HIGHER LOGIC
ALL TOGETHER

Higher Logic Upload Training Manual

The integration of user data onto your Higher Logic community site is known as an *Upload Integration* because the information from the spreadsheets is uploaded to the Higher Logic server manually, by the client.

This data transfer is one-directional, going from the uploaded spreadsheets onto your Higher Logic site. This means that any data changes need to be made through the upload process.

This document outlines the process of uploading individual records, ie: Contacts and Security Groups onto your Higher Logic community site as well as information on Single Sign On (SSO) for upload clients.

Upload Contacts

Sample Contact Upload

	A	B	C	D	E
1	**LegacyContactKey**	**EmailAddress**	**FirstName**	**LastName**	**CompanyName**
2	312314	John@abc.com	John	Doe	HigherLogic
3	345345	jim@abc.com	Jim	Dean	HigherLogic
4	984545	Tim@abc.com	Tim	Adams	HigherLogic
5	785454	joe@abc.com	Joe	Smith	ASAE
6	298594	stacy@abc.com	Stacy	Morgan	Community Roundtable
7					

Please note the required columns for a successful upload – the column headings in the spreadsheet must remain verbatim.

The **LegacyContactKey** how we identify a User's record in the backend. This unique identifier can be found in your database; if you do not have an assigned LegacyContactKey, you may assign each record with an arbitrary number.

**If you are utilizing SSO, please discuss this with your project manager. See Appendix for additional regarding the most common methods of SSO.*

FirstName is the first name of the user.

LastName is the last name of the user.

CompanyName is optional; however, the column header MUST be left in the Contact spreadsheet.

EmailAddress is the unique primary email address used to contact this individual record. Two users cannot have the same email address listed in the backend.

*Please see appendix for description of other column headers you may use in the Upload Contacts spreadsheet.

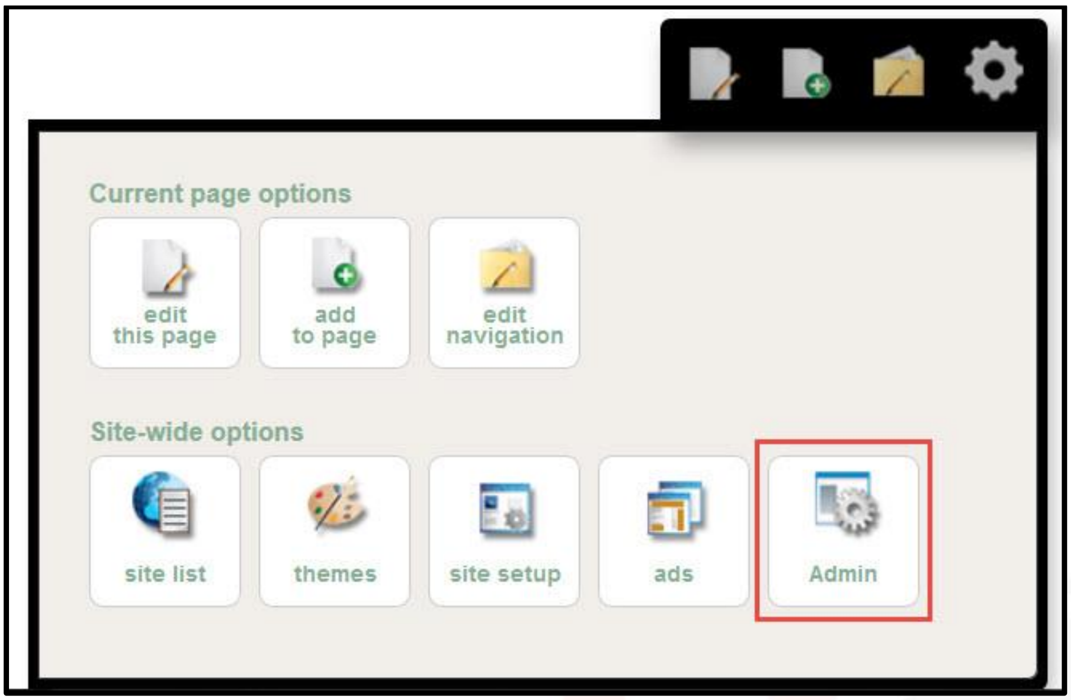
Best Practice: Delete all non-required columns that are not being used in the Contact spreadsheet.

