Background and Description

Toolkit is designed to allow designated users access to various aspects of Blue AD and Exchange Online, including group and shared mailbox management.

Access and Authentication

Toolkit is available on https://toolkit.blue.cam.ac.uk and is AzureAD authenticated. This means that, if enabled for your account, you might be prompted with MFA when you access it.

There are two ways for end users to authorize access to Toolkit:

1) Each institution has a self-managed Lookup group called “Toolkit Management Group”. Members of this group will gain full access to Toolkit for that institution. This includes being able to see an “Administration” tab to allow more selective access for others.
2) Being added via the above referenced “Administration” tab which will allow selective access to parts of Toolkit.

Selecting which institution to manage

If the user is associated with multiple institutions, then at the top section of the page there is a grey bar with an “Institution” dropdown list, containing the names of all institutions in Blue that that user is authorized to manage.

A user can choose any of the entries in the list, then click “Change” to switch to that site and display groups associated to that institution. This choice is saved in a browser cookie and will be automatically selected whenever a user returns to this page.

If a user only has access to a single institution, that institution will be automatically selected and the user will not see the grey bar.

Groups

The initial view shows a list of groups/distribution lists at the selected institution. This list shows:

- The display name
• The membership count
• Whether the distribution list is hidden in the Global Address List
• Whether the group is synchronized with a Lookup group and the last sync status message
• The email address for distribution lists

To the left of the display name is an information icon (ⓘ) which, when clicked, will show a little extra information (such as the underlying Blue AD name of the group).

Clicking on column headings will sort by that column.

The “Lookup synchronization” column will show either:

• Nothing, if the group is not being synchronized with Lookup
• An “upload” arrow to indicate the AD group is being synchronzed to the Lookup group
• A “download” arrow to indicate the AD group is being synchronzed from the Lookup group

Alongside the arrow will be a brief description of the latest sync status.

Above the column headers are a refresh icon to reload the group list, a group type filter dropdown, and two filter textboxes.

The group type filter can be used to only show groups of a certain type, either:

All groups

Security groups – these are the default type of group created by Toolkit

Shared mailbox access groups – these are the groups automatically created when a Shared Mailbox is created by Toolkit

Distribution lists – these are security groups with an added email address

This selection will be honoured even if additional filtering is specified by the following options -

Entering a CRSID into the “Filter groups by member” textbox and clicking ‘Apply filter’ will filter the list of groups to only those that have the specified user as a member. While that filter is applied a new ‘Remove '<user>' from these groups” button will become available. Clicking this button will remove the filtered user from all the visible groups in one go. Alternatively click the ‘Clear filter’ button to revert to showing all groups.

The list can also be filtered on group name – enter part of a group name in the “Filter groups by name” textbox to only show those groups that have names that (partially) match the entered text. Again, click “Clear filter” to remove this filter.

At the bottom of the page are buttons to create, delete and edit groups and, on the right-hand side, a button to export the currently displayed list of groups as a CSV file.
Create new group

This button will open a new window allowing you to create a group or distribution list. The only required field is the “Display name”, which must be unique across Blue AD. The group will be created using a GUID as the underlying AD object name (to ensure uniqueness). If you are creating a ‘normal’ group, this is all that is required and clicking ‘Create group’ will cause the group to be created.

If you wish to synchronize the membership of this group with a Lookup group, you can choose a sync type of “To Lookup” or “From Lookup”, and then pick which Lookup group you wish to sync with. The following conditions need to be satisfied for a Lookup group to appear in the list –

1. The current Toolkit user must be able to manage the Lookup group
2. The “uis-toolkit-group-sync” Lookup group must be granted either “Managed by” permissions on the target Lookup group (for syncing to/from) or “Privileged access by” permissions if only syncing from Lookup.

Once configured, syncing will occur approximately once an hour. Changes to the group membership will be logged in the “Audit” tab.

