all of the files must be:

* Comma Separated Values (CSV) format (see [Section 3.5](#_CSV_Format_1)).
* Include a properly formatted header record (see [Section 3.3](#_Header_Record)).
* Include a properly formatted trailer record (see [Section 3.4](#_Trailer_Record)).
* The exact number of fields/columns as defined in the respective file schemas in [Section 4](#_Feed_Files_Schema).
* Each row, including the trailer record, must be separated with a single newline character - either LF (Line Feed ‘\n’) or CR (Carriage Return ‘\r’).
* ASCII or UTF-8 encoded.

The system security data feed files are to be delivered as three (3) distinct CSV files, collected and compressed for delivery into one TAR file. The feed and files within the TAR-format feed must follow the naming convention in Figure 2.

Figure 2: Naming convention for feed and files in a feed

|  |  |
| --- | --- |
| **File** | **Naming Convention** |
| *GiAM SYSTEM ID is a unique ID created by the GiAM tool upon onboarding, followed by the file type (grmrdata, acct, entl and smod), and a timestamp in 24 hour format.* | |
| 🗍 System Security Data Feed | GiAM SYSTEM ID.grmrdata.YYYYMMDDHHMMSS.tar |
| 🗋 Accounts | GiAM SYSTEM ID.acct.YYYYMMDDHHMMSS.csv |
| 🗋 Entitlements | GiAM SYSTEM ID.entl.YYYYMMDDHHMMSS.csv |
| 🗋 Security Model | GiAM SYSTEM ID.smod.YYYYMMDDHHMMSS.csv |

For example, for a system’s accounts file with the GiAM SYSTEM ID “HNAH-US-A-JANESAPP-01” and a timestamp of “20100119145535”, the appropriate filename is “HNAH-US-A-JANESAPP-01.acct.20100119145535.csv”.

All three (3) CSV files must be included in the TAR file. In the case where no data is to be delivered, each CSV file should include, at minimum, a header and trailer record.

|  |
| --- |
| **🛈 Important Note** |
| 1. In the case where the system generating the source file cannot support the TAR format, CSV will be accepted. 2. In the case where no data is to be delivered, each CSV file should include, at minimum, a header and trailer record. 3. In case of TAR feed file, ensure that only three CSV files are enclosed. There must not be any sub-directories/folders included in the TAR feeds, in which case the files will not get validated. |

## Feed Transmission

The feed TAR file described in Section 3.1 must be securely transferred to the GiAM environment via secure copy (SCP) network protocol or Connect Direct.

**Production Data Feeds must be automated and sent daily.**

The authentication to the "grmrdata" file transfer account will be managed via SSH key pairs. Prior to the initial file transfer, the application team will need to provide the public key from an RSA SSH private-public key pair to the GRMR data. The password of the "grmrdata" account will NOT be provided to application teams.

For further reference, please refer to ***GiAM Data Feed Transmission Design Specification*** document, available from [this Sharepoint link](https://team.global.hsbc/sites/ACT/SitePages/Onboarding_New.aspx?RootFolder=%2Fsites%2FACT%2FGiAM%20Procedures%2FGiAM%20Guides&FolderCTID=0x01200038611FC86143CA4F9395340849683A71&View=%7BFC63BA6E%2D1076%2D4859%2D9881%2D04162E55268D%7D).

## Header Record

Each file included in the System Security Data Feed must have a header record. The header record must be included as the first line in each file. The specific header records for each of the Accounts, Entitlements and Security Model files are provided in Sections [4.1](#_Accounts), [4.3](#_Entitlements) and [4.4](#_Security_Model) respectively below.

Header records are required for audit compliance and are a control point in the process of loading feeds into the GiAM tool.

|  |
| --- |
| **🛈 Important Note** |
| Please ensure that the headers match exactly as shown in the Appendix A, which means ensuring the correct case (lower). Header records must be included in each CSV data feed file. |

## Trailer Record

A trailer record must appear as the last line of each file included in a System Security Data Feed. The trailer record must include:

* Total number of records in the file (total number of lines, excluding header and trailer lines).
* Timestamp of file creation date in the format MMDDYYYYHHMMSS, 24-hour format.

