

Fastpath Lifecycle Users Guide

Fastpath Solutions, LLC

October 25, 2023 — v2023.10.0.release



FASTPATH

Contents

1	Introducing Fastpath Lifecycle	5
1.1	Features	6
1.2	Fastpath Lifecycle User's Guide	6
1.3	Finding Information about Fastpath Lifecycle	7
2	Understanding Fastpath Lifecycle	8
2.1	Terminology Overview	8
2.2	Interface	9
2.2.1	Menu	9
2.2.2	Alerts	9
2.2.3	Your user profile	10
2.2.4	Your User Filters	10
2.2.5	Notifications	10
2.2.6	Access Keys	11
2.2.7	Quick Filter links	11
2.2.8	Search Filter	11
2.2.9	Page navigation	12
2.2.10	Quick Tips	12
2.2.11	Jump to top	12
2.2.12	Forms	12
2.2.13	Mobile Phones & Tablets	12
2.3	Application Access	15
3	Getting Started	16
3.1	Logging into Fastpath Lifecycle for the first time	16
3.2	First Steps	16
3.2.1	Credential Policy	16
3.2.2	Resources & Roles	17
3.2.3	Categories	17
3.2.4	Organisational Units	17
3.3	Next Steps	17
4	Administering Fastpath Lifecycle in your Organisation	18
4.1	Setting up Organisational Units	18
4.2	Setting up Fields	19
4.2.1	Ordering Fields	21
4.2.2	Field Label translations	21
4.2.3	Field Data Types	21
4.2.4	Per-category Form Field settings	23
4.2.5	Form Field Transformations	23
4.3	Setting up Credential Policies	24
4.3.1	Password Protection	26
4.3.2	Username Formats	26
4.3.3	Password Complexity	28
4.4	Setting up Acceptable Usage Policy (i.e., AUP)	28
4.5	Workflow Configuration	29
4.5.1	Assure SOD Risk Assessment	30
4.5.2	Workflow step conditions	31

4.6	Administer Pending Workflow Events	32
4.7	Setting up Self Service Forms	32
4.8	Pending Invitations View	34
4.9	Email Templates	34
4.9.1	Setting up Email Templates	34
4.9.2	Embedding photos	35
4.9.3	Available Templates	35
4.10	Compliance Policies	37
4.11	Setting up Roles	37
4.11.1	Role Policies	38
4.11.2	Default Roles	39
4.12	Setting up Resources	39
4.13	Setting up Entitlements	41
4.14	Setting up Labels	41
4.15	Setting up Catalogues	41
4.16	Setting up Categories	42
4.17	Administrative Users, Roles & Privileges	44
4.17.1	Administrative Users	44
4.17.2	Administrative Roles	44
4.17.3	Administrative Privileges	45
4.18	Lua Scripts	45
4.18.1	Setting up Lua Scripts	45
4.18.2	Getting started with Lua programming	46
	Native Lua Functions and Variables	50
	Fastpath Lifecycle Lua Library	52
4.18.3	Differences from standard Lua	58
4.19	Mapping Tables	58
4.19.1	Setting up Mapping Tables	58
4.20	Bulk Import	58
4.21	Tasks	58
4.22	Email Configuration	58
4.23	Auditing Fastpath Lifecycle Usage	59
4.23.1	Exporting the Audit Log	59
4.23.2	Limiting the size of the of Audit Log	59
4.24	Fastpath Lifecycle Reporting	59
5	Integration	60
5.1	Connecting Fastpath Lifecycle to your Identity Management System	60
5.2	Provisioning	60
5.2.1	Setting up Provisioning Endpoint Connections	60
5.3	Fastpath Connect status	63
5.4	Staging	63
5.4.1	Fastpath Staging Schema	64
5.4.2	Database Table: staging	64
5.4.3	Database Table: resources	66
5.4.4	Database Table: affiliateresources	66
5.4.5	Database Table: event	66
5.4.6	MySQL Data Types Explained	67
5.5	Fastpath Lifecycle API	68
5.5.1	Field/Schema attribute mappings	68
5.5.2	API Configuration.	70
5.6	OAuth Clients	70
5.7	Fastpath Self Service Configuration	71
5.7.1	Applications and Roles in Fastpath Self Service	71
6	Managing Identities	73
6.1	Adding / Requesting an Identity	73
6.2	Invite external people	74
6.3	Importing Identities	75
6.4	Finding Identities	76