HIGHER LOGIC
ALL TOGETHER

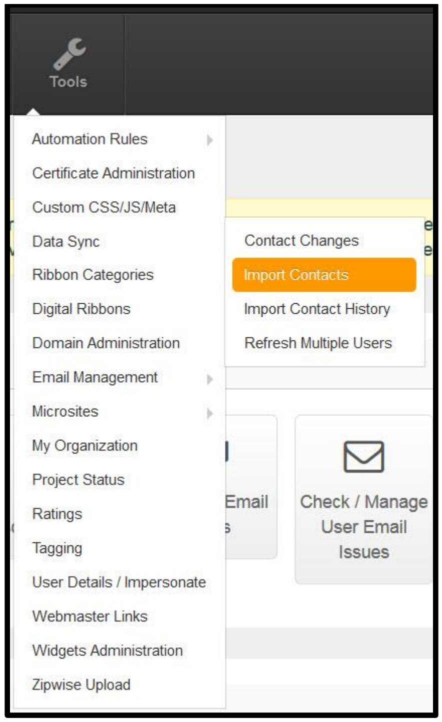
How to Upload a Contact Spreadsheet

Once you have the completed spreadsheet with all mandatory fields, you will begin the process to upload these into the system manually. *The file must be saved as a .csv document.*

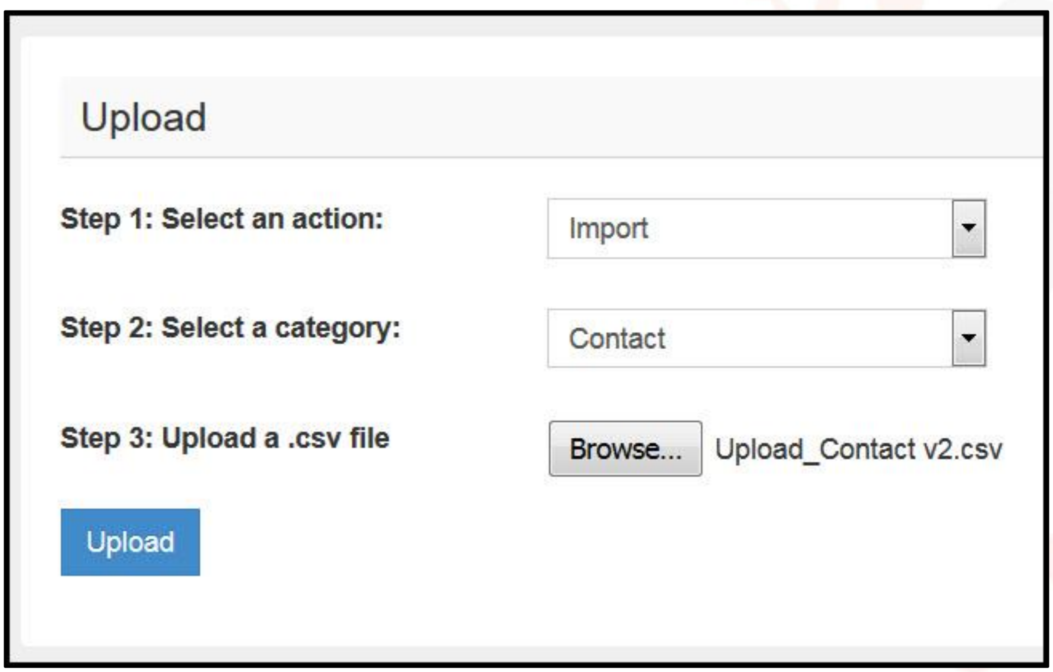
1. Select Admin from the Admin Toolbox on your Community Site.



2. Navigate to Tools > Data Sync > Import Contacts



3. Select actions from the Upload drop-down menu.
   Browse and choose your .csv file, then select **Upload**.



HIGHER LOGIC
ALL TOGETHER

Common Errors may occur when the required headings are not in the spreadsheet.