The trailer line of a file must begin with **TRAILER**, followed by a timestamp and the number of records. Figure 3 describes the required field layout for the trailer line of a file:

Figure 3: Trailer line schema

| **Field Name** | **Required** | **Type** | **Length** | **Format/values** | **Description** |
| --- | --- | --- | --- | --- | --- |
| Record Type | Required | String | 256 | **TRAILER** is the required value. | Identifies the line as a trailer record. |
| Timestamp | Required | Date | 14 | MMDDYYYYHHMMSS, 24-hour format | Timestamp of when the feed data was created/pulled from the source system. |
| Record count | Required | String | 256 | Numeric value | Number of records in the file, or number of lines, excluding header and trailer lines. |

Trailer records are required for audit compliance and are a control point in the process of loading feeds into the GiAM tool. It is imperative that feeds contain accurate trailer records.

|  |
| --- |
| **🛈 Important Note** |
| The value **TRAILER** in the first trailer field must be in uppercase.  There must not be any data or blank rows after the TRAILER record. |

### Trailer sample

The box below shows the example of a valid trailer record.

TRAILER,12312010090000,374

## CSV Format

Each file in the System Security Data Feed must be in CSV, compliant with the following requirements:

* Fields/columns are separated by a comma character (“,”).
* Records are separated by a new line/carriage return character.
* Each record should have the same number of fields/columns (the number of commas should be consistent across each row of the file).
* Each record should have the same number of fields/columns as specified by the file schema/layout defined within this document. Records should not have trailing commas, which would erroneously be read as an additional field.
* Fields/columns should be encapsulated with double quote marks, but it is only mandatory when the field/column contains a comma character. A double quote character within a field/column must be escaped by two sequential double quote marks (“”).

|  |
| --- |
| **🛈 Important Note** |
| Ensure that leading and trailing whitespaces in each of the fields – even if the field is enclosed in double quotes - are removed in all the three files. In other words, ensure that there are no spaces before or after the comma. |

|  |
| --- |
| **🛈 Important Note** |
| Files must not contain the tilde (~) character. This will lead to incorrect validation results. |

# Feed Files Schema

## Accounts

All accounts on a system should be listed in the Accounts file sent to the GiAM tool. The Accounts file must include the fields outlined in Figure 4.

Exceptions: Those accounts that are in a disabled state and must remain on the system permanently for historical audit purposes. Standard locked or disabled accounts (those that can be reactivated) must not be excluded from the feeds.

Figure 4: Accounts file schema

| **Field Name** | **Required** | **Type** | **Length** | **Format/values** | **Description** |
| --- | --- | --- | --- | --- | --- |
| Account ID | Required | String | 256 | Alphanumeric | Unique account identifier within the system, typically the login ID. |
| Person ID | Required | String | 256 | Alphanumeric | The Group Human Resources System (GHRS) PeopleSoft ID. *Alternate if GHRS ID is not available, Lotus Notes ID.* |
| Native First Name | Conditional | String | 256 | Free form text | First name (or common name). If the host system stores the name in a single field, it is not required to split that field – place the entire name intothe Native First Name field. |
| Native Middle Name | Conditional | String | 256 | Free form text | Middle name or initial. |
| Native Last Name | Conditional | String | 256 | Free form text | Last name (surname). |
| Last Login Timestamp | Required | Date | 14 | MMDDYYYYHHMMSS, 24-hour format | Timestamp of last successful authentication by Account ID. If the specified format cannot be supported, omit this field. |
| Creation Timestamp | Required | Date | 14 | MMDDYYYYHHMMSS, 24-hour format | Timestamp of creation of Account ID. If the specified format cannot be supported, omit this field. |
| Account Type | Required | Enum | 6 | "User" or "System" | Use/purpose of the account, where “User” is for an individual and “System” is for a computerized process**. The value for this field is case sensitive in case it is populated with “User” or “System” values.** |
| Account Status | Required | Enum | 8 | "Active" or "Disabled" | See Section 4.2 on properly translating system status to an active/disabled value. **The value for this field is case sensitive.** |
| Native Account Status | Required | String | 256 | Free form text | Native Account ID status within the system (e.g. “Suspended”). |
| System ID | Required | String | 256 | Alphanumeric | Unique identifier for the system created by the GiAM tool during the Onboarding process. |
| System Region | Required | Enum | 5 | “AMG”, “GBM”, ”GPB”, ”GLT”, ”GR”, “HASE”, "HBAP", "HBEU", “HBME”, “HLAH”, “HNAH”, “SABB” | Region that owns the system. |
| System Entity | Required | Enum | 2 | ISO Country Code | Country where the system/application is hosted – Based on ISO 3166 Alpha-2 country codes: <http://www.iso.org/iso/country_codes>  \*\*This is NOT to be the Country Code for the Account/Employee owning the account. |