6.4.1	Identity actions	76
6.4.2	Quick filters	76
6.4.3	Export to CSV	77
6.5	Requests	77
6.5.1	Listing	77
6.5.2	Edit	77
6.5.3	Reassign	77
6.5.4	Approve	77
6.5.5	Decline	77
6.5.6	Self Service Requests	77
6.5.7	Identity Statuses	78
6.6	Active Identities	78
6.6.1	Listing	78
6.6.2	Additional access	80
6.6.3	Renewing	80
6.6.4	Extend	80
6.6.5	Terminating	80
6.7	Inactive Identities	80
6.7.1	Listing	80
6.7.2	Re-enabling	80
6.8	Editing Identities	80
6.8.1	Identity Bulk Edit	81
6.9	Effective Resources	81

Important Notice

COPYRIGHT © 2023 Fastpath Solutions, LLC. All Rights Reserved.

The Fastpath logo is a trademark of Fastpath Solutions, LLC. Other brand and product names are service marks, trade names, trademarks or registered trademarks of their respective owners.

Chapter 1

Introducing Fastpath Lifecycle

Fastpath Lifecycle is a web based application providing Identity life-cycle management and governance capabilities for users which need to interact with the enterprise. Examples of such users include staff, students, contractors, partners, suppliers or customers, who need to have access to online services or applications, according to their role within or relationship to the organisation.

Fastpath Lifecycle provides Workflow driven automation to ensure that not only can the enterprise quickly provision access to users with minimal overhead on central IT services, but crucially that the life-cycle of these accounts can be properly managed, ensuring that access is cleanly removed when it is no longer required.

Designed to be quick-to-value, Fastpath Lifecycle can rapidly deliver the following benefits:

Productivity Quickly enrol users and provide access to the applications they need, via delegated administration or Self Service.

Security Ensure that access is removed when it is no longer required, so there is no risk of users accessing sensitive applications after their association with the enterprise is over.

Compliance Role based approach ensures that users only have access to services they need and built-in Workflows make sure that access is reviewed and approved on a regular basis according to policy.

Built to support open standards such as OAuth and SCIM, Fastpath Lifecycle can be deployed either as a standalone application, or alongside existing IAM platforms in an orchestration role.

