

Version History

- 1.0 Original version.
- 1.01 Changed: the URL that gets called (the previous URL was too long for SASP!)
Changed: "adminUsername" is renamed to "adminLoginName".

1. Request

The request should be POSTed (rather than GETed) to the above URL.

Required variables are in **bold**.

Optional variables are in *italics*.

Variable Name (case insensitive)	Type	Max. Length	Description
orderNumber	string	128 chars	The Order Number of an order that has been placed on SASP
<i>adminLoginName</i>	string	64 chars	The Username of an Admin User of a SASP account
<i>adminEmailAddress</i>	string	255 chars	The Email Address of an Admin User of a SASP account

Note: one of "adminUsername" or "adminEmailAddress" must be specified. This must match the admin user of the account that placed the order referenced by "orderNumber".

2. Response

The MIME type will be `application/x-www-form-urlencoded`, because the format of the response will be the same "URL-encoded" format as the request (e.g. `name1=value1&name2=value2`).

Here are the names of the various variables that will or may appear in the response:

Variable Name (case insensitive)	Type	Description
errorCode	integer	Error code (see list below for possible values)
<i>errorMessage</i>	string	Explanation of error
confirmPassword	string	Unique password required for confirmation of password reset
adminEmailAddress	string	The Email Address of the Admin User

Here are the possible values for "errorCode" and "errorMessage":

errorCode	errorMessage
0	Successful
-1	Request was not made over HTTPS!
-2	'xxx' is an unrecognized argument!
-3	The 'xxx' argument is missing!
-4	The value of the 'xxx' argument is invalid!
-14	An unknown error occurred!
-16	Permission denied!
-17	Request used GET rather than POST!

After making this call, the caller will want to call the Tier 2 Partner Password Reset Confirm API.

This must NOT be done immediately/synchronously.

The caller must first send an email, which contains the "confirmPassword" and further instructions, to the "adminEmailAddress".

Only the legitimate user will receive this email. Once they do, they will need to copy-n-paste the "confirmPassword" onto a webpage.

The caller should use the copy-n-pasted "confirmPassword" to call the Tier 2 Password Reset Confirm API.