|  |
| --- |
| **🛈 Important Note** |
| The values for Account Type and Account Status are case sensitive and must be as shown in the schema above. |

The following table defines the specific header record that must be included in the Accounts file.

NOTE, the double quotes are optional. The GiAM system will accept the data in both formats, with or without quotes.

| **Line** | **🗋Accounts file header** |
| --- | --- |
| 1 | "account\_id","person\_id","native\_first\_name","native\_middle\_name","native\_last\_name","last\_login\_timestamp","creation\_timestamp","account\_type","account\_status","native\_account\_status","system\_id","system\_region","system\_entity"  **OR**  account\_id,person\_id,native\_first\_name,native\_middle\_name,native\_last\_name,last\_login\_timestamp,creation\_timestamp,account\_type,account\_status,native\_account\_status,system\_id,system\_region,system\_entity |

### Orphan Accounts

Accounts listed in the Accounts file that do not have a value in the Person ID field, or a value that does not match an identity within GHRS, will be loaded as “orphans.” These accounts will need to be remediated through the orphan account management process. The GHRS PeopleSoft ID (Staff ID / Contingent ID) should be provided in the Person ID field. It serves as the key for correlating an account to an identity and also combining the user access for line manager recertification; it is imperative that it is accurate and included in the feed. During instances where the PeopleSoft ID is not available in the source system, the feed should contain one of the alternate correlation attributes based on which account ownership can be determined.

\*The list of acceptable alternate correlation attributes includes the following:

* Lotus Notes ID

**Note**: If the system cannot send any of these IDs (PeopleSoft ID, Lotus Notes ID) in the feed, contact the Onboarding Facilitator prior to onboarding.

## Account Status Translation

Native system account status must be translated, or normalized, to be properly acted upon in the GiAM tool.

|  |
| --- |
| **🛈 Important Note** |
| Native Account Status and Account Status are for awareness and reporting purposes during access clean-up activities.  The GiAM tool does not act upon on any status in either the Native Account Status or Account Status fields. The inclusion of Account Status as a required field and in the format specified in the schema above, is from a reporting and a consistency standpoint and must be adhered to. |

### Active Accounts

Active accounts are in a state that allows login, or can be accessed for login without a provisioning request and approvals being executed. For example, an account that is locked because of a password reset would be an active account because password resets do not require that a provisioning request be created and/or appropriate approvals be obtained.

### Disabled Accounts

Disabled accounts are in a state that prevents login to the system. To obtain access to a system through a disabled account requires a new access request with appropriate approvals and audit trails. For example, an account that has been logically deleted (physically maintained due to architectural/inferential integrity constraints), but cannot be accessed in any way by a user, is a disabled account.

Where an account is in a disabled state but has to be permanently maintained on a system for historical audit trail purposes (will never be deleted), this should be documented accordingly and only in those instances can those disabled accounts be ommited from the feeds.

### Account Status Mapping Examples

Figure 5 contains examples of system statuses and the appropriate GiAM tool status that should appear for the account in the Accounts feed.

