Contents

[Welcome to the Quest On Demand Technical Preview Program! 2](#_Toc476223073)

[On Demand Policy Management 2](#_Toc476223074)

[On Demand Policy Management test parameters: 3](#_Toc476223075)

[On Demand Policy Management test cases: 3](#_Toc476223076)

[On Demand Backup and Recovery 3](#_Toc476223077)

[On Demand Backup and Recovery test parameters: 3](#_Toc476223078)

[On Demand Backup and Recovery test cases: 4](#_Toc476223079)

[Sign-in, Sign-up [Illustrated test case #1] 5](#_Toc476223080)

[On Demand Policy Creation and Export [Illustrated test case #2] 11](#_Toc476223081)

[Backup and recover user attributes [Illustrated test case #3]: 17](#_Toc476223082)

[Part one: Configuration 17](#_Toc476223083)

[Part two: Recover user attributes: 20](#_Toc476223084)

# Welcome to the Quest On Demand Technical Preview Program!

Thank you for your interest in the Quest On Demand Technical Preview Program scheduled from March 1 to May 1, 2017.   This new platform is the beginning of a portfolio transformation that will enable consumption of Quest management capabilities through a software as a service (SaaS) model. The Technical Preview is an early access program designed to allow valued customers and Quest “friends” to help shape the future. We strive to enhance value through feedback and we will accelerate the pace of innovation once the platform is released to the general public. We hope to get honest and constructive feedback from tech preview participants through various means, including face-to-face, conference calls, email, product support, and social media. Together we can make managing the cloud effortless.

Our On Demand Technical Preview will feature two distinct product modules:

* Backup and Recovery for Azure AD
* Policy Management for Skype for Business Online

The tech preview of the Backup and Recovery for Azure AD module allows you to rapidly and reliably backup and recover Azure AD and Office 365 users, groups and group membership. Using the Policy Management for Skype for Business Online, you can set, enforce, and restrict Skype policies from a central console using Azure AD membership.

Over time, we will extend the scope of the On Demand solution to include other Quest product capabilities such as migration, license management, and audit.

During the technology preview time frame, upgrades and the addition of new features will require maintenance during business hours. You will be notified of planned maintenance windows and you will be able to access a web page that displays the status of the On Demand shell.

As part of the Technical Preview, we have provided a set of “kick start” test cases. These test cases are broken up based on the two modules referenced above. While you only need to execute the test cases for the product you signed up to evaluate, you have access to both modules and are strongly encouraged to explore both offerings. You are welcome to use the Technology Preview with a production Office 365 or Azure AD tenant, but we would recommend that you start your evaluation with a test tenant and move to a production tenant once you become familiar with the On Demand user interface and tasks.

# On Demand Policy Management

Native Office 365 tools do not provide a simple, scalable, and automated means of granting or restricting access to product features for groups of employees. Manual provisioning through multiple interfaces often creates disjointed security policies which can increase risk and complicate compliance.

On Demand Policy Management for Skype for Business Online provides a simple and efficient way to dynamically enforce Skype policies based on Azure AD group membership. A simple step by step interface facilitates the creation of policies (e.g. disallow attachments) that can be applied to groups of users. Once enabled, policies are automatically enforced with users always receiving the correct policy setting based on group membership.

## On Demand Policy Management test parameters:

The following test parameters are recommended for effective testing of On Demand Policy Management for Skype for Business.

* A test or production Office 365 tenant. We recommend starting with a test tenant and then moving to a production tenant once you are familiar with On Demand operations.
* Limit usage to 50,000 provisioned users. If you need to increase the number of users managed by On Demand Policy Management, please contact support.
* We encourage you to test On Demand Policy Management with more than one tenant if possible.  The platform supports multi-tenant registration.

## On Demand Policy Management test cases:

The following test cases will help you evaluate whether On Demand Policy Management is a good fit for your environment.

* **Sign-in, Sign-up [Illustrated test case #1]**: If you have a current Quest account with the support portal you can use your current user name and password for Sign-in. If not, please Sign Up to create an account.
* **On Demand Policy Creation & Export [Illustrated test case #2]**: On Demand Policy Management allows you to set, enforce, and restrict access to Skype for Business Online policies features automatically for large groups of users. To perform the use case:
  1. Provide Skype for Business Online credentials.
  2. Create policy management rule and associate with a group.
  3. Enable one or more rules.
  4. Optionally export rule contents to a CSV file.

# On Demand Backup and Recovery

Many organizations assume that Azure Active Directory functions the same way as on premises Active Directory. However, there are important differences. For example, for Azure AD:

* Groups are not stored in the recycle bin after deletion.
* Deleted users can only be restored within 30 days and there’s no way to recover them afterward?

On Demand Backup and recovery removes these limitations, enabling you to easily backup and restore Azure AD users, individual user attributes, groups, and even users that have been removed from the Office 365 recycle bin. This greatly simplifies the process of recovering from errors or malicious attack, saving your organization time and money.

## On Demand Backup and Recovery test parameters:

The following test parameters are recommended for effective testing of On Demand Backup and Recovery for Azure AD.

* A test or production Office 365 tenant. We recommend starting with a test tenant and then moving to a production tenant once you are familiar with On Demand operations.
* Limit usage to 50,000 provisioned users. If you need to increase the number of users managed by On Demand Backup and Recovery for Azure AD, please contact support.
* We encourage you to test On Demand Backup and Recovery for Azure AD with more than one tenant if possible.  The platform supports multi-tenant registration.

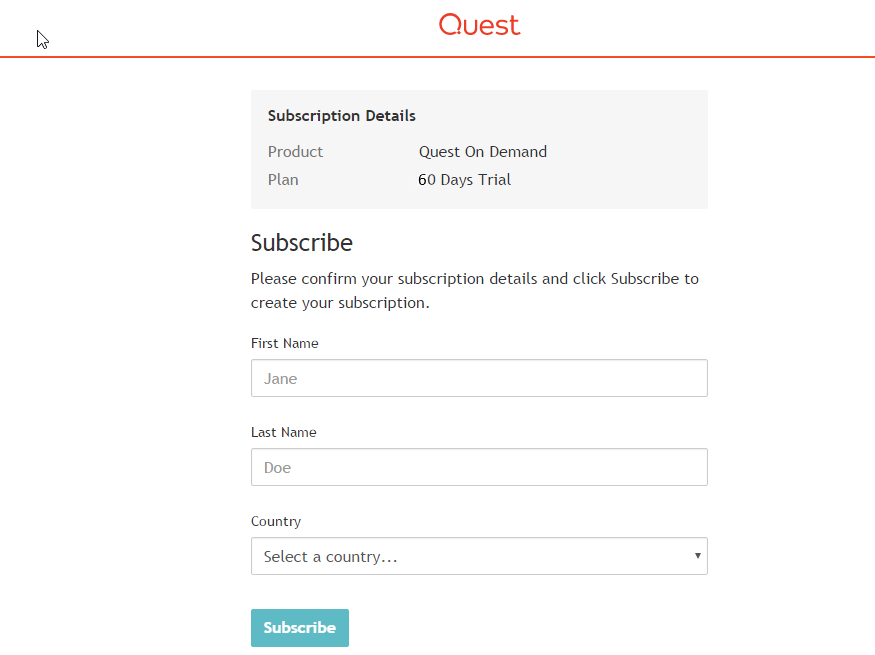
## On Demand Backup and Recovery test cases:

The following test cases will help you evaluate On Demand Backup and Recovery.

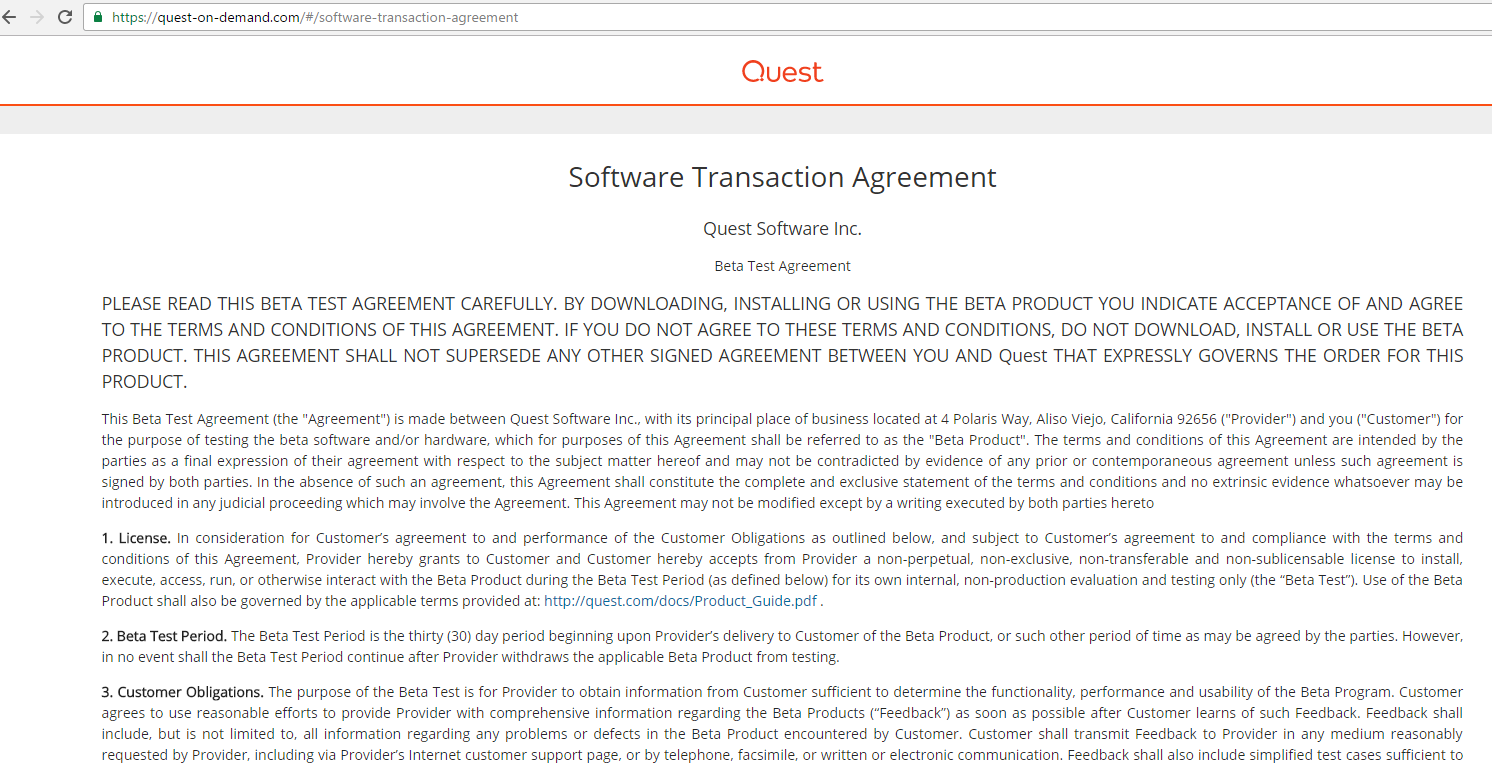
* **Sign-in, Sign-up [Illustrated test case #1]:** If you have a current Quest account with the support portal, you can use your current user name and password for Sign-in. If not, please Sign Up to create an account
* **Backup and recover a user attributes [Illustrated test case #3]**: On Demand Backup and Recovery allows you to backup and restore individual user attributes, enabling rapid recovery from bulk attribute changes that have been made in error or maliciously. To perform the use case:
  1. Create an Azure AD backup using On Demand Backup and Recovery.
  2. Change one or more attributes in the Azure AD portal.
  3. Restore the back up using On Demand Backup and Recovery.
  4. Confirm that user attributes have been restored to their original state.
* **Backup and recover a group**: On Demand Backup and Recovery allows you to backup and recreate[[1]](#footnote-1) user groups including group membership and subgroups. This can save hours of labor and avoid lengthy support calls with Microsoft since groups cannot be recovered natively through the Azure AD portal or the Office 365 Admin portals. To perform the use case:
  1. Create an Azure AD backup using On Demand Backup and Recovery.
  2. Delete an Azure AD group in the Azure AD portal.
  3. Restore the group using On Demand Backup and Recovery.
  4. Confirm that the group has been restored to Azure AD.
* **Backup and recover a deleted user**: On Demand Backup and Recovery allows you to backup and restore users from a single interface instead of having to navigate between multiple interfaces in native tools. To perform the use case:
  1. Create an Azure AD backup using On Demand Backup and Recovery.
  2. Delete one or more Azure AD users in the Azure AD portal.
  3. Restore the users using On Demand Backup and Recovery[[2]](#footnote-2).
  4. Confirm that users have been restored to their original state.
* **Backup and recover a user deleted from the O365 recycle bin**: On Demand Backup and Recovery allows you to backup and recreate users that have been permanently deleted from the Office 365 recycle bin.[[3]](#footnote-3) Since Microsoft maintains a strict 30 day retention policy on items in the recycle bin, users can be permanently deleted without the admins knowledge. On Demand Backup and Recovery makes it possible to recover these users without opening a support case with Microsoft. To perform the use case:
  1. Create an Azure AD backup using On Demand Backup and Recovery.
  2. Delete one or more Azure AD users in the Azure AD portal.
  3. Remove those same users from the Office 365 recycle bin.
  4. Restore users using On Demand Backup and Recovery.[[4]](#footnote-4)
  5. Confirm that users have been restored to Azure AD.