If you wish to create a distribution list then, in addition to a display name, you will need to assign an email address to the list. The domain for this address must be selected from a dropdown list which will contain only those domains available to the current institution.

The selected domain can be cleared by clicking on the dropdown list then tapping the backspace key.

You can also choose whether the distribution list will be hidden in the Global Address List. By default they will be visible.

If required, you can add a number of ‘Permitted Senders’ to the distribution list. ‘Permitted Senders’ are users or groups that are allowed to send email to the distribution list; adding anything to ‘Permitted Senders’ will stop everything not listed from sending email to the distribution list. Click “Add sender” then enter either the CRSID, display name or email address for the sender. Clicking the information icon next to a permitted sender will show the full ‘distinguished name’ which you can use to check that the correct person has been added.

Selecting one or more permitted senders will allow you to remove them by clicking “Remove sender”.

Once done, click “Create group” to create the distribution list.

Delete selected group

When a group is selected, this button will be available. Pressing the button will open a confirmation dialog, asking if you are sure you want to delete the group. Choosing ‘Yes’ will do so. There is no undo function. Choose ‘No’ to cancel the action.
**Edit selected group**

When a group is selected, this button will be available. Pressing the button will open an edit dialog, similar to the “Create group” dialog. You can then alter any aspect of the group and click “Apply changes” to make the change permanent.

**Viewing group membership**

To view group membership, double-click on the group in the group list. This will open a dialog showing the current list of members, and buttons to “Add new users”, “Remove users” and “Clear group”, with an “Export to CSV” button on the right.

If any users in the list are selected, the “Remove users” button will change to “Remove selected user(s)”. For each user, membership of licensing groups is also shown, indicating whether the user has access to EES-provided services (such as Teams, OneDrive, SharePoint etc), and also whether they are licensed for Exchange Online (and therefore whether they have a mailbox in that system). Because this shows licensing group membership, users may appear to be licensed before the automated processes have actually assigned the relevant licenses – a delay of approximately three hours may be noticed in some cases.

Double-clicking on a user will take you to the “User Information” tab, showing you additional data for that user.

**Add new users**

Clicking this button will open a dialog in which you can choose which users to add to the group. You can do so by:

- Entering CRSID(s) into the “Users” field. You can separate multiple CRSIDs by commas or spaces.
- Entering email addresses into the “Users” field. Blue AD will be searched for an object having this email address, and that object will be added to the group. If none found, then a new “Contact object” will be automatically created.
- Selecting an institutional group – the members of that group will be made members of this group.
- Selecting an institutional group – that group will become a nested member of the current group.
- Selecting a file – this file will be assumed to have one CRSID or email address per line.

Any combination of the above selections can be used. Clicking “Add users” will then attempt to add all chosen users to the selected group. A dialog will open which will show which users have been successfully added and which ones couldn’t be (for example because they are already members).

**Note:** This option will not be available if the group is synced from Lookup
**Remove users**
Clicking this button will open the same dialog that “Add new users” opens, which will allow you to select which users you would like to remove from this group. See “Add new users” for the ways to specify a set of users.

**Note:** This option will not be available if the group is synced from Lookup

**Remove selected user(s)**
Clicking this button will open a message box asking you to confirm the removal from the group of the selected users. If you agree to this confirmation, the selected users will be removed from the group.

**Note:** This option will not be available if the group is synced from Lookup

**Clear group**
Clicking this button will open a message box asking you to confirm that you wish to remove all users from the group. If you agree to this confirmation, all users will be removed from the group.

**Note:** This option will not be available if the group is synced from Lookup

**Export to CSV**
In most places where a list of items is displayed (for example the group list or the membership list) you will find an “Export to CSV” button on the right-hand end of the toolbar. Clicking this will convert the currently visible entries in the list into a CSV file which can be downloaded or opened in a suitable application.