Figure 5: Accounts file schema

|  | **GiAM Status** | |
| --- | --- | --- |
| **System status** | **Active** | **Disabled** |
| Login enabled | ⚫ |  |
| Password lockout | ⚫ |  |
| Leave of absence | ⚫ |  |
| Short term disability | ⚫ |  |
| Long term disability | ⚫ |  |
| Suspended | ⚫ |  |
| Logically deleted |  | ⚫ |
| Other | ⚫ |  |

|  |
| --- |
| **🛈 Important Note** |
| The GiAM tool does not process or action upon any statuses indicated in the feeds. Status is captured for reporting and awareness purposes only.  **Where disabled accounts are maintained on a system for historical audit trail purposes (i.e. will never be deleted), this should be documented and those accounts excluded from the data feed.** |

### Account File Sample:

Please refer to the account file sample attached below. Note that the naming convention for the Accounts file must be as indicated in Figure 2 of [Section 3.1](#_System_Security_Data).



## Entitlements

System entitlements or profiles associated with accounts are defined in the Entitlements file. All entitlements or profiles associated with an account should be listed in the file sent to the GiAM Tool. The Entitlements file must include the fields outlined in Figure 6.

Figure 6: Entitlements file schema

| **Field Name** | **Required** | **Type** | **Length** | **Format/values** | **Description** |
| --- | --- | --- | --- | --- | --- |
| Account ID | Required | String | 256 | Alphanumeric | Unique account identifier within the system (must match the Account ID used in the Accounts file). |
| System ID | Required | String | 256 | Alphanumeric | Unique identifier for the system created by the GiAM tool during the Onboarding process. (must match the System ID used in the Accounts file). |
| Account Source | Required | String | 256 | “System” | Should be “System”. **The value for this field is case sensitive.** |
| Entitlement Type | Required | Enum |  | "E" or "P" | Describes the use of the proceeding fields (System profile, entitlement and action), where granular entitlement is "E" and system profile is "P". **The value for this field is case sensitive.** |
| System Profile | Conditional | String | 256 | If Entitlement Type is "P" field value must be specified | Collection of related entitlements within system, defined in the System’s Security file. |
| Entitlement | Conditional | String | 256 | If Entitlement Type is "E" field value must be specified | Specifies the name of the system granular entitlements. |
| Action | Conditional | String | 256 | If Entitlement Type is "E" field value can be specified | Action(s) that can be performed based on the assigned Entitlement (e.g. view, update, modify). |

|  |
| --- |
| **🛈 Important Note** |
| The values for Account Source and Entitlement Type are case sensitive and must be as shown in the schema above. |

The following table defines the specific header record that must be included in the Entitlements file.

NOTE, the double quotes are optional. The GiAM system will accept the data in both formats, with or without quotes.

| **Line** | **🗋Entitlements file header** |
| --- | --- |
| 1 | "account\_id","system\_id","account\_source","entitlement\_type","system\_profile","entitlement","action"  **OR**  account\_id,system\_id,account\_source,entitlement\_type,system\_profile,entitlement,action |

### Entitlement Collections

In the Entitlement Type field, the value “P” can be used to reference a profile, or collection of entitlements, that is granted to the user in the system. This reduces the overall size of the Entitlements file (entitlements do not need to be flattened, where detailed granular entitlements are listed for each user) and provides a means of defining the hierarchy or layers of security granted to a user.

To reference a set of entitlements in the Entitlements file, the collection must be defined in the Security Model file (see section 4.4) with a unique name in the System Profile field. The unique name specified in the Security Model’s System Profile Field must appear exactly the same in the Entitlement file’s Entitlement field. Figure 7 illustrates the use of the referencing of a System Profile in the Security Model file.

Figure 7: Example entitlement collection

| 🗋**Security Model file for application “Banking Application”** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **System ID** | **System Profile** | **Security Definition Type** | **System Profile Child** | **Entitlement** | **Action** |
| Banking Application | Manually Post Checks | E |  | CREDIT | POST |
| Banking Application  The user js83ncs has access to a total of three entitlements, with two of the entitlements granted by the “Manually Post Checks” System Profile referenced in the Entitlement file. | Manually Post Checks | E |  | CREDIT | AUTHORIZE |

| 🗋**Entitlement file for application “Banking Application”** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Account ID** | **System ID** | **Account Source** | **Entitlement Type** | **System Profile** | **Entitlement** | **Action** |
| js83ncs | Banking Application | System | P | Manually Post Checks |  |  |
| js83ncs | Banking Application | System | E |  | ADDRESS\_MENU | UPDATE |

### Entitlement File Sample

Please refer to the entitlement file sample attached below. Note that the naming convention for the Entitlements file must be as indicated in Figure 2 of [Section 3.1](#_System_Security_Data).