4. Review the imported contacts to ensure a successful upload. These will be shown under the Imported Contacts.

The important line item to note is **"Contacts were successfully loaded."** If you see 0 contacts successfully loaded OR the number of contacts successfully loaded does not match your count in the spreadsheet you uploaded, this means there is a discrepancy in the **LegacyContactKey**. Please review your original .csv file.

5. Select an option under the My File Contains drop-down.

a. **All User Records** and will replace all user data that has been previously imported. You will select **All User Records** upon initial Contact Upload.
**After the initial upload if you choose this option it will override all contact data in the system.*

b. **Only Some User Records** and will only add or replace previously imported user data For maintaining your Contacts going forward, the Contacts spreadsheet can be a partial upload. Reasons for a partial contact import include adding new users or deactivating previously imported users.

If you are adding a new record or changing an existing User's record, you may populate the document with these updated rows.

	A	B	C	D	E
1	LegacyContactKey	EmailAddress	FirstName	LastName	CompanyName
2	298594	stacy@abc.com	Stacy	Johnson	Community Roundtable
3	35135	monica@abc.com	Monica	Williams	FDA
4					

Note: Updated Record for LastName change from Morgan to Johnson, highlighted in yellow; Added new record, highlighted in green.

6. Select **Import Data**—you will receive a message at the top of your screen indicating data a successful import.

- The data has been imported and all affected clients have been added to the refresh queue.

*The refresh queue is how the system receives and updates your contacts. Depending on the number of contacts in your upload, this will determine the time it takes for your refresh to finish.

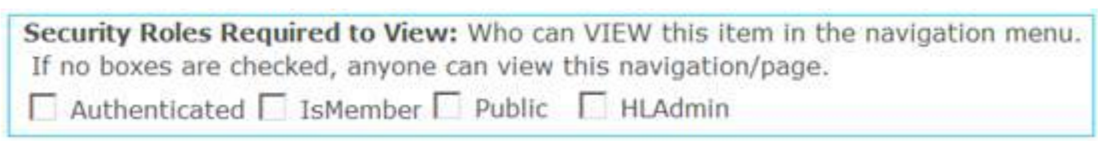
Best Practice: After the first initial import of contacts, first export the file to make future updates/changes.

Upload Security Groups

Security groups are often created based on **member types**; users can belong to more than one security group. These groups can be used to restrict access to specific pages within the site (such as the member directory), assign ribbons, and populate communities; however, they should not be confused with permissions for users to access communities.

Security Groups can be thought of as 'roles' and are a powerful tool for limiting viewing and access for navigation and content items on your community site. On your community site, users are broadly batched into Security Groups. Individual users can belong to multiple Security Groups.

Out of the box, your site has four Security Groups:



1. Authenticated – Any logged in user (they may or may not have member status)

2. IsMember – An aggregate of AMS-managed security groups. Content and functionality is routinely protected to Members as a benefit of membership. Those with IsMember privileges also belong to the "Authenticated" Security Group.

3. Public – Any user who is not logged into the site

4. HLAdmin – Global administrators (SuperAdmins) with universal access and editing privileges.

Security Groups can be either non-members or members. Content and functionality is routinely protected to Members as a benefit of membership.

In addition to the out-of-the-box security groups, clients should have at minimum two security groups "Member" and "Staff." Member Security Group is the Security Group that gives a User "IsMember" access.

If you need to make an uploaded Security Group a member, please contact your Project Manager or the Higher Logic Support Team to update your configuration on the backend.

Since each Contact can belong to more than one Security Group, this gives you the ability to target users.

For Example, John Adams is a member of the organization, on the Board of Directors, Finance Committee, and Secretary of the Northwest Chapter. Therefore, he will be in the Member, Board of Directors, Finance Committee and Chapter Officers Security Groups. These groups can be used to restrict access to specific pages within the site (such as the member directory), assign ribbons, populate communities, and other Automation Rule actions.

Note: It is not necessary to create Security Groups around any of your Community Groups.