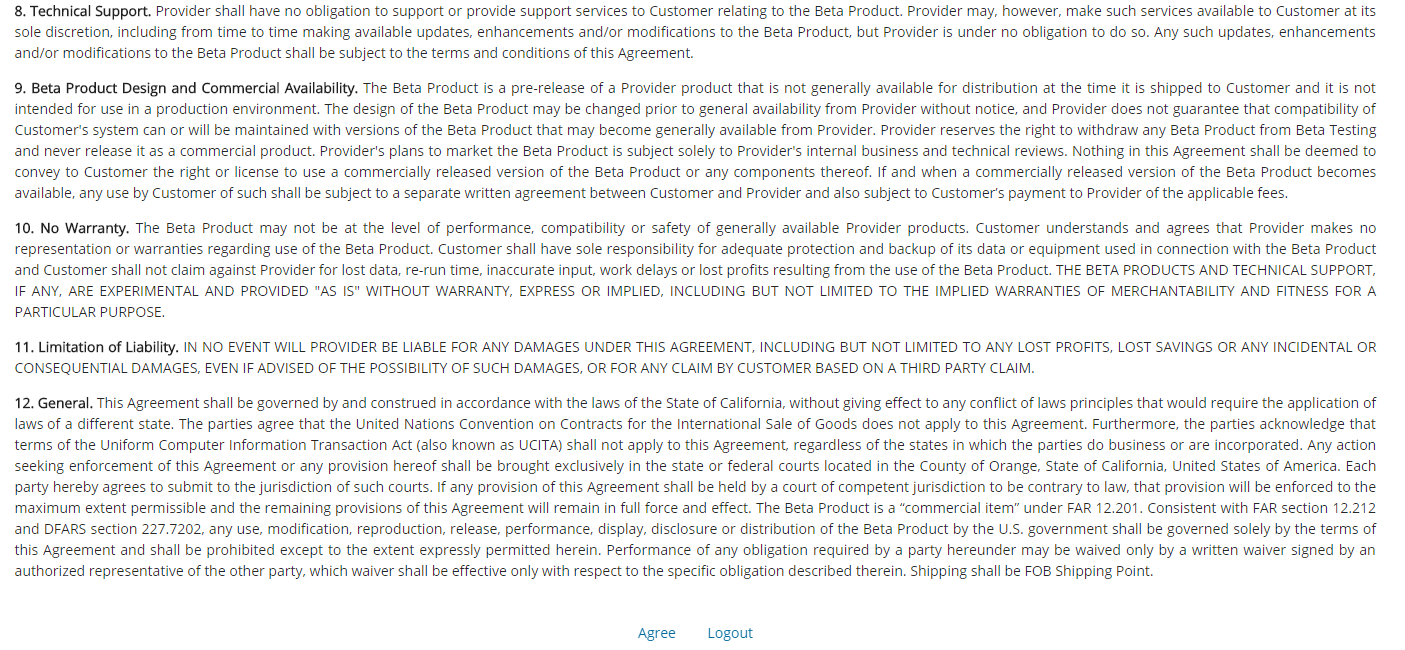
# Sign-in, Sign-up [Illustrated test case #1]

**Go to:** <https://quest-on-demand.com/landing>to subscribe and Register by adding your information

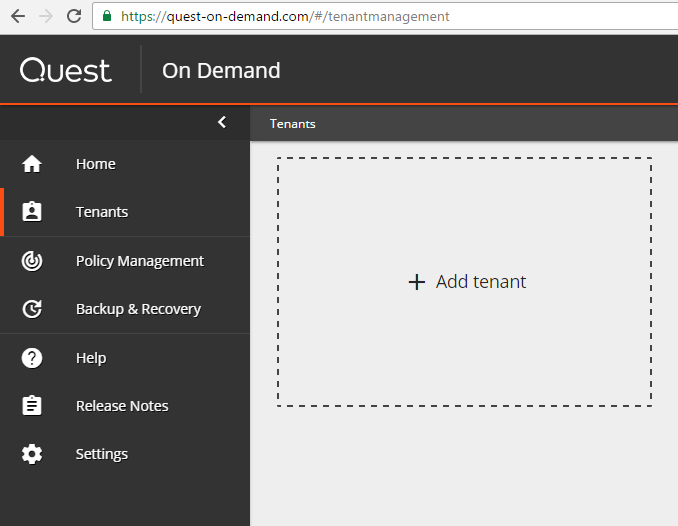


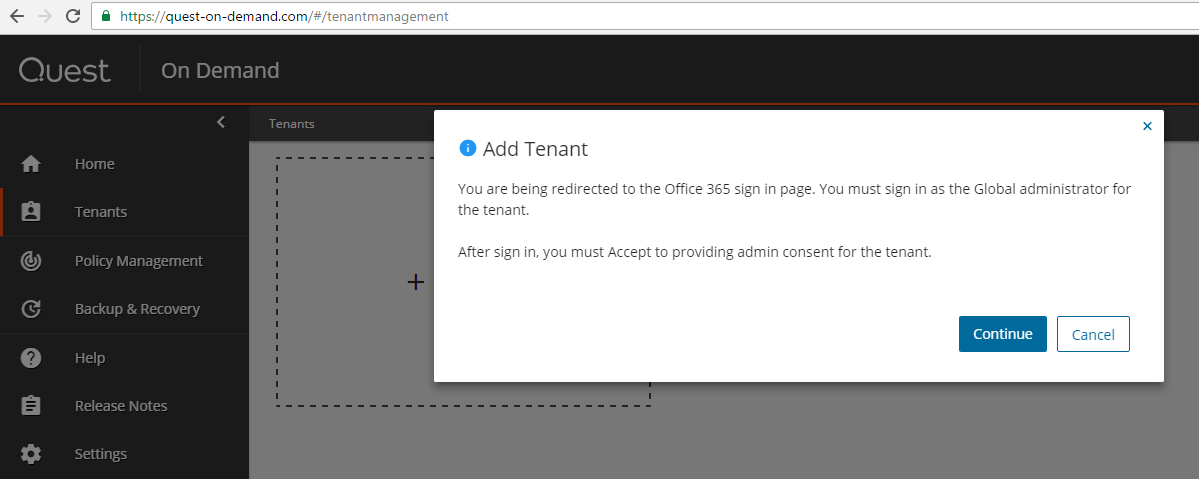
**Step Two:** Agree to the Software EULA