## Security Model

The Security Model file defines security elements or layers of the system. The Security Model allows a set of entitlements to be defined once and referenced as needed in the Entitlements file. For example, in the Entitlements file accounts may be associated with a profile and in the Security Model file the profile is defined with all of the associated granular level entitlements.

Figure 8: Security Model file schema

| **Field Name** | **Required** | **Type** | **Length** | **Format/values** | **Description** |
| --- | --- | --- | --- | --- | --- |
| System ID | Required | String | 256 | Alphanumeric | Unique identifier for the system created by the GiAM tool during the Onboarding process (must match the System ID used in the Accounts file). |
| System Profile | Required | String | 256 | Free form text | Name of collection of related entitlements within a system, defined within this file (must match the System Profile name used in the Entitlements file). |
| Security Definition Type | Required | Enum |  | “C” or “E” | “C” should be used when defining a child profile, and “E” for defining the granular entitlements of a system profile. |
| System Profile Child | Conditional | String | 256 | If Security Definition Type is "C" field value must be specified | Defines a child system profile. |
| Entitlement | Conditional | String | 256 | If Security Definition Type is "E" field value must be specified | Granular application entitlements for the system profile. |
| Action | Conditional | String | 256 | If Security Definition Type is "E" field value can be specified | Value specified if an action can be performed on the entitlement (e.g. view, update, modify). |

For examples on using the System Profile field to define a collection of entitlements, refer to [Section 4.3.1](#_Entitlement_Collections).

The following table defines the specific header record that must be included in the Security Model file.

NOTE, the double quotes are optional. The GiAM system will accept the data in both formats, with or without quotes.

| **Line** | **🗋Security Model file header** |
| --- | --- |
| 1 | "system\_id","system\_profile","security\_definition\_type","system\_profile\_child","entitlement","action"  **OR**  system\_id,system\_profile,security\_definition\_type,system\_profile\_child,entitlement,action |

|  |
| --- |
| **🛈 Important Note** |
| If there are no additional security elements or layers within the system, the Security Model file must still be included in the transmitted feed with a header and trailer record. The trailer record count should then be listed as zero (0). |

### System Profile Hierarchy

System Profiles in the Security Model can be defined with parent/child hierarchies. To define a relationship, the System Profile Child field should be populated with the name of the System Profile to reference. Figure 9 contains an example of this usage.

Figure 9: Example System Profile hierarchy

| 🗋 **Security Model file for a sample application** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **System ID** | **System Profile** | **Security Definition Type** | **System Profile Child** | **Entitlement** | **Action** |
| HYP-TT-A-BANK-01 | Clerk | E |  | ACCOUNT | INQUIRY |
| HYP-TT-A-BANK-01 | ASST\_Mgr | C | Clerk |  |  |
| HYP-TT-A-BANK-01 | ASST\_Mgr | E |  | CREDIT HISTORY | INQUIRY |
| HYP-TT-A-BANK-01 | ASST\_Mgr | E |  | CREDIT | RECOMMEND (YES) |
| HYP-TT-A-BANK-01 | ASST\_Mgr | E |  | CREDIT | RECOMMEND (NO) |
| HYP-TT-A-BANK-01 | Manager | C | ASST\_Mgr |  |  |
| HYP-TT-A-BANK-01 | Manager | E |  | CREDIT | AUTHORIZE |

### Security Model File Sample

Please refer to the security model file sample attached below. Note that the naming convention for the Security Model file must be as indicated in Figure 2 of [Section 3.1](#_System_Security_Data).



