Configuring Self Service Password Reset

There are a number of elements to Self Service Password Reset that need to be agreed upon with the end customer.

The following table outlines the features and functions that need to be agreed upon with the end customer to proceed with the configuration of Self Service Password Reset.

Self Service Password Reset Option	**Description**	**End Customer Setting**
Users enabled for password reset	Designates whether users in this directory who have an office phone, mobile phone, or alternate email address specified in their profile can reset their own password.	**Yes**
Restrict Access to Password Reset	Select YES to restrict user password reset to only a limited group of users.	*Yes/No*
Group enabled for password reset	Defines the group of users who are allowed to reset their own passwords.	*AD Group Name*
Authentication Methods Available to Users	Select the alternate method types that the user may use to verify their identity when resetting their password.	*Authentication Methods:* ☐ *Office Phone* ☐ *Mobile Phone* ☐ *Alternate Email Address* ☐ *Security Questions*
Number of Authentication Methods Required	Defines the number of alternate methods of identification a user in this directory must have to reset their password.	*Number*
Require users to register when signing in?	Designates whether unregistered users are prompted to register their own authentication information when they sign in	*Yes/No*

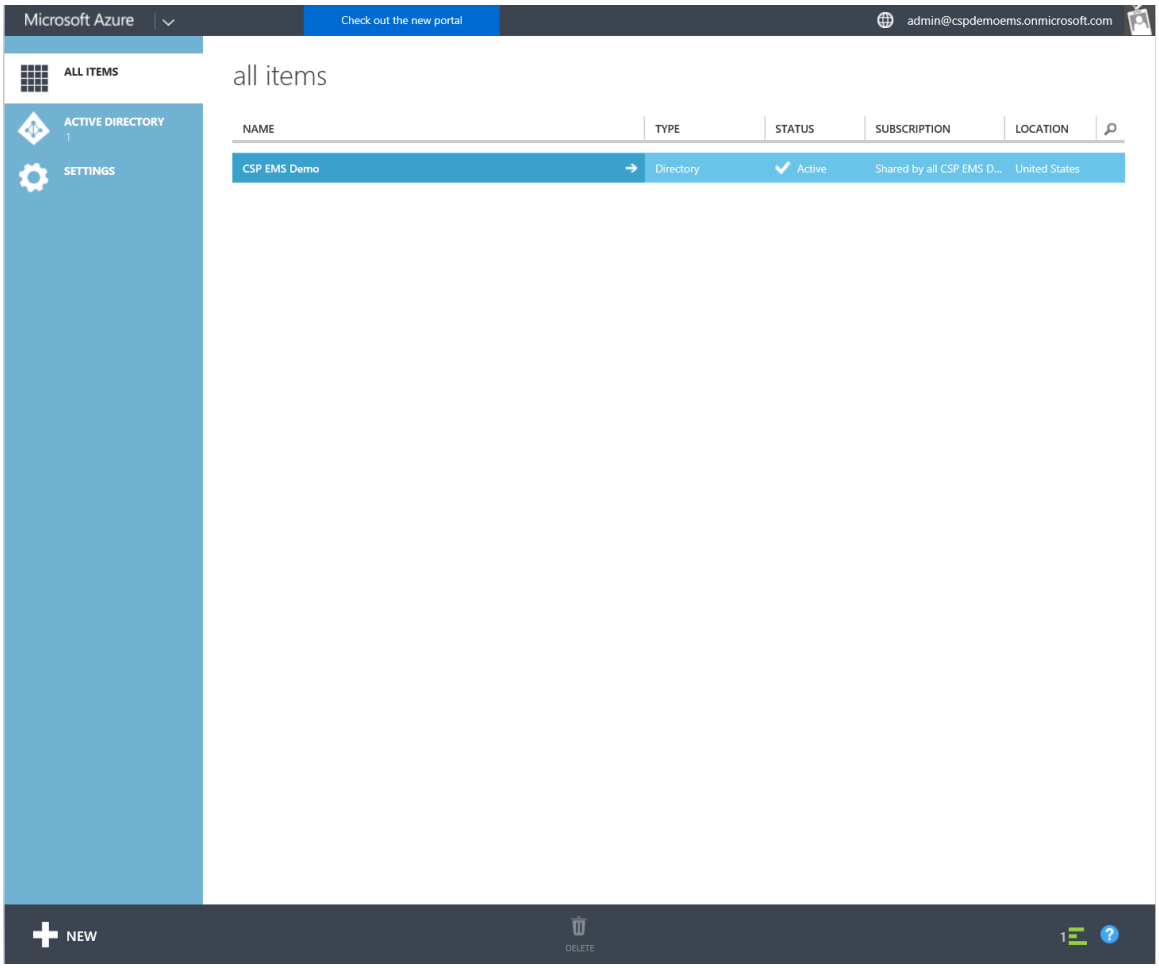
	for the first time. This is not yet supported for Office 365 sign ins.	
Number of days before users are asked to re-confirm their authentication information	Designates the period of time before registered users are prompted to re-confirm their existing authentication information is still valid, up to a maximum of 730 days. If set to 0 days, registered users will never be prompted to re-confirm their existing authentication information.	*Default: 180* *Number of days*
Customize "Contact Your Administrator" Link?	Designates whether or not the "Contact your administrator" link that normally allows users to contact a service administrator directly is overridden to point to a custom location.	*Yes/No*
Custom Email Address or URL	Designates the URL or email address to which your custom "Contact your administrator" link will point. If you provide a URL, we will open it in a new window. If you provide an email address, we will turn it into a mailto: link that will be sent to the email address you specify.	*URL or Email address:*
Write back passwords to on-premises active directory	If you deployed password write back when installing Azure AD Sync, you can control whether or not this feature is enabled here. If set to "no", federated or password synchronized users will not be able to reset or change their passwords, even if	*Yes/No*