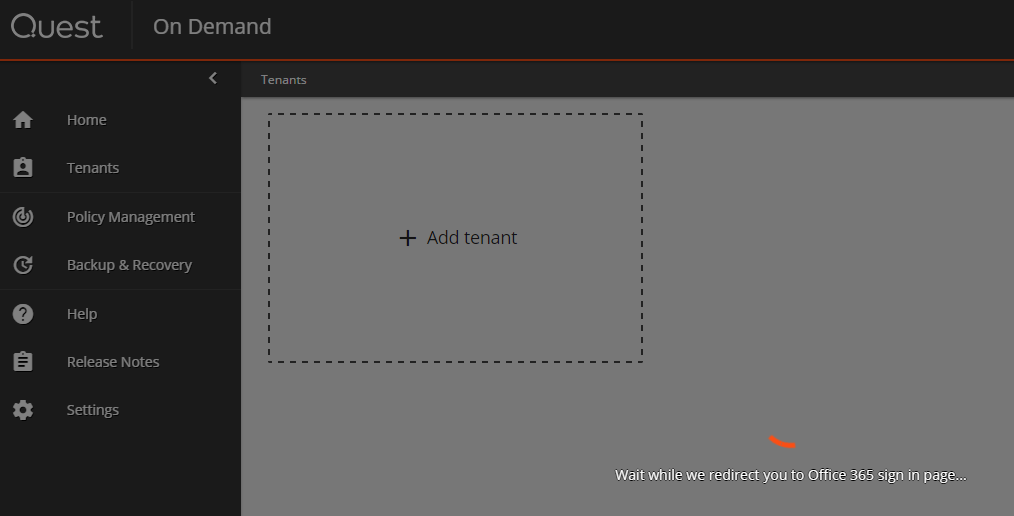




**Step Three:** Add Tenant

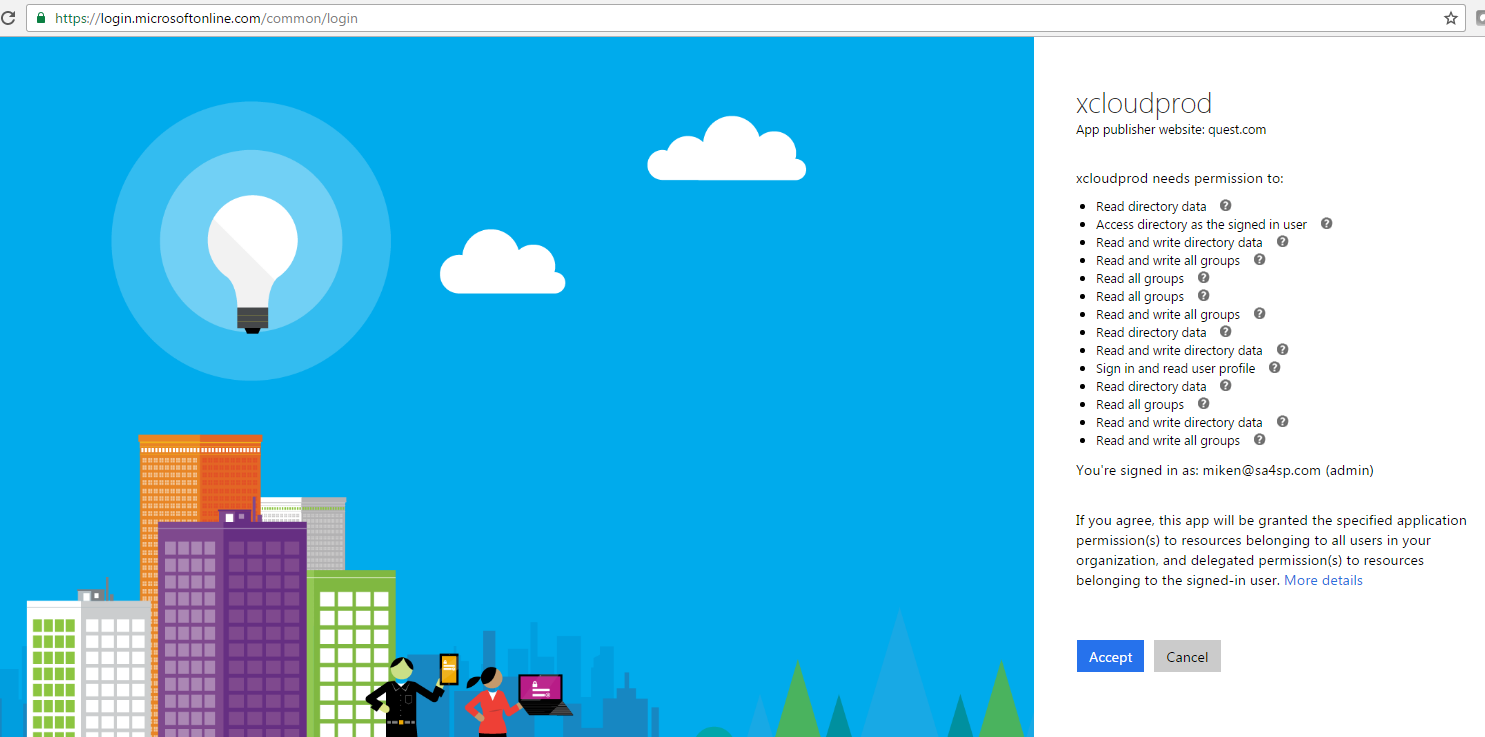




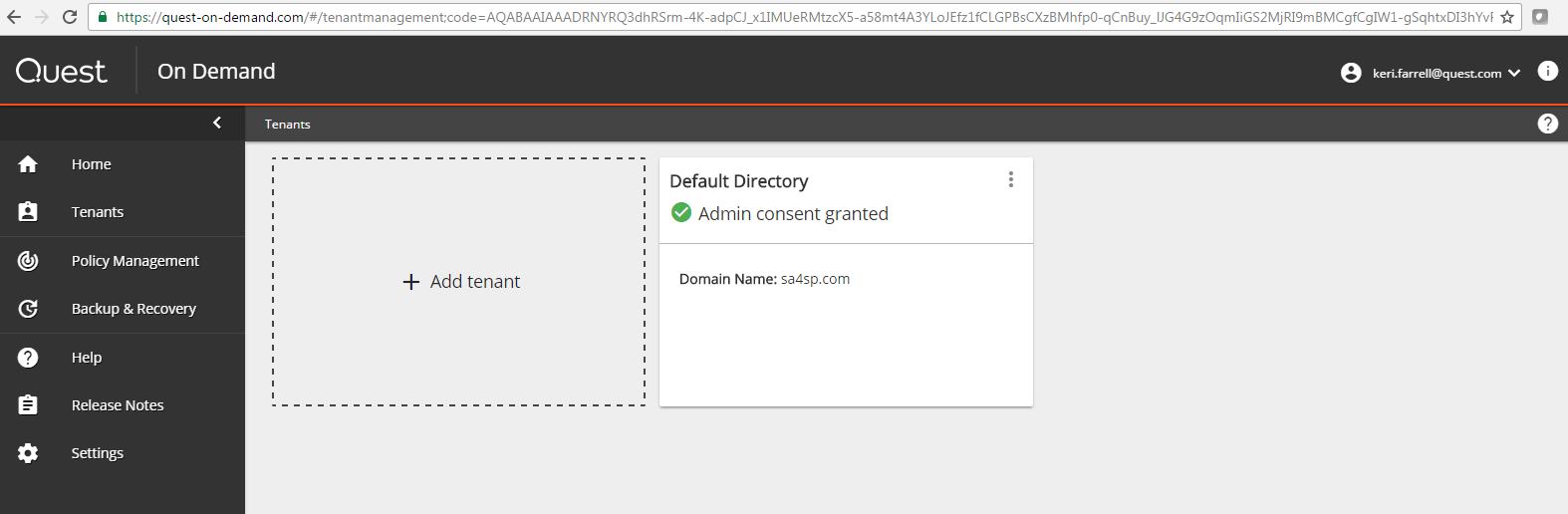


**Step Four:** You will be redirected to the O365 sign in page where you will have to login with your existing tenant to link it to the On Demand portal:

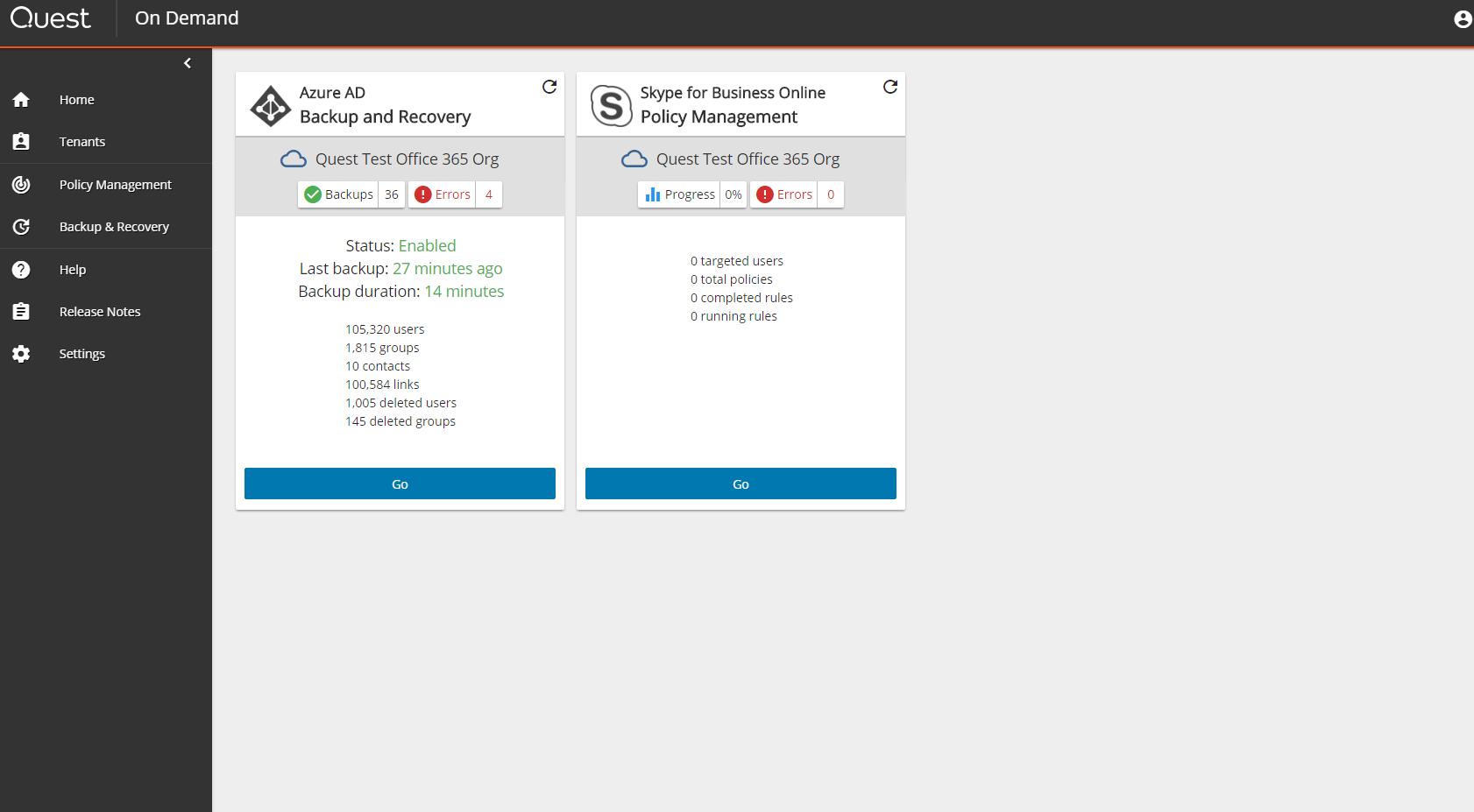




Once your O365 tenant is registered with the On Demand portal, it will be linked and you will be redirected back to the **Tenants** page.



**Step Five:** Select **Home** and you are ready to start using **Backup and Recovery for Azure AD** and\or **Policy Management for Skype for Business Online**. Proceed to the next chapter for instructions on how to use each module.



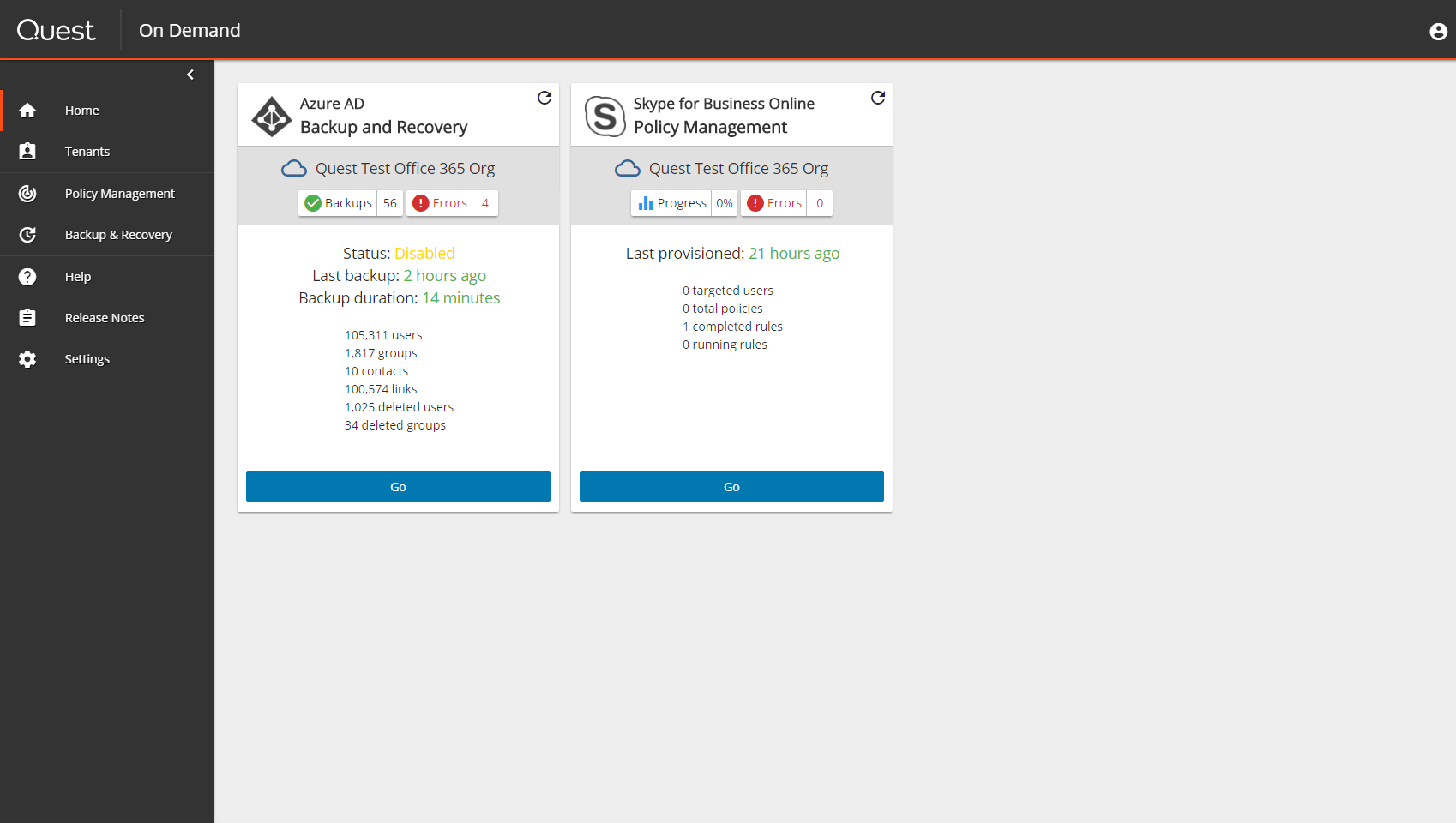
# On Demand Policy Creation and Application [Illustrated test case #2]

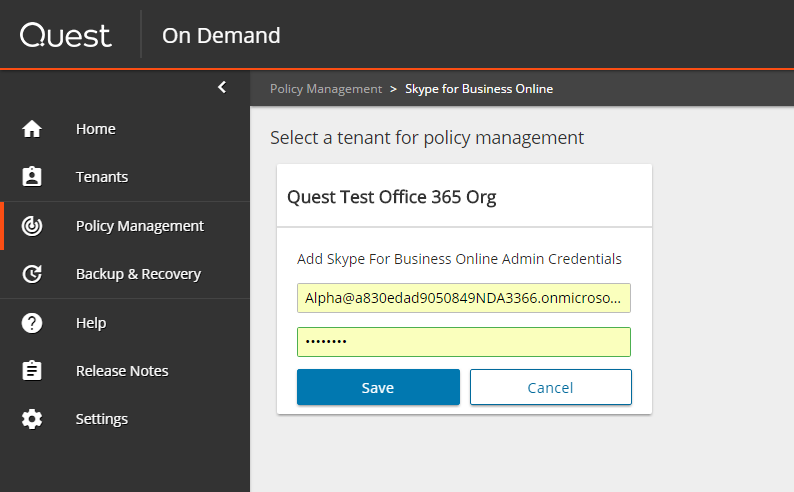
Policy Management consists of 3 key steps:

1. Add and name a rule
2. Add a target list of groups and users.
3. Choose the Skype for Business Online policy features that you want to enable or disable for the target groups and users.