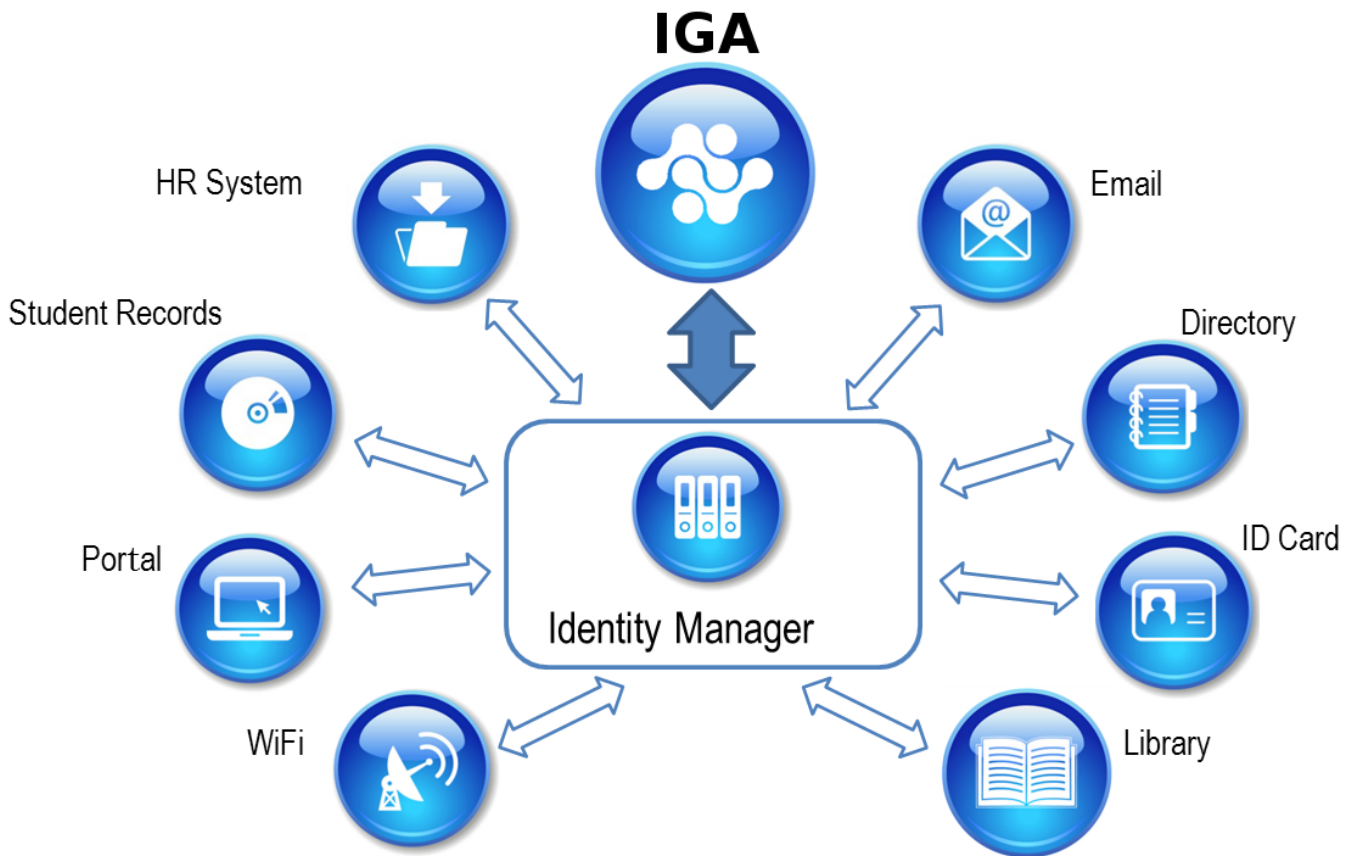


Figure 1.1: Fastpath Lifecycle and IDM

1.1 Features

- End-to-end life-cycle management of identities
- Manage workforce, B2B, B2C and contractor scenarios
- Authoritative source or directory modes
- Devolved administration of Identities
- Out-of-the-box delegated approval and certification Workflows
- Configurable Workflow engine for custom scenarios
- Local, SAML 2.0, and LDAP Authentication
- Self Service registration, attribute management, and access requests
- Self Service password and username recovery
- Role-based architecture
- SCIM Provisioning
- SCIM compliant RESTful API
- OAuth 2.0 authorisation flows
- Audit trail
- Integration with commercial Identity and Access Management products including Ping Identity, Microsoft and NetIQ

1.2 Fastpath Lifecycle User's Guide

This guide introduces the main topics of interest related to Fastpath Lifecycle for Users. The following chapters provide usage information and general instructions.

1.3 Finding Information about Fastpath Lifecycle

This User's Guide provides information about all aspects of Fastpath Lifecycle and has guidance that will be useful to Fastpath Lifecycle Users. This user's guide is available within the Fastpath Lifecycle interface from the **System » Help** menu option and as a PDF included with the software distribution package.

In addition, most pages within the Fastpath Lifecycle interface show a 'Quick Tips' link that hovers at the bottom right side of each page. Clicking this will show some contextual help for the current page as well as provide a direct link to the corresponding section in the User's Guide. There are many form fields throughout Fastpath Lifecycle that also have context-sensitive help and/or tips for filling in values. Simply hover over the help icon attached to each field (the blue question mark) and a tooltip will pop up.

For assistance with the installation and operation of the system, refer to the separate Administrator's Guide included with the installation package and installed to `/usr/share/doc/iga`.

Find more about Fastpath and information about getting Technical Support from the [Fastpath website](#)

Chapter 2

Understanding Fastpath Lifecycle

Fastpath Lifecycle provides a store of Identities and related information with the ability to manage the full life-cycle of those Identities, including approving and controlling access. Fastpath Lifecycle can be connected to other systems including other Identity Management systems both as source and a destination.

2.1 Terminology Overview

The following definitions explain a few of the main terms that relate to Fastpath Lifecycle.

Identity An Identity stored in Fastpath Lifecycle. A person who is associated with your organisation (typically temporarily) and who does not currently have an account in another authoritative source.

Identity Role An Identity Role is a set of Resources/Applications (and optionally Entitlements too) which control access. An Identity Role describes the level of access that Identities have for their account. Privileges can also be assigned to Roles to provide administrative access to the Fastpath Lifecycle Application itself.