**Shared mailboxes**
The initial view shows a list of shared mailboxes at the selected institution. This list shows:

- The display name
- The primary email address for the mailbox
- Whether the mailbox is hidden in the Global Address List
- A list of additional email addresses for the mailbox

To the left of the display name is an information icon (ⓘ) which, when clicked, will show a little extra information (such as the underlying Blue AD name of the group).

Clicking on column headings will sort by that column.
Above the column headers are a refresh icon (which will reload the mailbox list), and a filter textbox. Entering an email address into this box and clicking ‘Apply filter’ will filter the list of mailboxes to only those with the specified address associated with it. While a filter is applied, click ‘Remove filter’ to revert to showing all mailboxes.

At the bottom of the page are buttons to create, delete and edit mailboxes and, on the right-hand side, a button to export the currently displayed list of mailboxes as a CSV file.

**Create new shared mailbox**

This button will open a new window allowing you to create a shared mailbox. The required fields are the “Display name” and the “Primary email address”, which must both be unique across Blue AD and Exchange Online. The domain for this address must be selected from a dropdown list which will contain only those domains available to the current institution.

The selected domain can be cleared by clicking on the dropdown list then tapping the backspace key.

If required, you can add additional email address to the mailbox. Click “Add address” then enter email address you wish to add. This address must not already exist, and the domain must be associated with the current institution.

Creating a mailbox will automatically create an associated access group named “Access group for <primary email address>”

By default, a mailbox will appear in the Global Address List. If you do not want this to happen, you can tick the box to hide it. Be aware that you will not be able to add the mailbox to Outlook if it is hidden.

Also by default, sent mail from a shared mailbox will be stored in the sending user’s mailbox, not the shared mailbox. You can tick “Retain sent mail in mailbox” to ensure that mail is kept within in the shared mailbox.

Once done, click “Create mailbox” to initiate the creation process. As the creation process involves various interactions with Microsoft’s cloud environment this may take an indeterminate amount of time to complete, so progress can be monitored by refreshing the mailbox list. Mailboxes being provisioned will be shown first in the list. Typically, a mailbox should be created within about 30 minutes after passing through nine processing steps, with steps 2, 5 & 8 taking the longest amount of time to complete.

**Delete selected mailbox**

When a mailbox is selected, this button will be available. Pressing the button will open a confirmation dialog, asking if you are sure you want to delete the mailbox. Choosing ‘Yes’ will do so as well as deleting the associated access group. **There is no undo function**. Choose ‘No’ to cancel the action.

**Edit selected mailbox**

When a mailbox is selected, this button will be available. Pressing the button will open an edit dialog, similar to the “Create new shared mailbox” dialog. You can then alter any aspect of the mailbox and click “Apply changes” to make the change permanent. An extra action available in this dialog is the ability to
choose any of the additional addresses and then “Make primary” to swap it with the currently configured primary address.

If you change the primary email address of the mailbox, the associated access group will be renamed to keep the naming scheme consistent.

## User information

User information allows you to see basic information about a user account. You can determine when the password was last set and why a specified user has been given a particular EES license. Enter a CRSID, and click “Find”. For valid users, you will see the date of last password change, and the sequence of tests/checks that the licensing script has gone through to determine whether the user should have an EES license and, if so, whether it’s the staff or student version.

You can also see a summary of the institutional group memberships for this user. Double-clicking on a group will take you to the group membership dialog in the Groups tab.

## Audit

The Audit tab displays a list of actions performed by users of Toolkit on objects that are associated with the currently selected institution. The most recent actions are listed first. You can search this list if required by applying a filter or “Export as CSV” as necessary. Double-clicking an entry will display additional information (in JSON format) detailing the specific attributes being changed.

## Application Registration

Application (App) Registrations are endpoints in AzureAD which are used to provide cloud-based authentication for applications. This will be of use to individuals who wish to use, say, Open ID Connect when writing software as a means to authenticate users against AzureAD. At present basic functionality is provided and further enhancements are planned for future Toolkit releases.