Once the Rule is created you must **Save** it. If you checked the **Enabled** box, the policies are applied immediately. You can leave the **Enabled** box unchecked and apply the rule later. The set of screen captures below describe these steps.

When in the Quest On Demand Home page you can select to enter the Skype for Business Online Policy Management by selecting **Go** at the bottom of the tile.

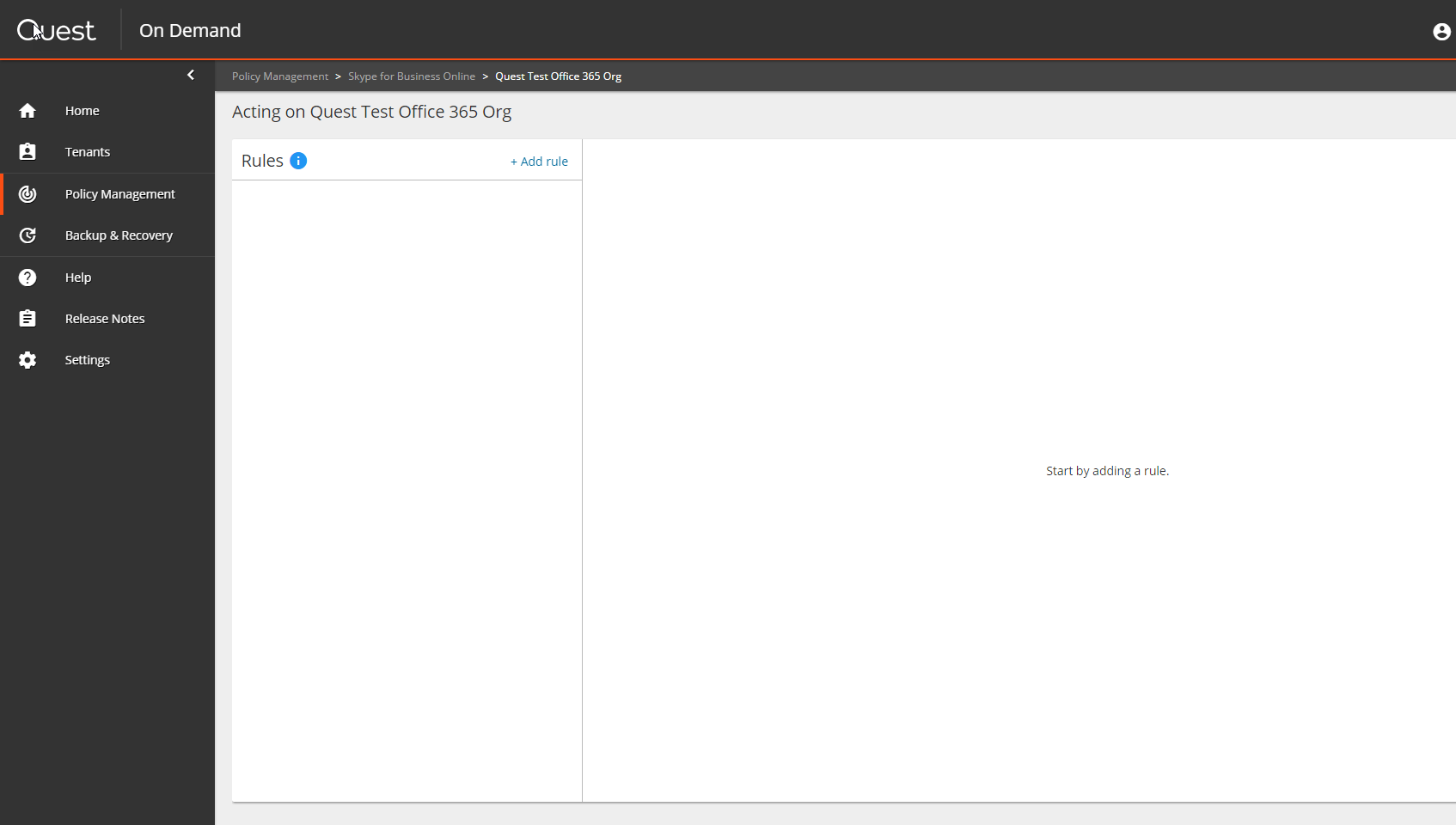


The first prompt from the application is to add Skype for Business credentials. 

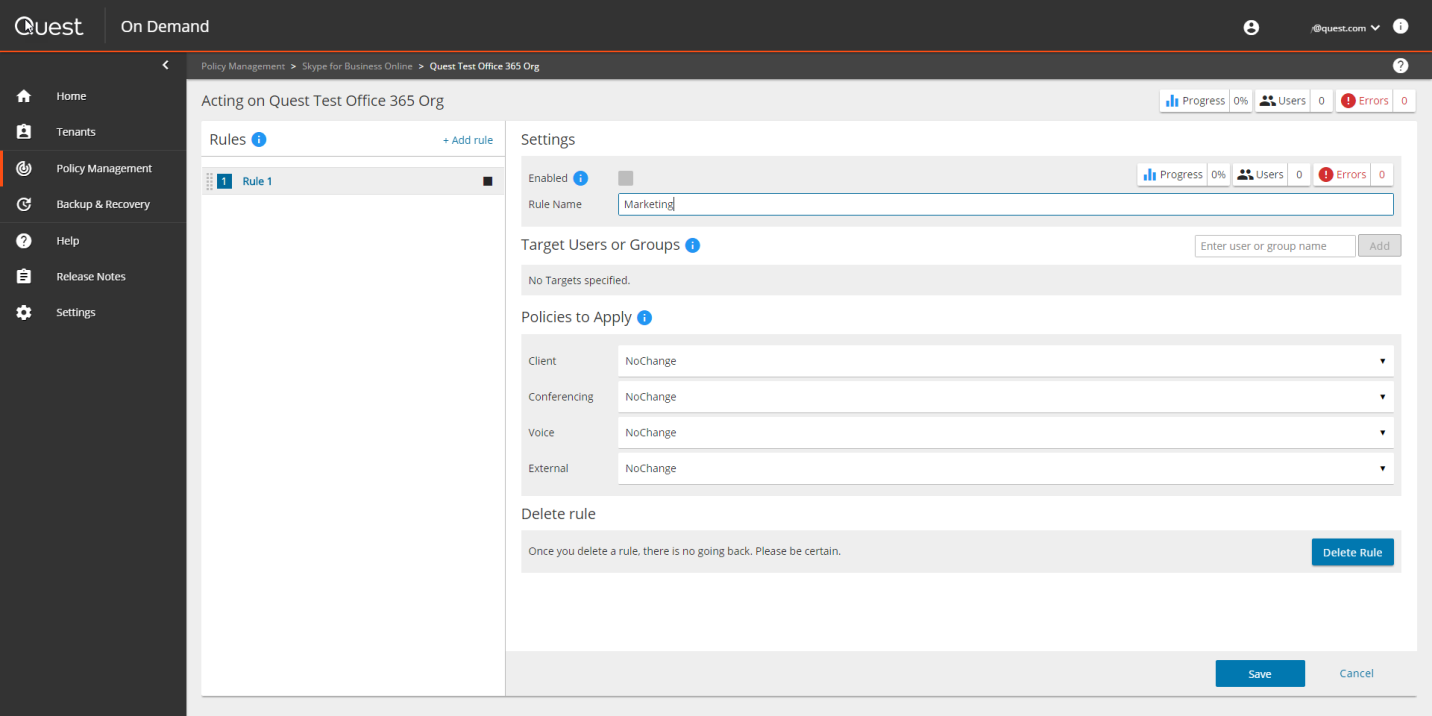
The following Office 365 administrator roles grant full access to Skype for Business Online:

* Global administrator
* User management administrator
* Password administrator
* Skype for Business administrator

After adding credential to access the Skype for Business Online tenant, you must specify a **Rule Name**. The application will automatically prompt you for the rule name at your first entry.



Here, we are creating a new rule named Marketing. We are not saving the workflow at this time, so the interface will still show Rule 1, as it did on start up, but once saved, the rule name and all its values will be applied.



After naming the rule, we will now add target users or groups. In the screen capture below, under **Target Users or Group**s, you can see that we have added **Technical Training** via the pull down menu on the right. This pull down menu auto populates the search based on existing groups in Azure AD. Once you have selected the target user or group, click **Add** and the action is complete.