	password write back has been configured. You can change this setting at any time.	
Allow users to unlock accounts without resetting their password	Designates whether or not users who visit the password reset portal should be given the option to unlock their on-premises Active Directory accounts without resetting their password. By default, Azure AD will always unlock accounts when performing a password reset, this setting allows you to separate those two operations. If set to "yes", then users will be given the option to reset their password and unlock the account, or to unlock without resetting the password. If set to "no", then users will only be able to perform a combined password reset and account unlock operation.	*Yes/No*
Email Language Preference	Language for notification email sent to users in your organization	*Locale based on subscription*
Notify admins when other admins reset their own passwords	Determines whether or not all global administrators receive an email to their primary email address when other administrators reset their own	*Yes/No*

	passwords via the Self-Service Password Reset Portal.	
Notify users and admins when their own password has been reset	Determines whether or not users receive an email to their primary and alternate email addresses notifying them when their own password has been reset via the Self-Service Password Reset portal.	*Yes/No*

1. Once the above information has been gathered, sign in to the [Azure Management Portal] and login as a co-administrator for the end customer tenant.

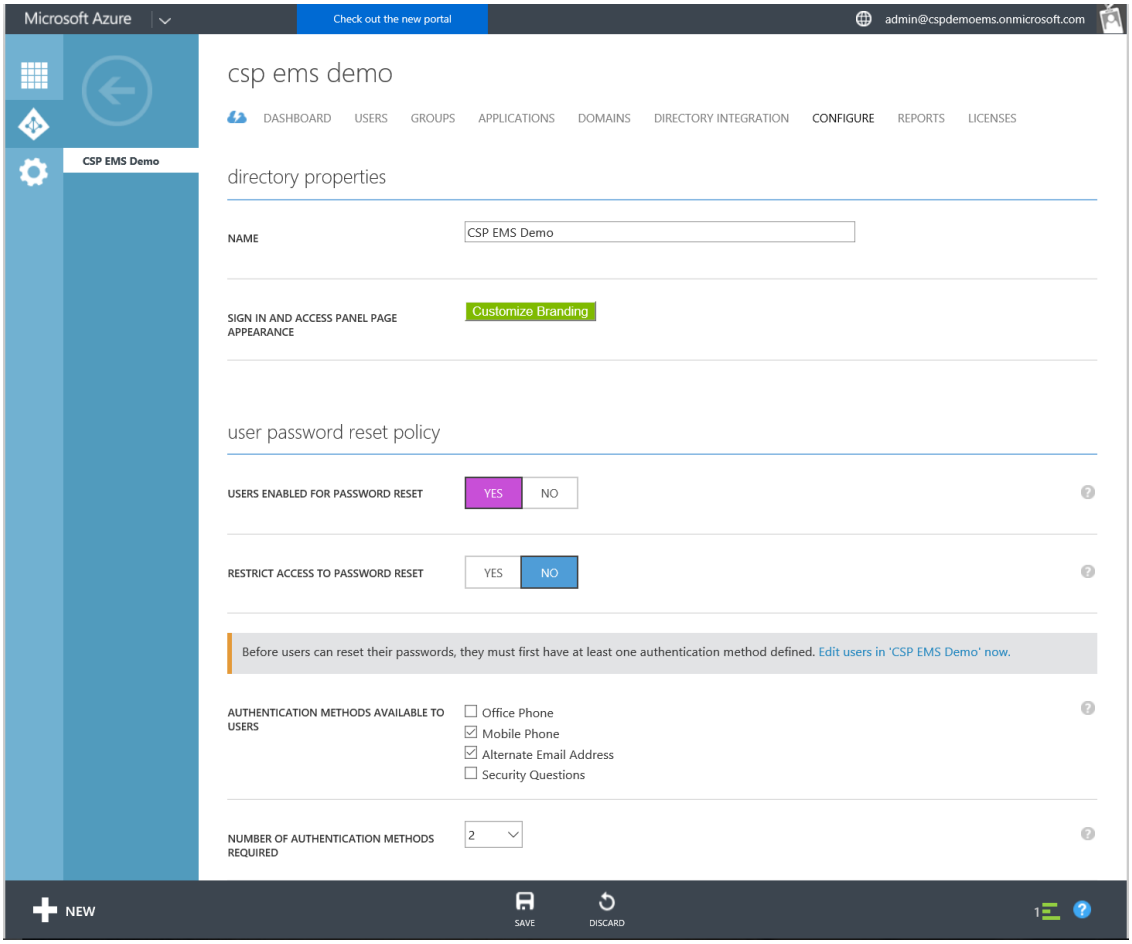
2. Select the Azure Active Directory (AAD) tenant for the end customer.



3. Select the **Config** tab

4. Under the heading **User Password Reset Policy** select **Yes** to enabled **Self Service Password Reset**

5. The User Password Reset Policy will populate will the configurable options



6. Complete the configuration as per the information gathered from the end customer.

7. Once complete, select **Save**