It is highly advised that you familiarise yourself with app registrations using Microsoft’s developer documentation as this is an advanced subject that requires some in-depth technical knowledge.

The initial view will show all app registrations that are owned by the current Toolkit user. If you have previously requested an app registration directly and cannot see it in this list, please contact the Service Desk so that we can assign it accordingly. Each entry has an “i” icon to the right of the display name which, when clicked, will display the full configuration of the entry, in JSON form. Not all of these parameters are currently editable via Toolkit.

At the bottom of the page are buttons to create, delete and edit registrations.
Create new application

This will open a window where you can specify initial details for a new registration. A display name is required and should be informative but is not visible to others.

A replyURI is required to allow the app registration to redirect the users browser back to your application after authentication. More that one URI is allowed and each one can refer to a web app (WEB) or a single-page application (SPA). Click “Add URI” to allow you to specify the type and value of the new entry. Double-clicking on the type while editing will display a dropdown from where you can choose either the above types.

A client secret is a password that your application uses to ensure that only it can access the app registration. Multiple secrets can be present simultaneously and all are equally valid. Click “Add secret” to enter a display name and a lifetime of the secret (up to a maximum of 24 months). New secrets will be created only when you finish creating the registration.

Finally, a registration can have multiple owners. These are users who can view and edit the registration via Toolkit. By default the current Toolkit user will be assigned as an owner, but additional users can be added. An owner cannot remove themselves.

Once finished, click “Create application registration”. If you have added new secrets, the values of these secrets will now be displayed. Please note that this is the only time these values will be visible so you must make a note of them before closing the window.

Edit selected application

You can alter any of the values entered when creating an app registration by selecting it from the list and clicking “Edit selected application”. From this window you can also find the “Tenant ID” which you may require when configuring your application.

As highlighted above, you will not be able to recover any of the client secret values, although you can delete and add new ones.

Delete selected application

After confirmation this will permanently remove the specified application from Azure.

Institution Configuration

This tab provides access to multiple aspects of an institution within Blue AD.

Service Accounts are user accounts that exist within your institution’s “Accounts” OU. You would generally use a service account if you need BlueAD credentials for institutional servers hosted in Blue.

When you create a service account there are two naming options – a ‘service account’ is named ‘<institution>-<something>’ whereas an ‘admin account’ is named ‘<something>admin’. Other than the naming scheme there are no differences between the two.

Visitor accounts are for special use only. They should not be used in place of a standard CRSID-based account, and will expire after 90 days (this limit cannot be altered). In addition MFA is enabled and no EES licenses will be assigned to these accounts.

In addition, if you have any shared mailboxes that you have requested login access for, then they will also appear in the list so that you can set the password.
Group Policy Objects

This is initial, basic, functionality for creating empty GPOs, after which management would need to be performed via standard Microsoft utilities. Please do not create GPOs without discussing your requirements with UIS first.

**Resources**

The Resources tab allows you to create and edit room, workspace and equipment resources which can be booked through Outlook.

After selecting the tab, a grid of all resources available for your institution is displayed. This list shows:

- The display name of the resource
- Main identifier of the resource, in most cases the same as display name
- The primary email address for the mailbox
- What type of resource the mailbox is setup as
- The number of people that can use the resource (rooms and workspaces only)
- Where the resource is situated

There are three different types of resource mailbox available – room, workspace and equipment. A room is any shared space that you wish to be bookable. A workspace is a shared office space, for instance a cluster of hot-desks or a shared working space. Workspaces can be booked by multiple people at once without conflict, up to the capacity set for the space. Equipment is anything shared in your institution such as laptops and projectors.

To open a resource to view more options, double click on it or selected it and click the ‘Edit selected resource’ button in the bottom left of the screen. To create a new resource, click on the ‘Create new resource’ button in the bottom left of the screen.