# Glossary Data Feed Overview

The Glossary file, which is generated by the IT Security IAM Onboarding Facilitator using the supplied Entitlements and Security Model files and then uploaded in to the GiAM Onboarding, **must** include all system entitlements and profiles, even those that do not appear in a system feed, with an accompanying business friendly description. Unlike the Account, Entitlements, and Security Model files, the Glossary file is not to be automated to ensure integrity of the data held within it.

**IMPORTANT NOTE: Entitlements or profiles NOT referenced in the Glossary but included in the Entitlement and / or SMOD files will be included for recertification and be challenging for Line Managers to accurately recertify access.**

It is imperative that glossary friendly descriptions be succinct, accurate and understandable by a general Line Manager population. For example, consider the long description for entitlement *LMS QPAA Function* – ***“The ability to add account demographics information as well as creation date, open date, close date and purge date”.*** Here, the privilege conferred by the entitlement is spelt out fully in a concise manner in simple, non-technical language.

The glossary file, via the Sensitive Business Transaction marker, can be used to mark entitlements as privileged.

## Glossary Data Feed Specification

The Glossary Feed file must be:

* In Comma Separated Values (CSV) format (see [Section 5.1.2](#_CSV_Format)).
* The exact number of fields/columns as defined in the glossary file schema in [Section 5.2](#_Glossary_File_Schema).

The glossary feed file is to be delivered as a CSV file that must follow the naming convention in 10.

Figure 10: Naming convention for glossary feed file

|  |  |
| --- | --- |
| **File** | **Naming Convention** |
| *GiAM SYSTEM ID is a unique ID created by the GiAM tool during the Onboarding process, followed by the file type (risk), and a timestamp in 24 hour format.* | |
| 🗋 Glossary | GiAM SYSTEM ID-risk-MM-DD-YYYY.csv |

For example, for a system’s glossary file with the GiAM SYSTEM ID “HNAH-US-A-JANESAPP-01” and a timestamp of “04-16-2010”, the appropriate filename is “HNAH-US-A-JANESAPP-01-risk-04-16-2010.csv”.

### Glossary File Maintenance

Production Glossary File must be reviewed and updated at least annually. Timely refreshes must be made upon the creation of any new entitlements or profiles and/or changes to the security architecture of the system(s).

## Glossary File Schema

The Glossary file must include the fields outlined in Figure 11.

Please utilize the [GiAM System Security Data Glossary Template](https://team.global.hsbc/sites/ACT/GiAM%20Procedures/GiAM%20File%20Templates/GiAM%20System%20Security%20Data%20Glossary%20Template.xlsm?Web=1) to assist in properly building the Glossary file.

Figure 11: Glossary CSV file schema

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Field Name** | **Required?** | **Type** | **Length** | **Format/values** | **Description** |
| Risk | Required |  | 20 |  | Final assessed risk for system profile/entitlement (High, Medium and Low). Risk value is case sensitive.  \*See Glossary Definition Template for Risk Definitions |
| System ID | Required |  | 256 |  | Unique identifier for the system created by the GiAM tool during the Onboarding process (must match the System ID used in the Accounts file). |
| Entitlement Type | Required |  | 256 |  | The type of access control, "Profile" or "Entitlement" (same convention as used in the System Security Data Feed files). |
| System Profile | Conditional |  | 256 |  | If Entitlement Type is "Profile", the corresponding Profile name from the System Security Data Feed should be noted. |
| Entitlement | Conditional |  | 256 |  | If Entitlement Type is "Entitlement", the corresponding Entitlement name from the System Security Data feed should be noted. |
| Action | Conditional |  | 256 |  | If Entitlement Type is "Entitlement", the corresponding Action from the System Security Data feed should be noted. |
| Alternate Name | Optional |  | 256 |  | Alternate name for the Profile or Entitlement (this will replace the Profile or Entitlement Name in the GUI, useful for when the value in the feed is too cryptic for end users to read). |
| ToolTip | Optional |  | 256 |  | Description displayed to the end user when the mouse cursor hovers over the Entitlement. |
| Long Description | Required |  | 4000 |  | In business friendly language, the full description of the entitlement. The descriptions should be traditional sentences that are understandable by the business. |
| Help URL | Optional |  | 256 |  | A URL with more information/help documentation about the entitlement. |
| Sensitive Business Transaction | Conditional |  | 256 |  | The specific transaction name as defined by the Business lines and Frameworks. For Privileged accounts populate with "Privileged Account Marker"  *\* This field is required for systems included in the GAMD Segregation of Duties initiative.* |
| Sensitive Business Transaction # | Conditional |  | 256 |  | Unique SBT identifier as per business definitions is input here. In addition, for Privileged access, list PRIVA, PRIVD or PRIVP here for Application, Database or Platform respectively |