By default, only the members of a particular community will be able to access the affiliated Discussion Group and Resource Library. For instance, it is not necessary to create a “Board of Directors” Security Group if the aim is to restrict access to a Discussion Group that is already a feature of the “Board of Directors” Community. (This is where the ‘invite-only’ status comes into play on the community settings.)

If you remove someone from having member status from the security group spreadsheet, if they still exist in the contact spreadsheet, then that user would be considered ‘authenticated,’ but not a ‘member.’

This allows you to customize access permissions based on these security groups.

How to Upload a Security Group Spreadsheet

Sample Security Groups

	A	B	C	D
1	LegacyContactKey	GroupType	GroupName	GroupKey
2	312314	STAFF	Staff	STAFF
3	345345	Staff	Staff	STAFF
4	984545	Staff	Staff	STAFF
5	785454	Member	Member	Member
6	785454	Committee	Finance Committee	Finance
7	298594	Member	Member	Member
8	298594	Committee	Technology	TECH
9	35135	Member	Member	Member
10	35135	Chapter	Chapter Officers	CO

	A	B	C	D
1	LegacyContactKey	GroupType	GroupName	GroupKey
2	312314	STAFF	Staff	STAFF
3	345345	Staff	Staff	STAFF
4	984545	Staff	Staff	STAFF
5	785454	Member	Member	Member
6	298594	Member	Member	Member
7	35135	Member	Member	Member
8	785454	Committee	Finance Committee	Finance
9	298594	Committee	Technology	TECH
10	35135	Chapter	Chapter Officers	CO

Please note the required columns for a successful upload – the column headings in the spreadsheet must remain verbatim.

The **LegacyContactKey** is what you assigned to the User in the Contact spreadsheet. This is how we associate the User to a Security Group.

GroupType is the type of Security Group; ie: Staff, Committee, Customer, etc.

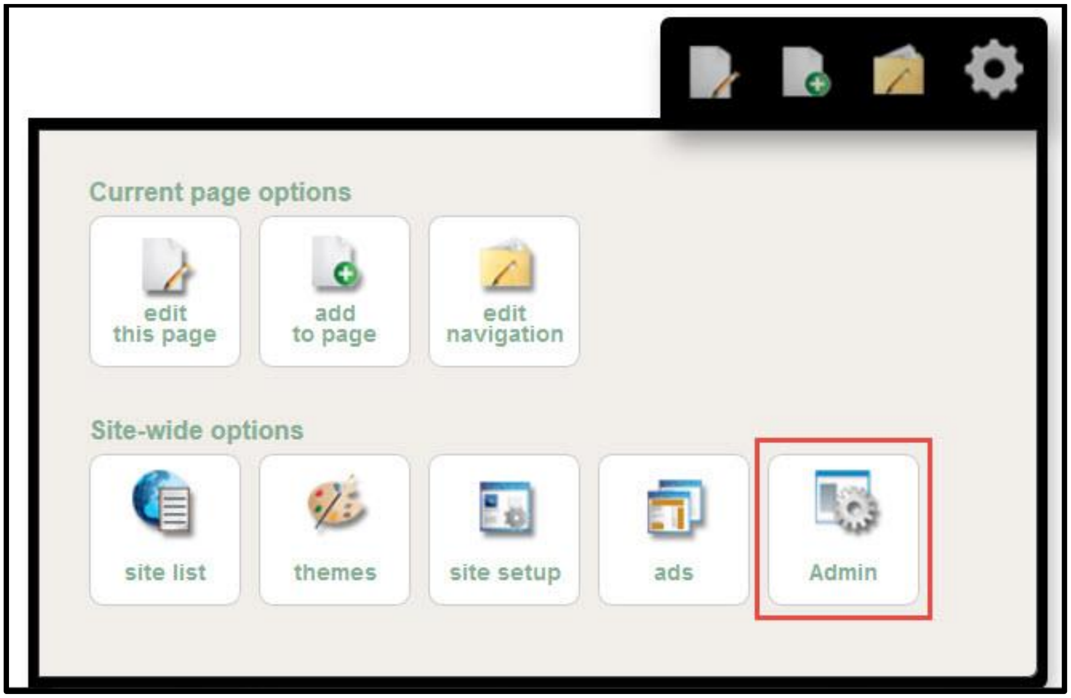
GroupName is the name of a Security Group; ie: Staff, Board of Directors, Prospects, etc.