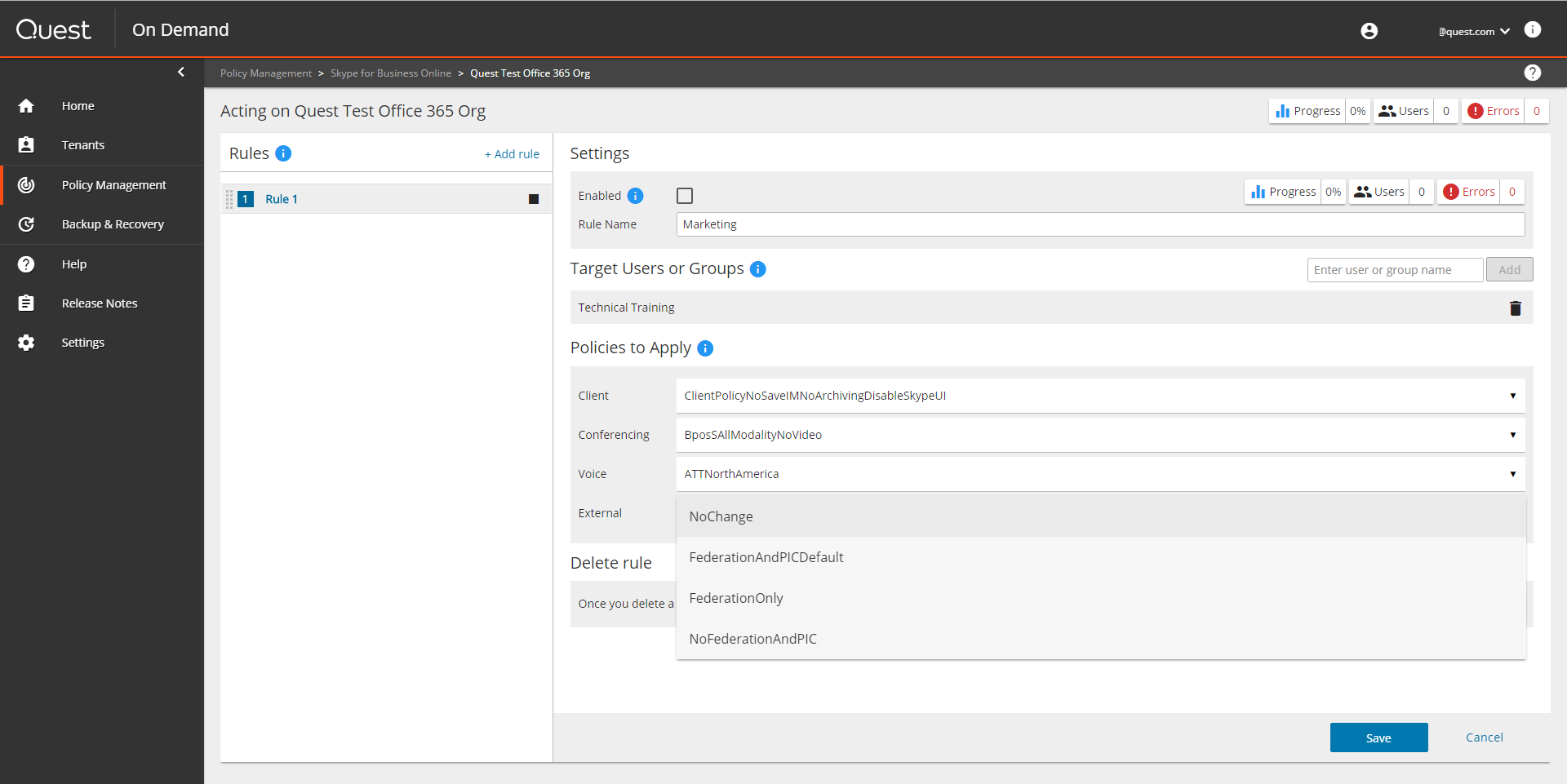


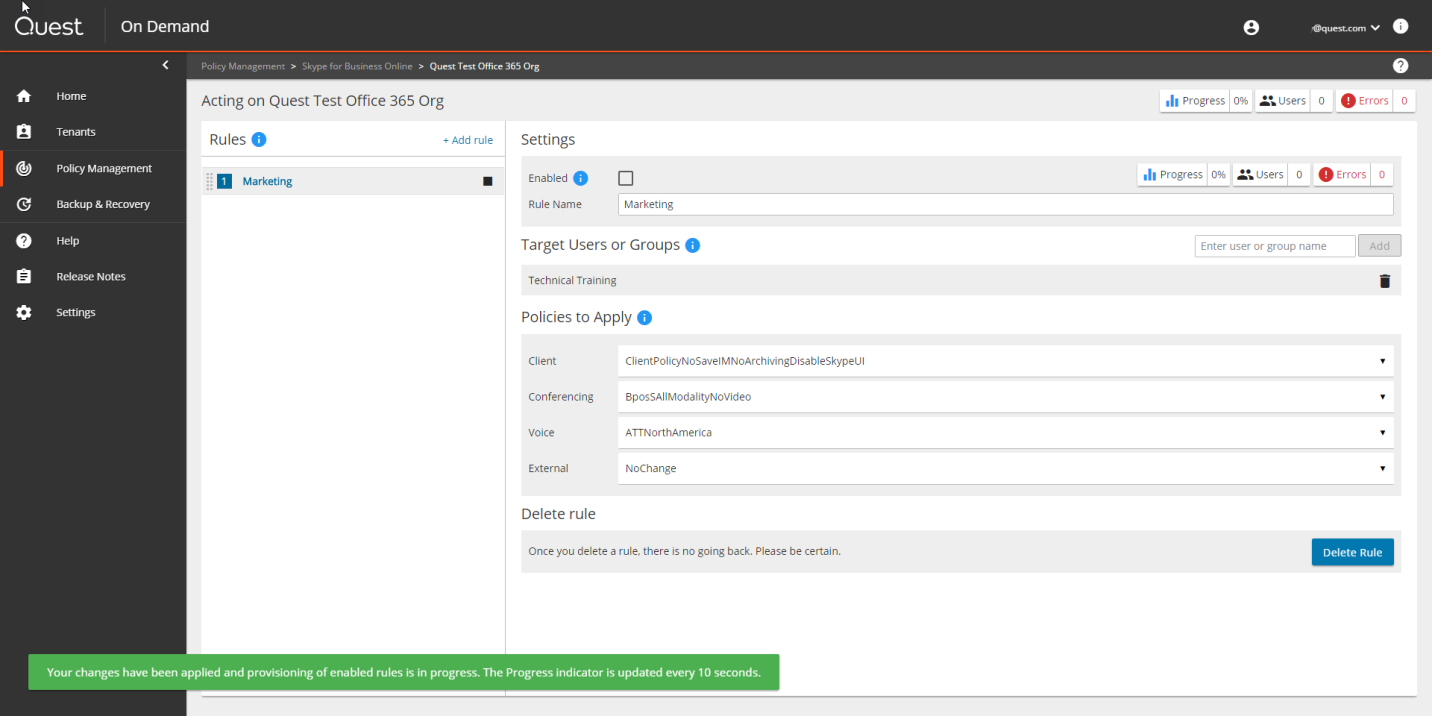
Once the rule name and target users or groups have been defined, it is now time to choose the Skype for Business Online policies (feature entitlements) that will be applied to this target. Once the policy is applied to the target, the application regularly monitors the group membership and ensures all new members are updated with the policy settings associated with the group. As well, when a member leaves the group, they no longer have the policy associated with the group. If they are assigned to a new group, they receive a different policy based on their updated group membership.

The group policies are categorized in 4 segments:

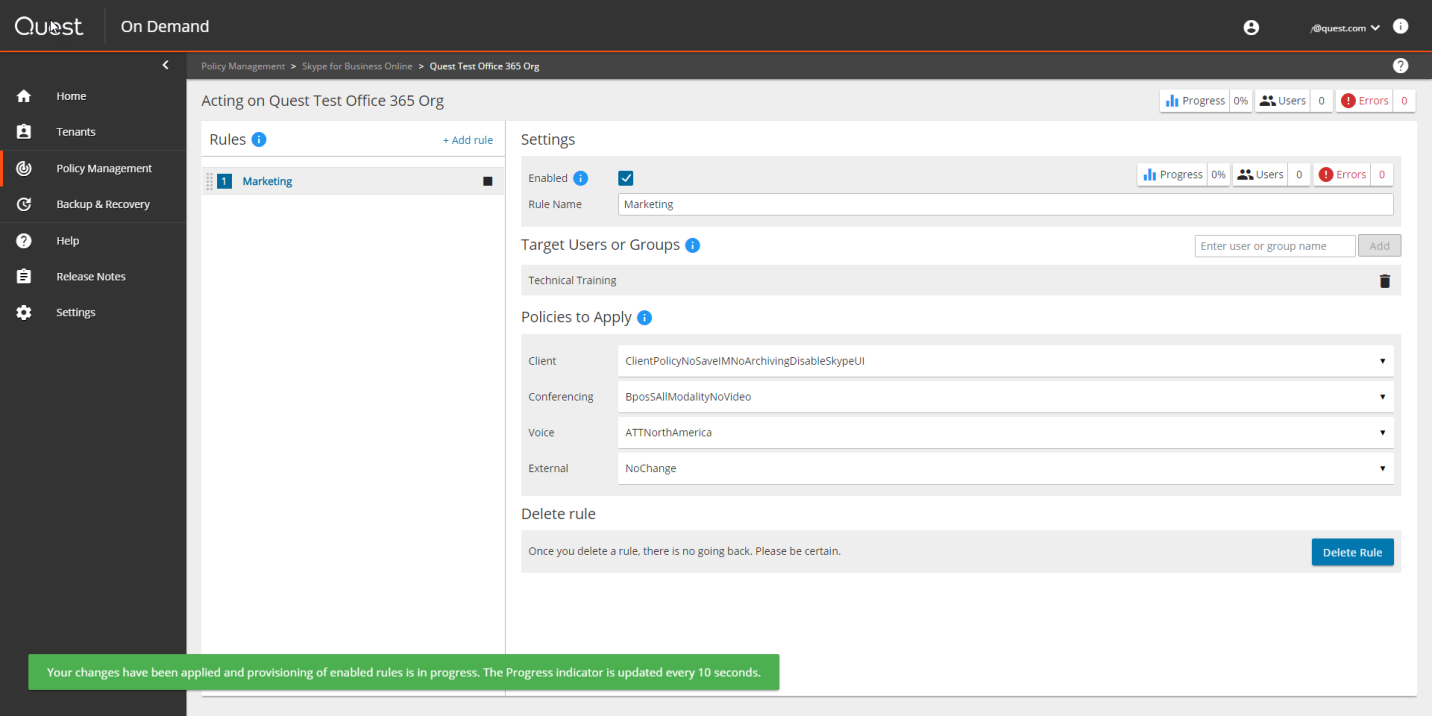
* Client
* Conferencing
* Voice
* External

Each selection box has a pull down menu from which you can choose the setting. In the screen capture below you can see we have selected **(NoSave/NoArchiving)**. For **Conferencing**, we have chosen to disable **(Dialout)**. Since the Skype for Business Online **Voice** capability is region specific we have chosen the **ATTNorthAmerica** provider. Lastly, we are showing the pull down menu on the last category **External**.



Once you have named a rule, added a target, and selected policies, you can now save the entire rule before enabling. 

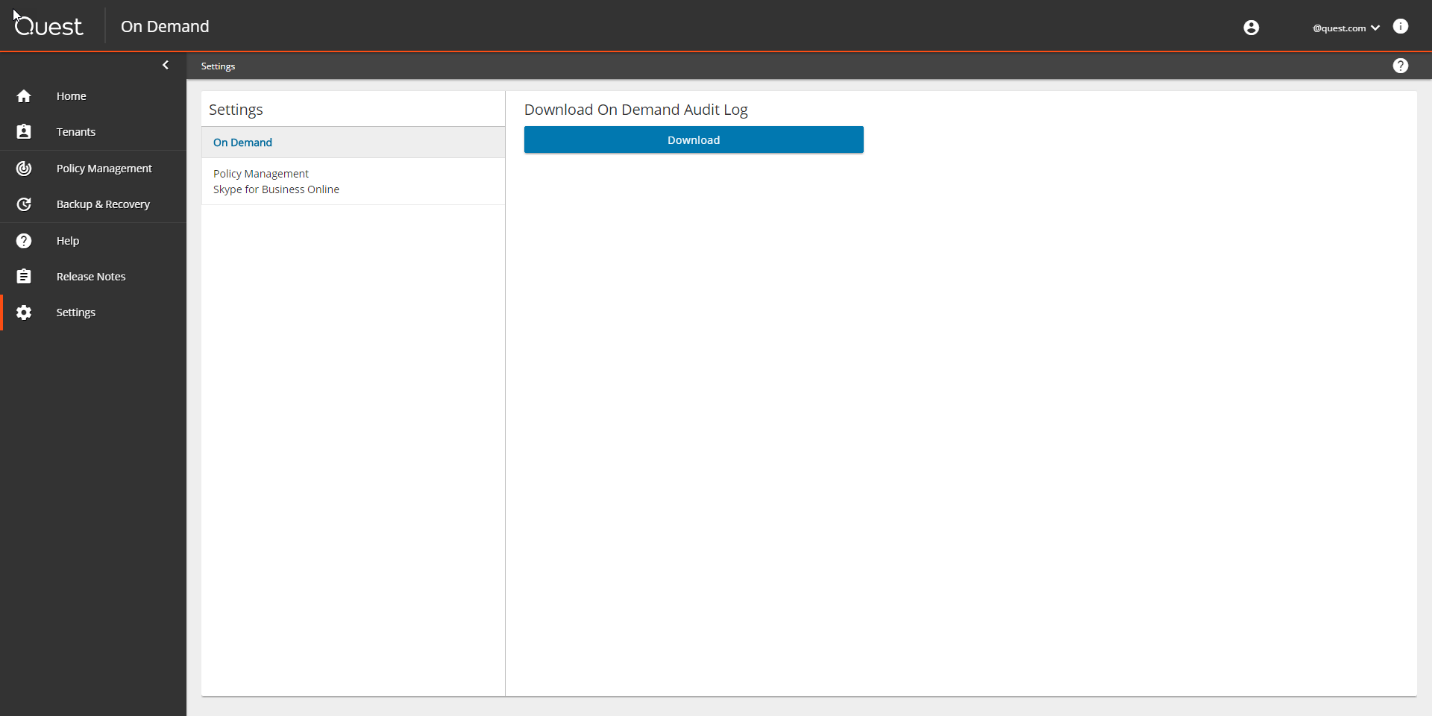
Once the Rule is saved you can select the box labelled “Enabled” to begin the provisioning process.