**Creating and editing resources**

When creating and editing a resource, the following options are available. Mandatory fields are marked with an asterisk. Note when editing a resource, some mandatory fields may be empty and will have to be filled before saving if the resource was created externally from Toolkit.

Resource type

Select the type of resource required. This field only appears in the ‘Create new resource’ popup.

Resource Name

Choose the display name and email address assigned to the resource mailbox. The display name must be unique across the whole University.

Booking approval settings

In this section you can set the booking permissions for the resource mailbox to control which users can book it. The options available are:

- Auto accepted group – Set this group to allow a set of users to book a resource without approval. When a group is selected, the members of this group receive an auto-acceptance email from the mailbox after sending a booking request. If this group is set for a workspace, the remaining capacity is reduced with each booking until the maximum number of bookings has been reached. If you don’t want to set this group, select the ‘None’ option.
• Booking approvers – Set this group if approval is required to book a resource. If this group is set, an email will be sent to the group members every time the resource is booked to approve the meeting request. Only one person has to approve the request. If you don’t want to set this group, select the ‘None’ option.

• Booking requestors – Set this group to identify users whose resource bookings require approval by the ‘Booking approvers’ group. If you don’t want to set this group, select the ‘None’ option.

Please note only mail-enabled security groups can be used to set the above booking approval options.

Booking options

These are additional features associated with the mailbox. Next to some options there is an information icon which can be clicked on for extra information about the setting.

Resource details

This sets further basic information about the resource. Capacity, location and phone number can be left empty, however a capacity should be set for workspaces. Rooms can be grouped into locations, known as room lists. These are used as filters in Outlook calendar, where a user can use them to find resources associated with their building. Set this if you wish to assign the room to a building. Please contact the Service Desk if you require a new room list to be set up. Equipment cannot be assigned to a room list, and the value for this defaults to “None”.

Click on ‘Apply Changes’/’Create Resource’ to save. Not the saving process may take a while depending on the settings selected. The save is complete once the window has disappeared.

Microsoft advise waiting 24 hours after creating a resource before using it to allow the mailbox to provision.

Administration

The Administration tab is visible to institutional administrators and provides a method of allowing access to Toolkit for other users. The left-hand pane shows a list of users who have been given access, and the right-hand pane shows which permissions those users have been granted.

To grant access to a user, click “Add user” then enter their CRSID. They will appear in the left-hand pane but will initially have no permissions. Choose the items in the right-hand pane that correspond to the set of permission you wish to grant, then “Apply changes” to set those permissions. That user will now be able to access Toolkit.

You can edit permissions by selecting any user in the left-hand pane and adjusting the settings in the right-hand pane (remembering to ‘Apply changes’ once done), or remove access for a user by selecting them in the left-hand pane and clicking ‘Remove user’.

Timeout messages

If your browser has been sitting with Toolkit open for some time then when you attempt to perform an action you may see the following message: “Your session has timed out. Click ‘Refresh’ to renew it.”

Clicking the ‘Refresh’ button will reload the webpage (and optionally request reauthentication via ADFS if necessary).
When using Toolkit, you may see one or more of the following error messages:

Message: **This email address is not valid for your institution.**

Reason: Email addresses can only be applied if Toolkit believes they are associated with that institution. If you find you are unable to set an email address, please contact the Service Desk.

Message: **This email address is not in a valid format. / The primary email address is not in a valid format.**

Reason: The email address you entered is not in the form <localpart>@<domain>.

Message: **This email address has recently been used. Please try again in 30 minutes.**

Reason: When an email address is removed or altered, the old value cannot be reused within 30 minutes due to synchronization delays between BlueAD and Azure.

Message: **This email address is already in use elsewhere. / The primary email address is already in use elsewhere. / An additional email address is already in use elsewhere.**

Reason: A different object in BlueAD already has this email address associated with it.

Message: **This display name is already in use elsewhere.**

Reason: Display names are visible in the Global Address List and therefore must be unique across all institutions.