GroupKey is what we will use as the backend key; to simplify, the GroupKey can be the same as GroupName.

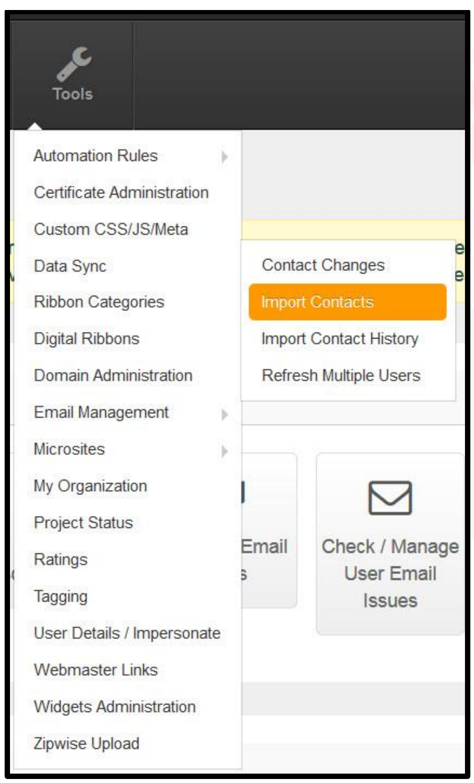
*Please see appendix for description of additional column headers you may use in the Upload Security Group spreadsheet.

Once you have the completed spreadsheet with all mandatory fields, you will begin the process to upload these into the system manually. ***The file must be saved as a .csv document.***

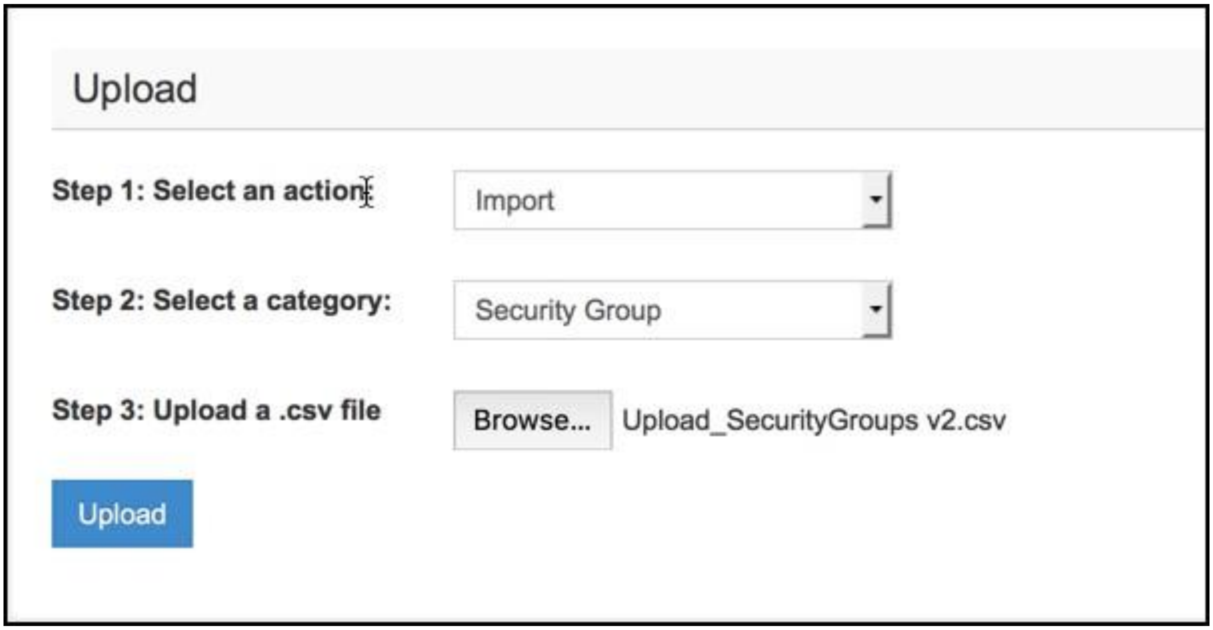
1. Select Admin from the Admin Toolbox on your Community Site.