Resource A service or Resource that can be made available to an Identity. Examples include email, files store access, car parking passes, id cards and Wi-Fi. Resources can be further expanded as Applications.

Category A collection of Identities with common Resource availability defaults, notification and renewal period settings. Categories can be assigned to Category Approvers who have the responsibility of managing Identities within their Category.

Organisational Unit An Organisational Unit will usually represent a division, department, branch, partners, sections, etc. These can be hierarchical and used to reassign Identities' management responsibilities.

Identity Management System An information system that is used for cross-network Identity management. Fastpath Lifecycle stages details of a person for an Identity Management System (often referred to as IDM) to synchronise and use in order to grant the Identity access to Resources.

Identity Vault A central directory or database which contains information about Identities for the Identity Management System. Where this is a directory accessible via LDAP, Fastpath Lifecycle can use it for authentication.

Group An existing group of Users within the Identity Vault. Permissions in Fastpath Lifecycle at the global, Category, or Organisational Unit level are granted to groups of Users.

Request A request, by an Identity or a Sponsor, for access.

Invite An invitation sent to an external person, by a Fastpath Lifecycle Administrator or a Sponsor, to become an Identity or Administrator.

Sponsor A Sponsor is a user in the Identity Vault who has added a request for access on behalf of an Identity or has been set as the Sponsor by an Approver adding an Identity themselves. This User receives email notifications when an Identity request that they are sponsoring, is approved or declined.

Credential Policy Username and Password generation rules.

Administrative User A person (an Identity) who authenticates to use the Fastpath Lifecycle application to manage Identities or to configure Fastpath Lifecycle settings.

2.2 Interface

The Fastpath Lifecycle application can be accessed with any modern Web Browser, for example Microsoft Edge, Mozilla Firefox, or Google Chrome.