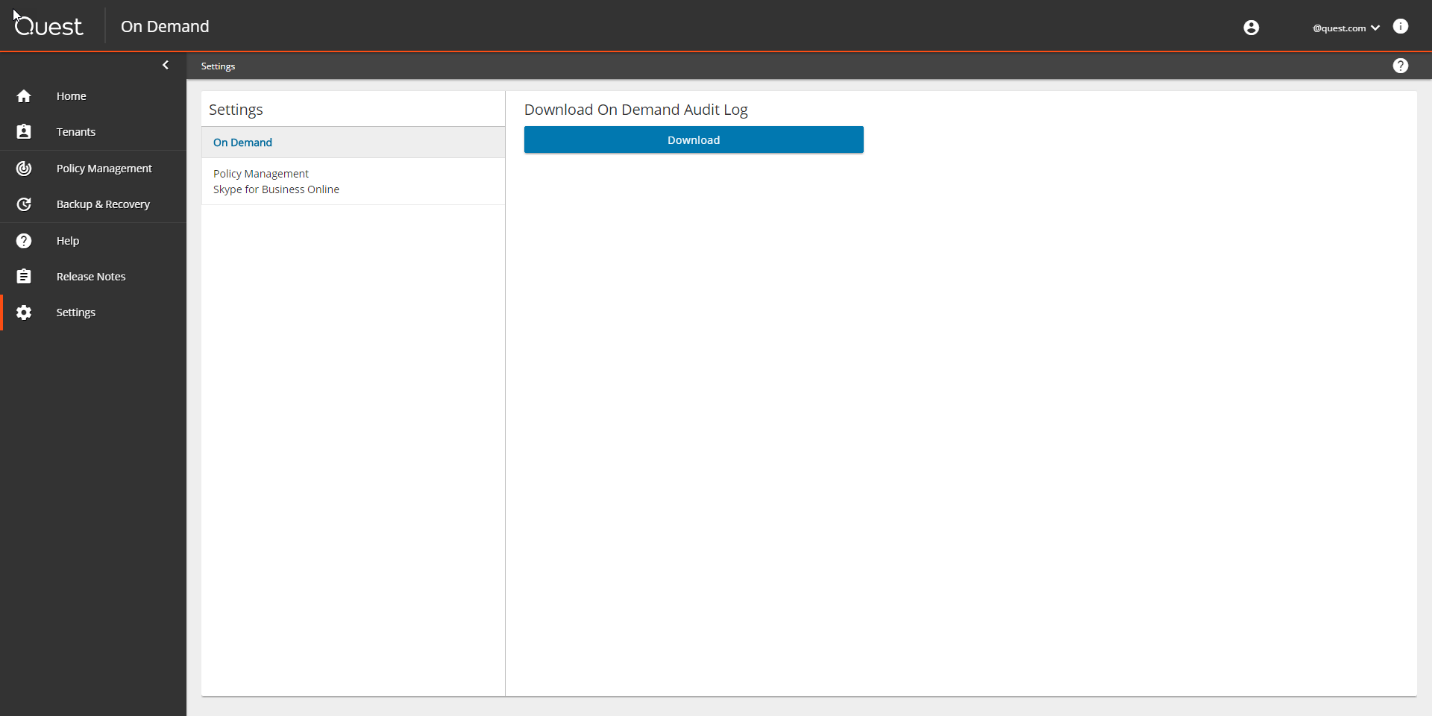
As the application begins to provision the rule, you are provided with a progress update pictured on the upper right. If you are provisioning a rule to a large number of users, this may take a considerable amount of time. Once provisioning is completed, a green checked circle in the **Rules** list associated with the rule named **Marketing** indicates that the rule is now live and active. Following this step, confirm that the policy has been applied by restarting your Skype for Business client and attempting to use the enabled or disabled function.



Finally, the Audit capability selection is under **Settings -> Audit**. Select the log for Policy Management and click Download to download the CSV format log file.



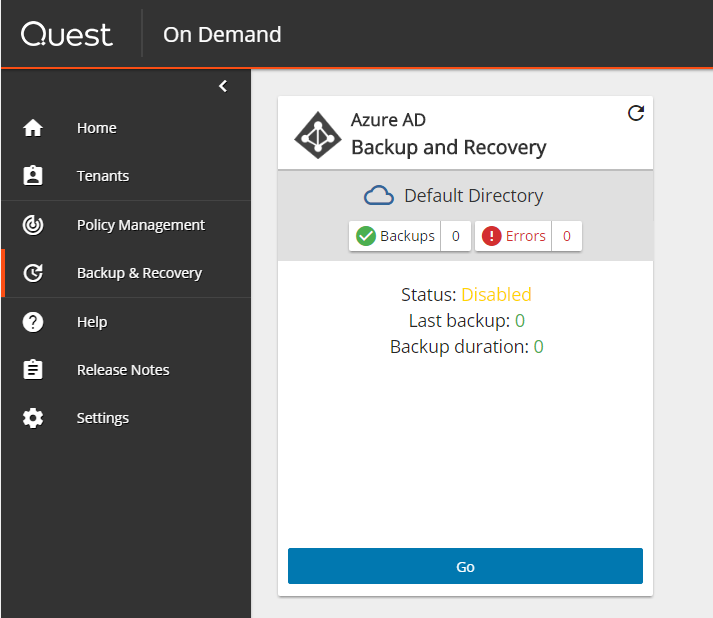
The Audit file is downloaded to your local machine to be reviewed.



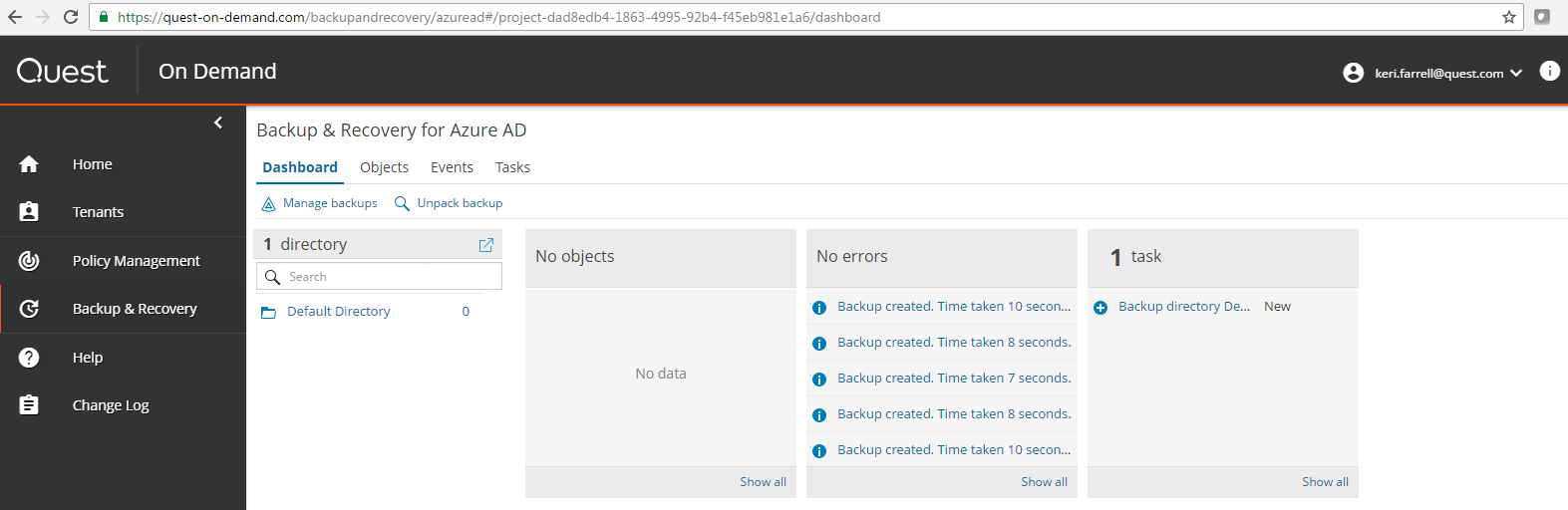
# Backup and recover user attributes [Illustrated test case #3]:

## Part one: Configuration

**Step One:** From the Quest On Demand Home page, on the **Azure AD Backup & Recovery** tile, select **Go.**



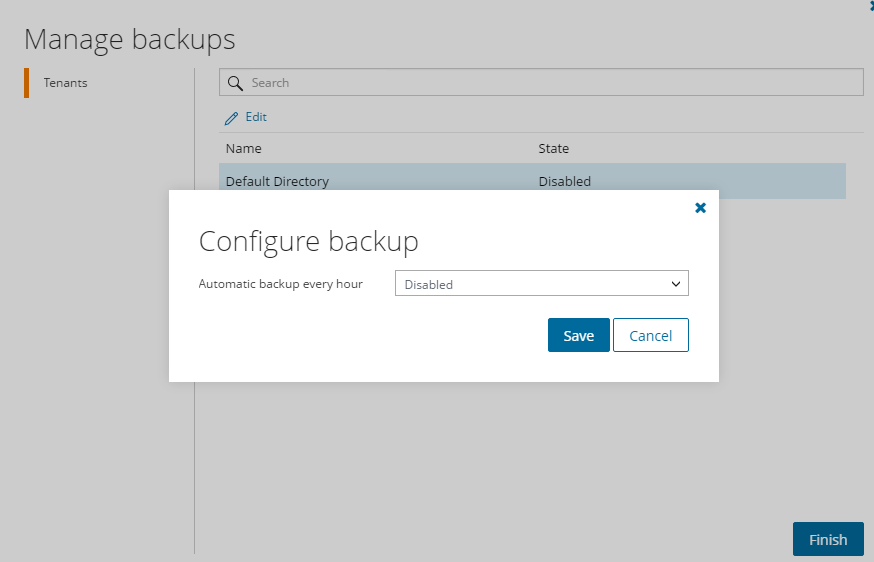
**Step Two:** From On Demand Backup & Recovery for Azure AD, select **Manage** **Backups**



Select **Default Directory** then click **Edit**.