2. Navigate to Tools > Data Sync > Import Contacts



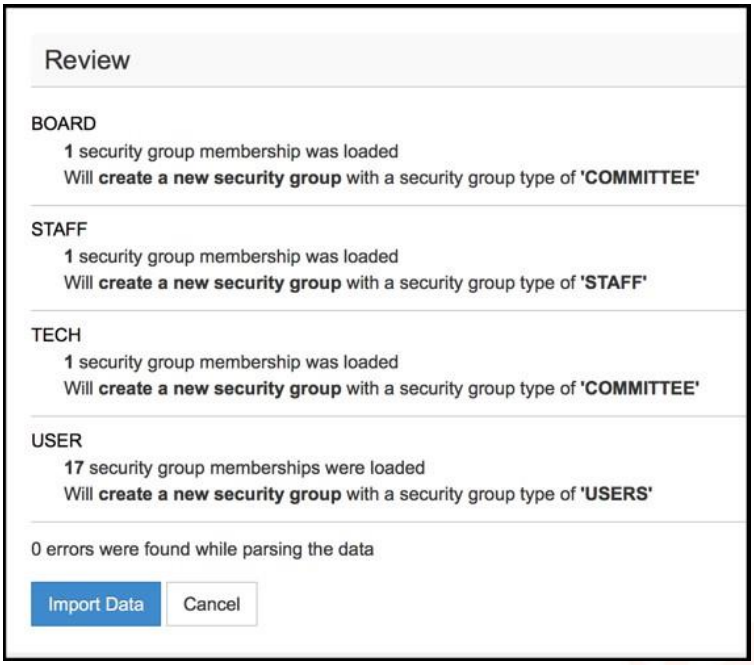
3. Select actions from the Upload drop-down menu.
   Browse and choose your .csv file, then select **Upload**.



Common Errors may occur when the required headings are not in the spreadsheet.

4. Review the imported Security Groups to ensure a successful upload. These will be shown under the Imported Contacts.

Review each line and validate the number (#) of **"security group memberships were loaded"** match up to your original count; if you see a discrepancy, please review your original .csv file.



5. Select **Import Data**—you will receive a message at the top of your screen indicating data a successful import.

*The refresh queue is how the system receives and updates your contacts. Depending on the number of contacts in your upload, this will determine the time it takes for your refresh to finish.

Best Practice: Do not make security groups for specific communities as the community view permissions can be set as 'invite only' which is essentially the same as creating a security group.

Best Practice: After the first initial import of security groups, use the exported file to make any future updates/changes.

HIGHER LOGIC
ALL TOGETHER

Appendix

Contact Spreadsheet Column Descriptions

Column Required?	Column Name	Description
Y	**LegacyContactKey**	The **unique** ID assigned to the record. Often known as the AMS or Member ID. LegacyContactKey MUST be unique for each user.
Y	**FirstName**	Individual (person) records must have either a first name or a last name.
Y	**LastName**	Individual records must have either a first name or a last name.
Y	**CompanyName**	The name of the company the individual works for or is associated to. Optional for individual records. Required for company records.
Y	**EmailAddress**	The **unique** primary email address used to contact the individual or company. Email addresses MUST be unique for each user. In other words, two users cannot have the same email address. All emails generated from your community site to the user will be sent to this address (initially).
N	Age	
N	Designation	List of designations or credentials following the individual's name.
N	PrefixCode	Prefix appearing before the individual's first name (e.g. Mr., Dr., Ms., etc.).
N	MiddleName	
N	InformalName	The individual's nickname (e.g. Katie for Kathleen or Nate for Nathan).
N	Gender	
N	SuffixCode	The suffix following the individual's last name (e.g. Sr., Jr., II, III, etc.).
N	Title	The individual's job title.
N	ParentMemberKey	The **LegacyContactKey** of the company/organization the individual works for or