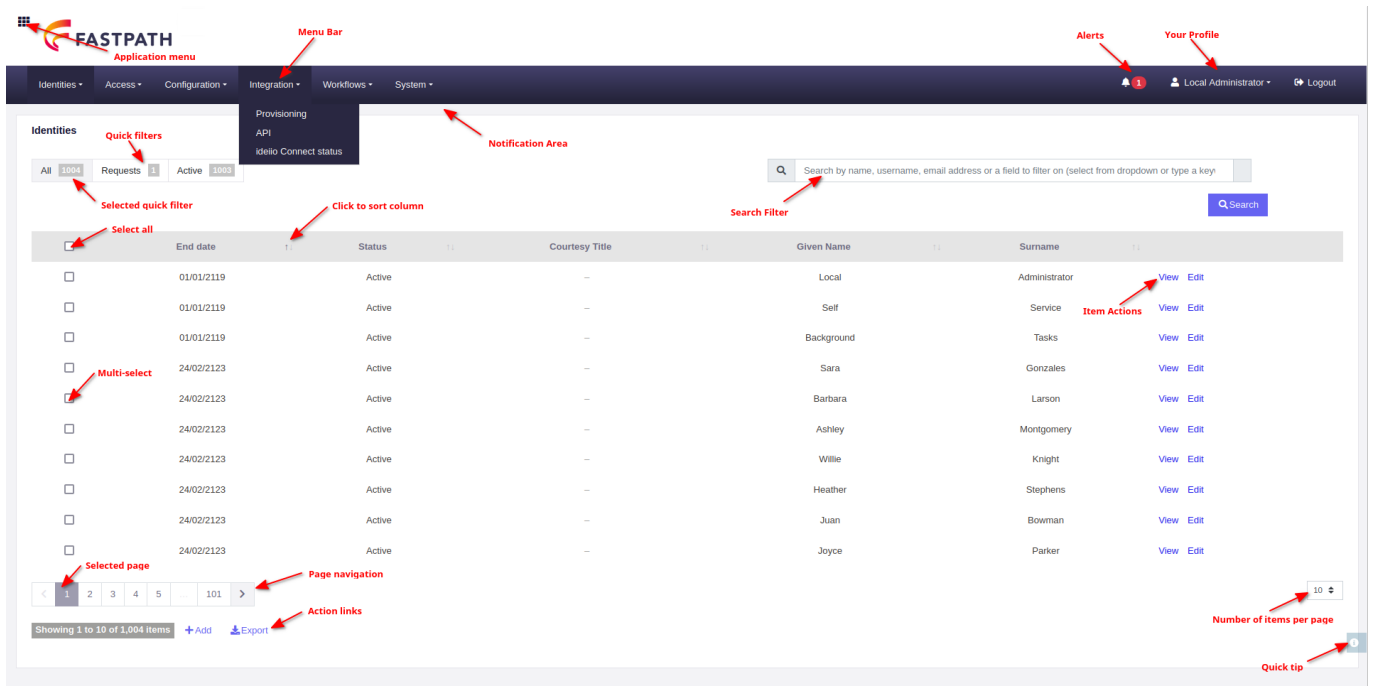


Figure 2.1: Fastpath Lifecycle Interface, Identity summary view

The web based administration interface can be used to configure Resources and Fields for Identities, delegate management to other Users and also for adding and managing Identities.

2.2.1 Menu

The Fastpath Lifecycle interface presents a two level menu as a horizontal bar across the top of each Fastpath Lifecycle page allowing navigation between pages. The menu options presented will vary according to the Role and Privileges of the User that is logged in.

On the right side of the menu bar, Alerts may show as a bell icon along with a number indicating the total number of actions requiring attention (see below).

The sub-menus open when clicking a top-level menu option and close when clicking a blank part of the page.

2.2.2 Alerts

Workflow actions requiring your immediate attention may appear as Alerts. A bell icon and a number shown in red will appear on the right of the menu bar.

Clicking the bell icon will show the list of items requiring your attention (e.g., expiring Identities, new Requests, etc).

2.2.3 Your user profile

Click on your name on the right-hand side of the menu bar and choose “Profile” to see your Administrative User Profile. This has details of your Fastpath Lifecycle User account including your Groups, Roles and Privileges.

From your user profile page you can also change your password (if enabled) or temporarily assign your permissions to another User (if configured).

2.2.3.1 Change password

If the feature is enabled, you can change your password from your user profile page by first filling in your existing password and then entering a new password twice. Your password must be at least 12 characters long and contain at least one upper case letter, one lower case letter, and a number.

2.2.3.2 Forgotten password

If you have forgotten your Administrative User password you will have to ask another Administrator to reset it for you. Or you can use Fastpath SFPR, which is a separate component of Fastpath Lifecycle that can allow Administrative Users and Identities to reset their own passwords.

2.2.3.3 Temporarily Assign Permissions

If you are going away on holiday or are otherwise unavailable for a period and would like a deputy to take over your usage of Fastpath Lifecycle during that time, you can tick the checkbox on your user profile page to **Temporarily Assign Permissions** and choose a User and period of assignment. Please note that this feature can be disabled by configuration. Please go to **System » Settings » Application** and toggle ‘Enable temporary User permissions’ to manage this option.

The user will be assigned the same access level as you have, thus, all your Privileges will be temporarily shared with the other User during the selected period of time.

Note: Only effective Privileges can be assigned, i.e., inherited permissions can not be further assigned to another User. Therefore, if a different Administrator has assigned their Privileges to you, those Privileges will not be further assigned to the User you are currently assigning your Privileges to.

2.2.4 Your User Filters

Click on your name on the right-hand side of the menu bar and choose “Filters” to manage your User Filters. Filters can be added from any page (e.g., Identities, Roles) by building a search form and then choosing the “Save filter” option. To find out more about building filters, please visit the [Search Filter](#) section. After building a filter, add a name for it and select whether it is private or not (i.e., visible to you or to all Administrative Users). Please note that after adding the filter, it will only be selectable on the page it was built on, from the top left-hand side, above the table of data. Clicking the Filter’s name will apply it. Filters from other Administrators, which were not made private, may also be available.

2.2.5 Notifications

From time to time, while using Fastpath Lifecycle, notification messages will appear in the Notification Area at the top of the page, just below the menu bar.

The colour of the notification indicates:

Colour	Meaning
Green	Success
Blue	Information
Yellow	Warning
Red	Error

These notifications provide confirmations of actions that Fastpath Lifecycle has performed (e.g.,

delete or edit) or will perform (e.g., tasks) as well as important notices and warnings. You can dismiss (remove) them by clicking the small cross icon on the top right-hand side of each notification.