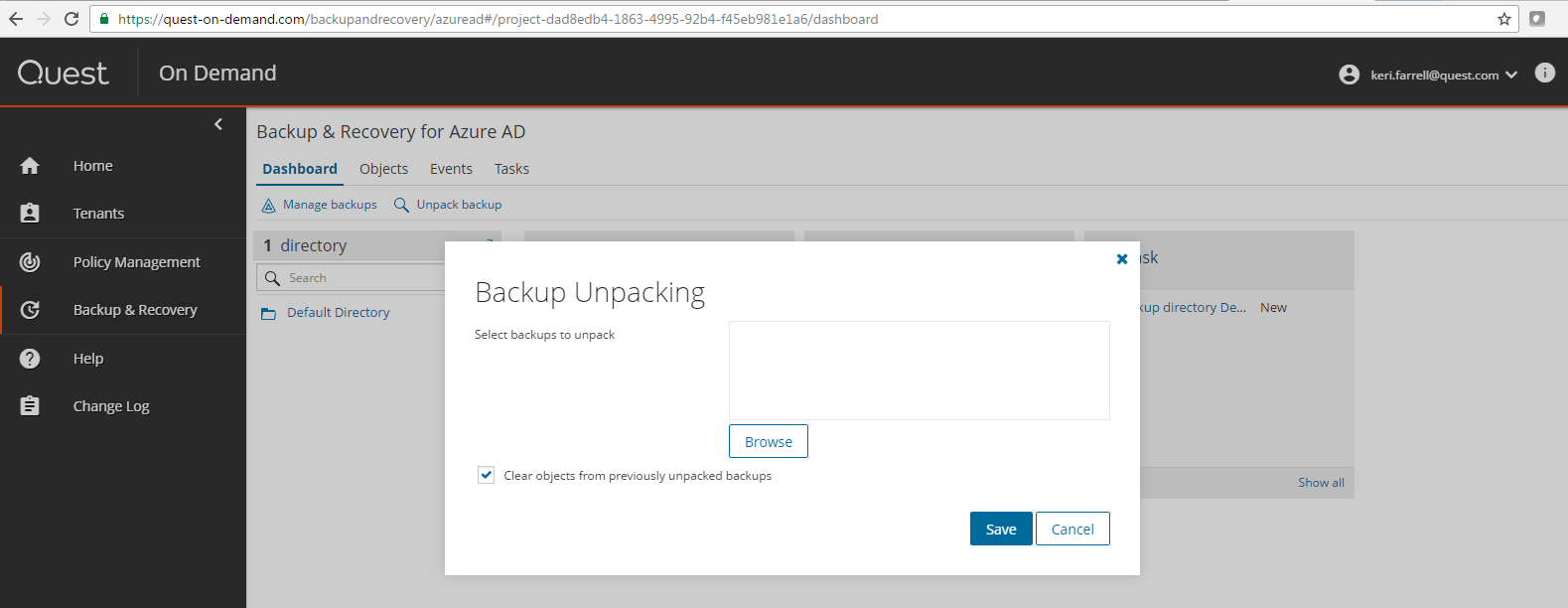
Under **Configure backup,** change **Automatic backup every hour** to **Enabled**.

Click **Save** andthen **Finish.**

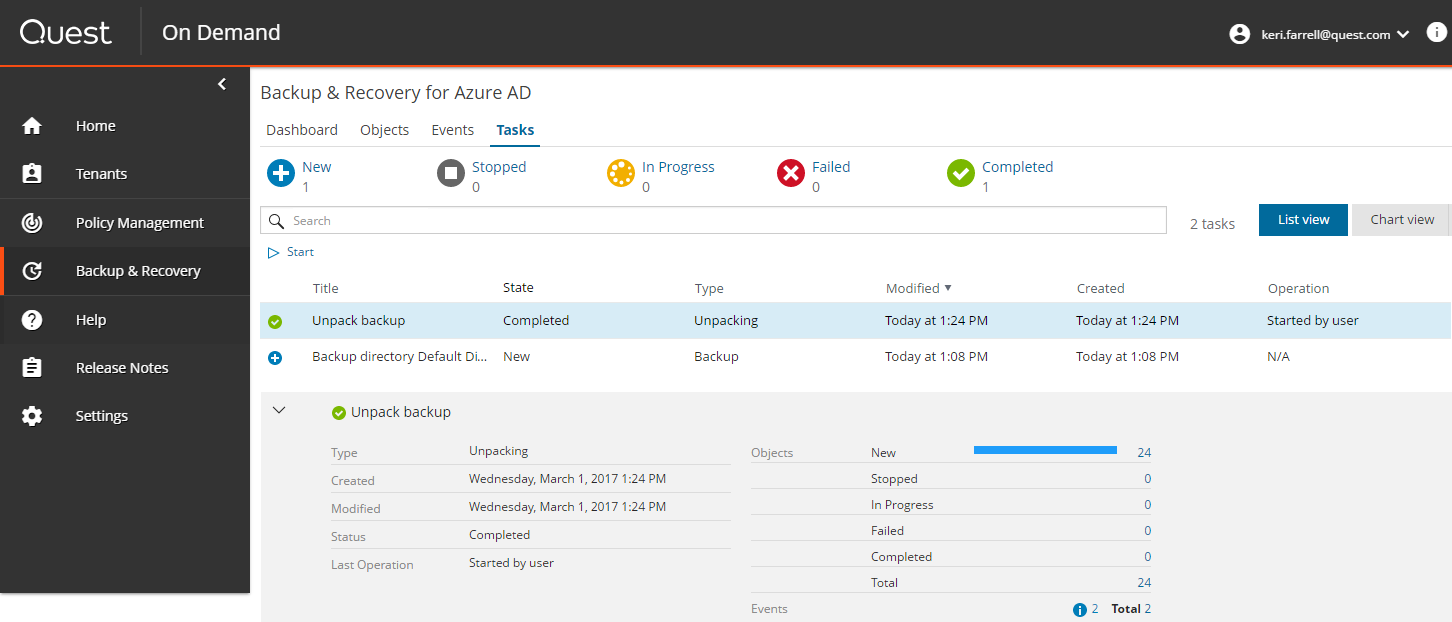


**Step Three:** Click **Unpack backup** (after your backup completes) and then click **Browse** to select your most recent backup

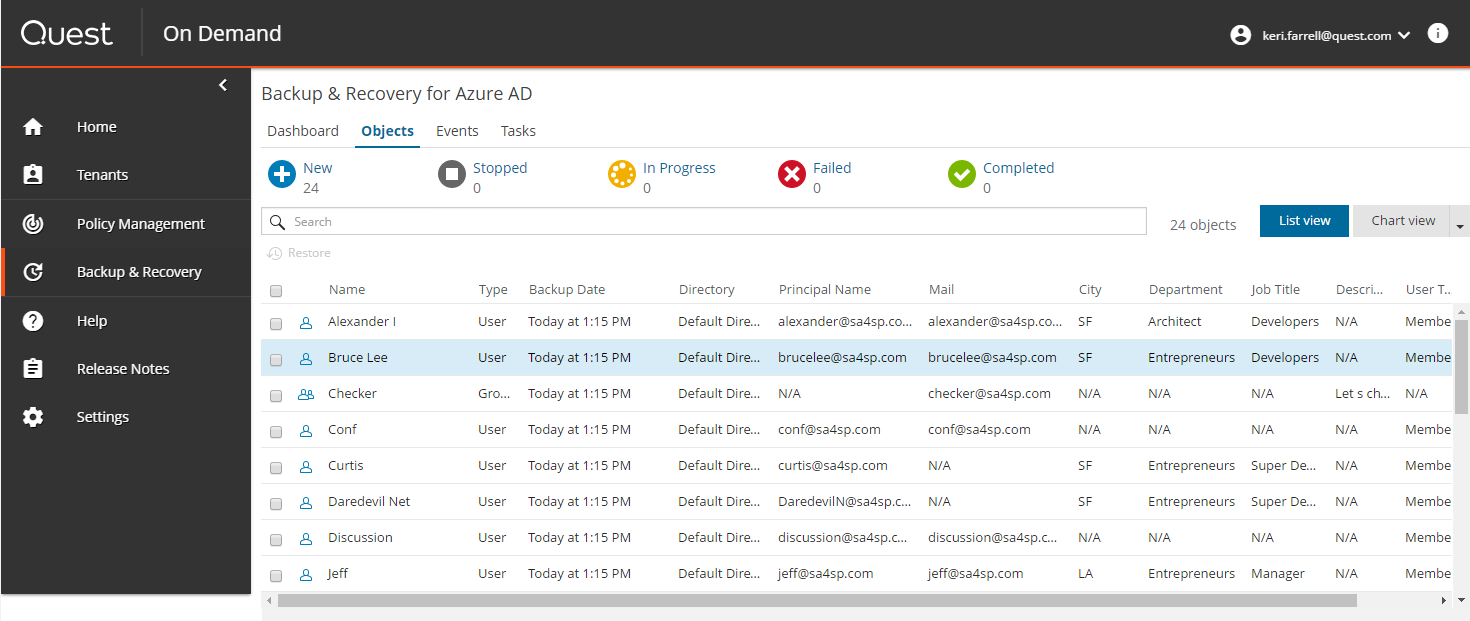
Click **Save**.



You can view the status under **Tasks**:



You can view the list of Azure AD objects in the backup under **Objects:**



## Part two: Recover user attributes:

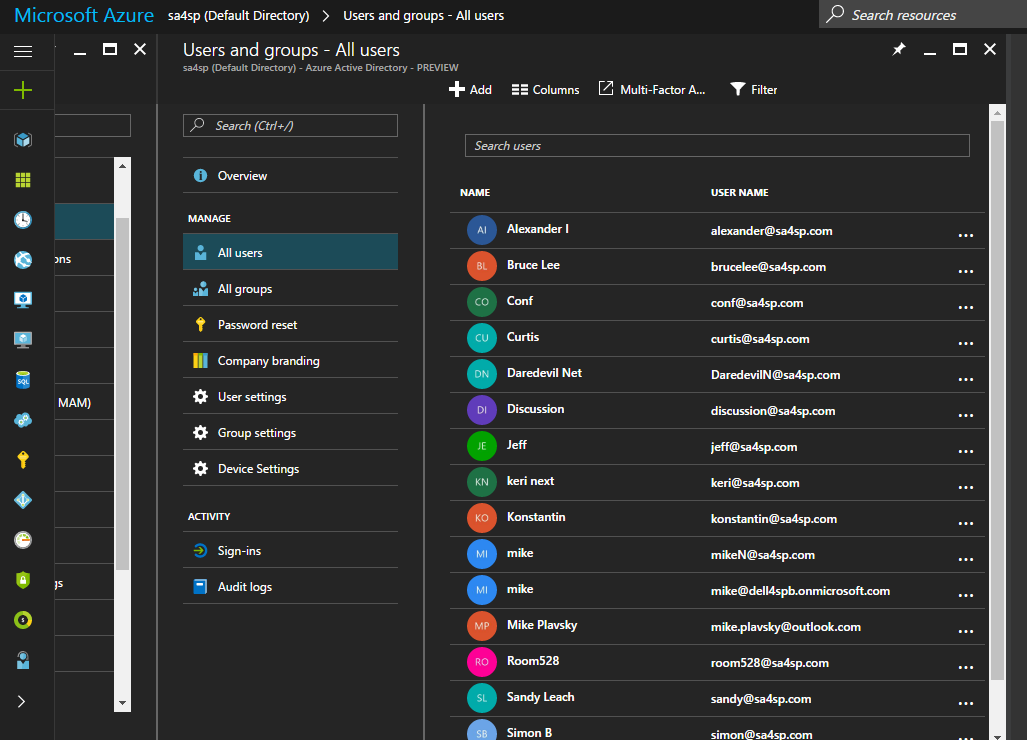
**Step One:** From Quest On Demand Backup & Recovery for Azure AD , click **Objects**.

Pick a user from your backup for which you will change and subsequently restore attributes. Here, the user is Bruce Lee. In the backup, his **Department** is **Entrepreneurs** and his **Job title** is **Developers**.