		is associated to. Recommended if desiring a company directory.
N	ExcludeFromDirectory	Set to “True” if the individual or company should not be searchable via the directory. Leave blank otherwise.
N	IsActive	Leave blank if the user should be allowed to log in and participate on the site. Set to “False” if the user’s account should be deactivated. Deactivated users are not able to log in or participate on the site.
N	IsOrganization	Leave blank for individual records. Set to “True” for company records.
N	Bio	Bio/description of the individual/company.
N	WebsiteUrl	Link to the individual/company website.
N	Phone1	Primary phone number for the individual/company.
N	Phone1Type	Work, Home, Cell, etc. (Pick one and be consistent for all records.)
N	Phone2	
N	Phone2Type	Work, Home, Cell, etc. (Pick one and be consistent for all records.)
N	Phone3	
N	Phone3Type	Work, Home, Cell, etc. (Pick one and be consistent for all records.)
N	Phone4	
N	Phone4Type	Work, Home, Cell, etc. (Pick one and be consistent for all records.)
N	Address1	
N	Address2	
N	Address3	
N	City	
N	Country	
N	PostalCode	
N	State	
N	YouTubeURL	Link to YouTube profile or channel.
N	FaceBookURL	Link to Facebook profile or page.

N	TwitterURL	Link to Twitter profile.
N	GooglePlusURL	Link to Google+ profile or page.
N	LinkedInURL	Link to LinkedIn profile or page.
N	BloggerURL	Link to Blogger page.
N	WordPressURL	Link to WordPress page.
N	OtherBlogURL	Link to other blog page.
N	ProfileImageURL	Link to profile/logo picture to be used for a one-time import.
N	Ethnicity	
N	MemberId	Only include MemberId if it differs from LegacyContactKey.
N	Birthday	
N	Password	Only to be used if importing passwords.
N	MemberBadgeKey	Only to be used if using the MVM badge.

Security Group Spreadsheet Column Descriptions

Column Required?	Column Name	Description
Y	**LegacyContactKey**	The **unique** ID assigned to the record. Often known as the AMS or Member ID. LegacyContactKey MUST be unique for each user.
Y	**GroupName**	Most commonly, security groups are created based on member types. The name of the security group as it will appear to site admins.
Y	**GroupKey**	The code associated to the member type or security group. If you don't have one, please re-use GroupName mentioned above.
N	GroupType	Similar to communities, security groups can be grouped into categories (e.g. Member Type). Leave blank if categorization is unnecessary.
N	SinceDate	The date the individual was initially added to the security group (e.g. the member join date).
N	BeginDate	The date the individual should be added to the security group.
N	EndDate	The date the individual should be removed from the security group. (e.g. the member end date). People can be removed from security groups in an automated fashion by including the end date, or by manually completing a new security group upload.

Single Sign-On and Authentication

Higher Logic can implement single sign-on (SSO) with your CRM to provide members with seamless login experience between both portals. Single Sign-On (SSO) allows members to move between your main organizational website and your HL site without having to log in to each site separately.

The most common SSO solutions include:

(1) Credential Authentication - A user control on the community site accepts a user name and password that are resolved to a Master Customer Id. You will provide the resolution method (most often a web service method). Higher Logic does not store passwords; the credentials are passed through to your authentication service. This method provides authentication on the Connected Community site only and is therefore not a cross-asset Single Sign-On.

(2) Cookie - The Login link on your community site redirects to a login page on your main organization website where authentication is performed, a domain cookie is dropped and the user is redirected back to the community site. This method allows for cross-asset Single Sign-On across sites on the same domain. The cookie process must adhere to the following specifications:

-The login page must accept a Return URL parameter

-The community site and the login page must be on the same domain

-The value of the cookie should be the Master Customer Id or be able to be resolved to a Master Customer Id, whether through pre-shared-key encryption/decryption (Implementable through .NET) or a service method that can resolve the value of the cookie to the Master Customer Id.