|  |
| --- |
| **🛈 Important Note** |
| Please follow the below shown standard convention for ‘Long descriptions’ of any platform accounts that link to an application. It is important that users know what they are reviewing and can associate to the application.  Provides <ACCESS> to <APPLICATION NAME(S)>  **Example**  Provides User access to Teller Application  In cases where the platform account is tied to more than one application, please list all the applications in the description. |

## Glossary File Sample

Please refer to the sample glossary files attached below. Note that the naming convention for the Glossary file must be as indicated in Figure 16 of [Section 5.1](#_Glossary_Data_Feed).

**

# Data Feeds for Active Directory/AD LDS Application Entitlements

|  |
| --- |
| **🛈 Important Note** |
| Nested groups must NOT be used in any new Application AD groups. If you currently have nested groups then it is compulsory to ensure the procedure in step 2 is adhered to. You must then perform remediation work to eradicate the nested groups from your existing application AD groups to conform to standard. |

1. Complete the resource registration process just like any other application and obtain a System ID. Ensure that the appropriate option is selected for the ‘Feed File Source’ field:

* ‘Active Directory (AD)’ must be chosen for applications that utilize Active Directory-based entitlements



* ‘Active Directory Light Weight Services (ADLDS)’ must be chosen for applications that utilize AD LDS-based entitlements

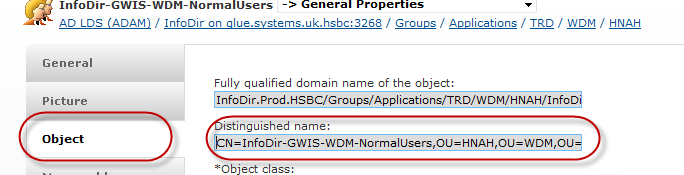


1. Submit Glossary (Risk) File which includes **all** parent and child groups (groups nested within a parent group). The Glossary file must list all the AD / AD LDS groups which are used by that application and from which user accounts must be extracted.

**Group names for AD groups** should be in the format "DOMAIN\GROUP NAME" as shown in the example below. All groups are of type 'Profile' since any group can contain any group.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk** | **GiAM System ID** | **Entitlement Type** | **System Profile** | **Entitlement** | **Action** | **Alternate Name** | **ToolTip** | **Long Description** | **Help URL** |
| High | HNAH-US-P-DCRLANSHARE-01 | Profile | HNAH\US HTSU-NTFS USBDCDSDB01-DCRAdminShare RO-S-D |  |  |  |  |  |  |

**Group names for AD LDS groups** should be the full CN value found in the Distinguised Name field in the Object tab of the group.



Example below. All groups are of type 'Profile' since any group can contain any group.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk** | **GiAM System ID** | **Entitlement Type** | **System Profile** | **Entitlement** | **Action** | **Alternate Name** | **ToolTip** | **Long Description** | **Help URL** | **SBT Name** | **SBT #** |
| High | HNAH-OH-A-ACCTOPEN-01 | Profile | CN=BR\_ADC\_JUNIOR\_ASSOCIATE,OU=business\_rules,OU=HBUS,OU=NA,OU=Roles,OU=Groups,DC=InfoDir,DC=Prod,DC=HSBC |  |  |  |  |  |  |  |  |

AD/AD LDS account and entitlement data is extracted in to GiAM for the AD / AD LDS groups defined in the Glossary file on a daily basis.

## Sample AD Glossary File

Please refer to the sample glossary file for AD groups attached below. Note that the naming convention for the Glossary file must be as indicated in Figure 16 of [Section 5.1](#_Glossary_Data_Feed).