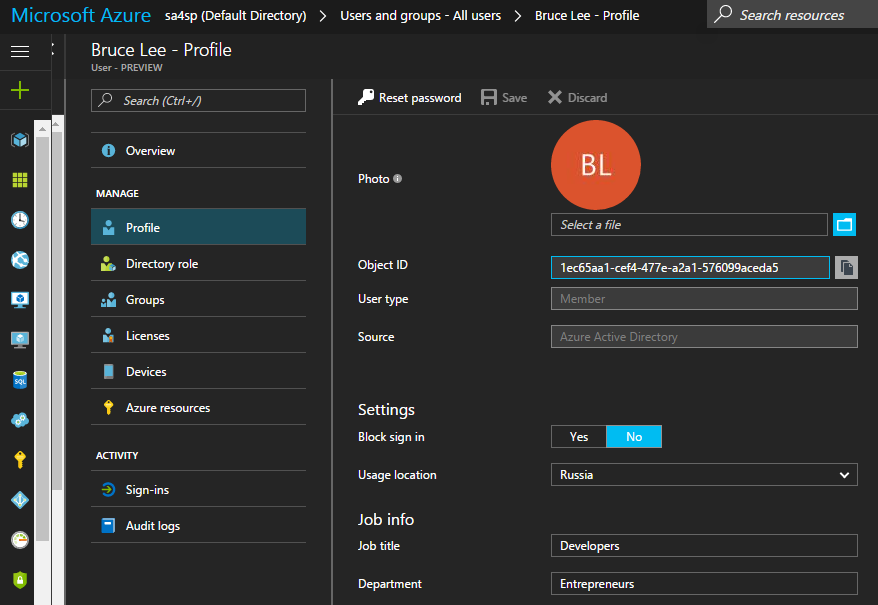


**Step Two:** Go to the **Microsoft Azure AD Portal:** <https://portal.azure.com/>

Select **All Users:**



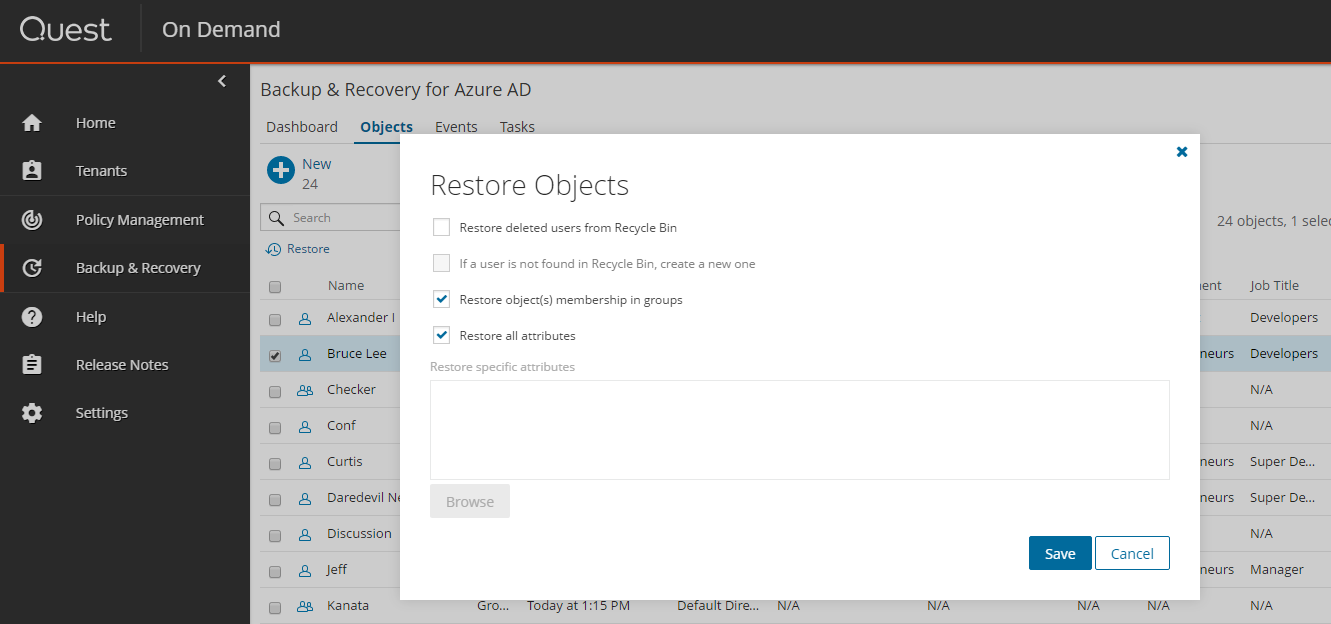
**Step Three:** Select the user **Bruce Lee** and then select **Profile** to edit attributes such as **Department** or **Job title**. Change the attribute contents to values of your choice.





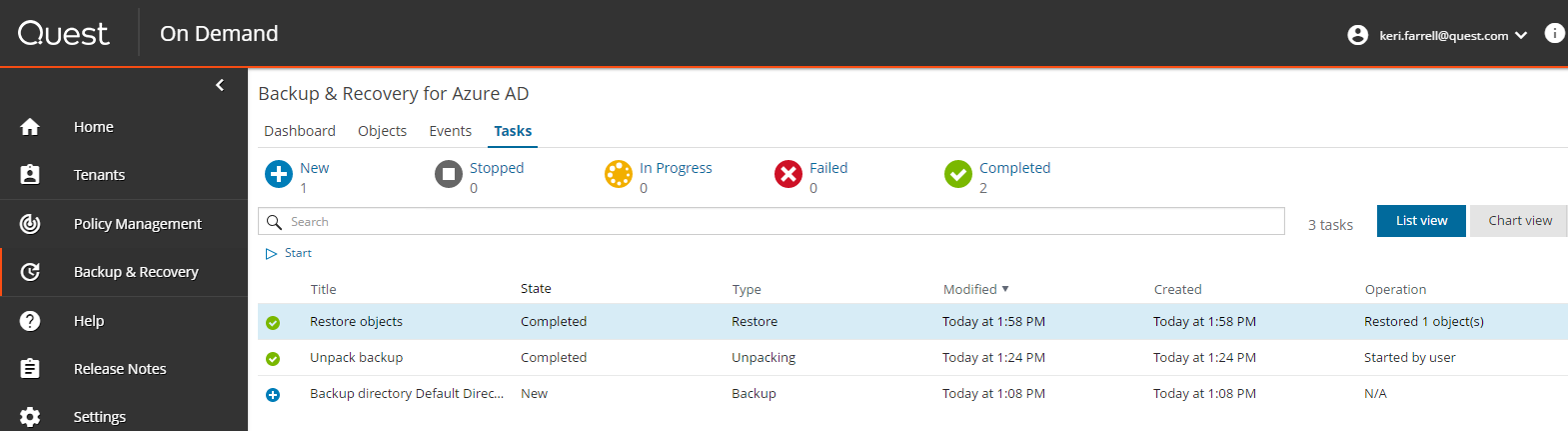
**Step Four:** Back in the **On Demand console**, select **Backup and Recovery** and restore the attributes we just changed.

Select **Bruce Lee** and click **Restore.** Make sure **Restore all attributes** is selected:

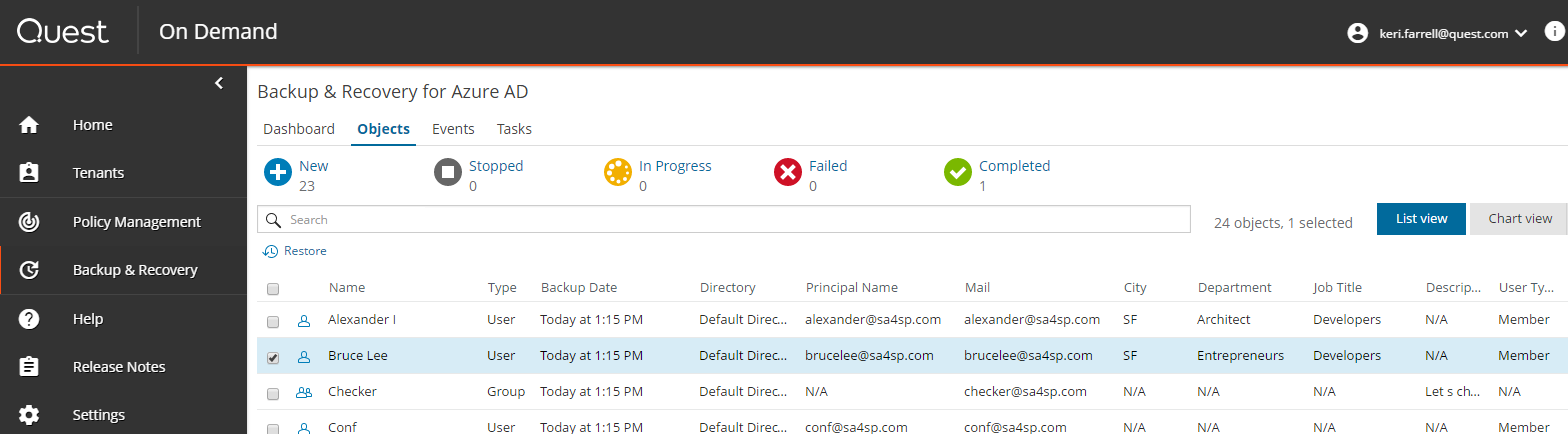


Select **Save** and this users attributes will be restored.

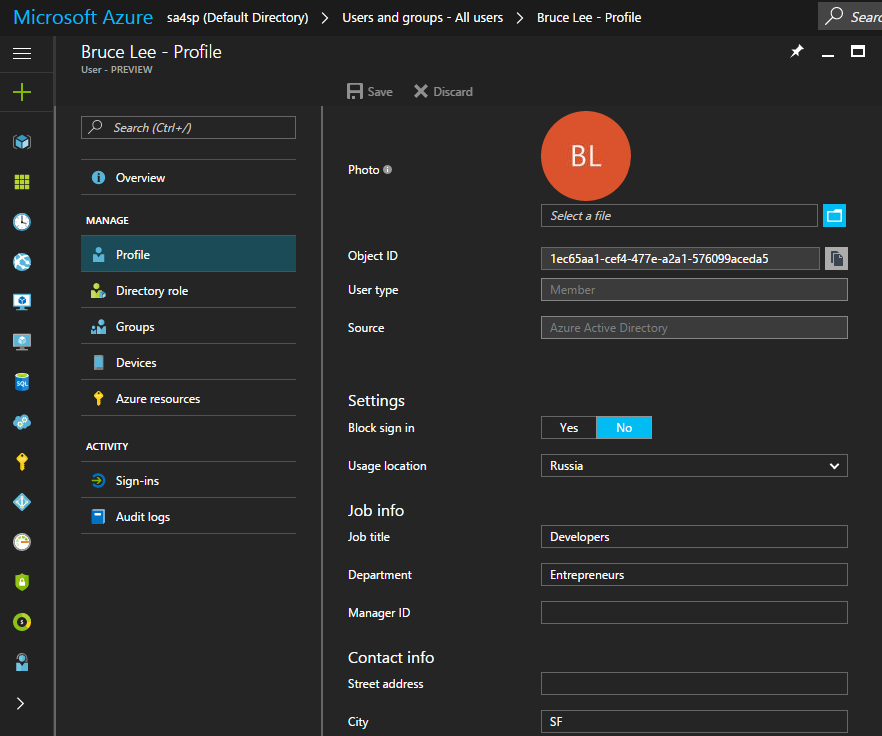
Select **Tasks** to see when the restore is complete.



Select **Objects**. **Bruce Lee** and his attributes have been returned to their original values:



**Step Five:** Return to the **Microsoft Azure AD portal** and look at your restored users profile. For **Bruce Lee’s Profile**, you can see his **Department** and **Job title** have returned to their original values.



1. On Demand and Backup and Recovery will recreate the user group, but in this initial release, defining permissions must occur outside of On Demand. [↑](#footnote-ref-1)
2. When recovering a user that has not been deleted from the Office 365 recycle bin, be sure to select **Recover user from recycle bin**. This option ensures that permissions are properly re-instated. [↑](#footnote-ref-2)
3. See footnote 1 above. [↑](#footnote-ref-3)
4. Make sure you select “If a user is not found in the recycle bin, create a new one.” [↑](#footnote-ref-4)