2.2.6 Access Keys

For accessibility Fastpath Lifecycle supports the following Access Keys, providing quick keyboard access to important features:

Access keys can be invoked in your web browser by pressing a key (Usually **Alt** or **Alt+Shift** on PC or **Ctrl+Opt** on Mac) simultaneously with the appropriate character on the keyboard.

Access Key	Action
1	Manage Identities
2	Add An Identity
3	Add a Request
4	Add an Invitation
5	Import Identities
a	Add
v	View
e	Edit
d	Delete

Hover over a menu entry to see a tooltip if an access key is defined.

2.2.7 Quick Filter links

You can easily filter the list of items on the Manage Identities page by clicking one of the Quick Filter links. These will show only the items that match the filter. For example, to show only Requests, click the Quick Filter link labelled Requests.

Each Quick Filter link also shows the number of matching items for each.

Note: Only the quick filters that are useful will be shown. So if there are no requests, the quick filter that shows only requests will be not be shown.

When you click on a Quick Filter link, the filter is shown in the Search Filter form on the right, from here you can further refine the filter if you wish.

Clicking on the 'All' quick filter link will remove any filter and display all items.

Furthermore, custom filters can be created by applying filters via the filter form and then clicking the Save filter button below the form. Please read below for more details.

2.2.8 Search Filter

The Search Filter form provides a powerful way to query your data in order to quickly retrieve the exact information you need.

The search filter field is a combination of autocomplete fields that allows you to choose a filter to add to your filter query, you can click and select from the list. Or you can type into it and see filters that match as you type.

To perform a simple keyword search type the word or words that you want to search for and select 'Filter by keyword' from the dropdown list.

You can also filter the items shown by selecting "Filter by Field-name" where Field-name is one of the form fields. The field will be added to your filter query, and you can fill in a value to match.

You can keep on adding multiple filter to further refine your results.

For example, to find all the Requests for a particular Organisational Unit:

1. Select 'Filter by Status' from the search filter field. You can do this by choosing from the list, or by typing a few letters from the word 'status' and choosing it from the shortened list.
2. Choose 'Request' from the Status field.
3. Select 'Filter by Organisational Unit' from the search filter field. You can do this by choosing from the list, or by typing a few letters and choosing it from the shortened list.
4. Make a selection from the Organisational Unit field.
5. Click the 'Search' button.

These filters, once constructed, can be saved for future use by clicking the Save filter button located below the filter form. After a filter is saved, it will become available as a Quick Filter link, on the page it has been applied (e.g., Identities, Categories, etc). If more filters are created, these will be truncated under a drop down menu located at the end of the Quick Filter links. To increase the number of Quick filters visible by default go to **System » Settings » Application** and update the "Number of visible filters" field which is set to show 4 items by default.

2.2.9 Page navigation

When there are more items than will fit on a page, a bar will appear at the bottom of the list for navigating through the pages of items. Click the arrows to navigate forward and back, one page at a time, or click a number to jump straight to a particular page. You can also use the drop-down on the right to adjust the number of items shown for each page.

2.2.10 Quick Tips

A 'Quick Tips' link that hovers at the bottom right side is available on each page. Clicking this will show contextual help for the current page as well as provide a direct link to the corresponding section in the User's Guide.

2.2.11 Jump to top

On long pages, when you scroll a distance down the page, a "Scroll to top" link will appear and hover at the bottom left of the page. Clicking this will navigate the browser to the top of the page to save you from having to manually scroll.

2.2.12 Forms

Form fields that are mandatory (i.e., fields that must not be left blank) are marked with a red asterisk.

Many form fields are accompanied by context-sensitive help which is available by hovering the mouse over the blue question mark symbol.

At the bottom of each form, the Save or Cancel options are available to persist the form data or cancel the changes respectively. If the Cancel option is chosen, all the form data will be discarded.

By selecting the View button from a list of items (e.g., Organisational Units, Identity Roles, etc), a preview of the data will be shown without the ability to make changes. In order to make changes, please navigate to the Edit panel by selecting Edit from the list view or from the left-hand side panel, when viewing an item. The edit page will provide more available options alongside the ability to change data. Please note that both the Edit and View options are available depending on the logged in Administrative User's permissions.

2.2.13 Mobile Phones & Tablets

The GUI will scale to be usable on smaller screens (e.g., mobile phones or tablets), however, the nature of the data shown within the application (tabular data in particular) makes a large screen preferable (e.g., laptop or desktop).

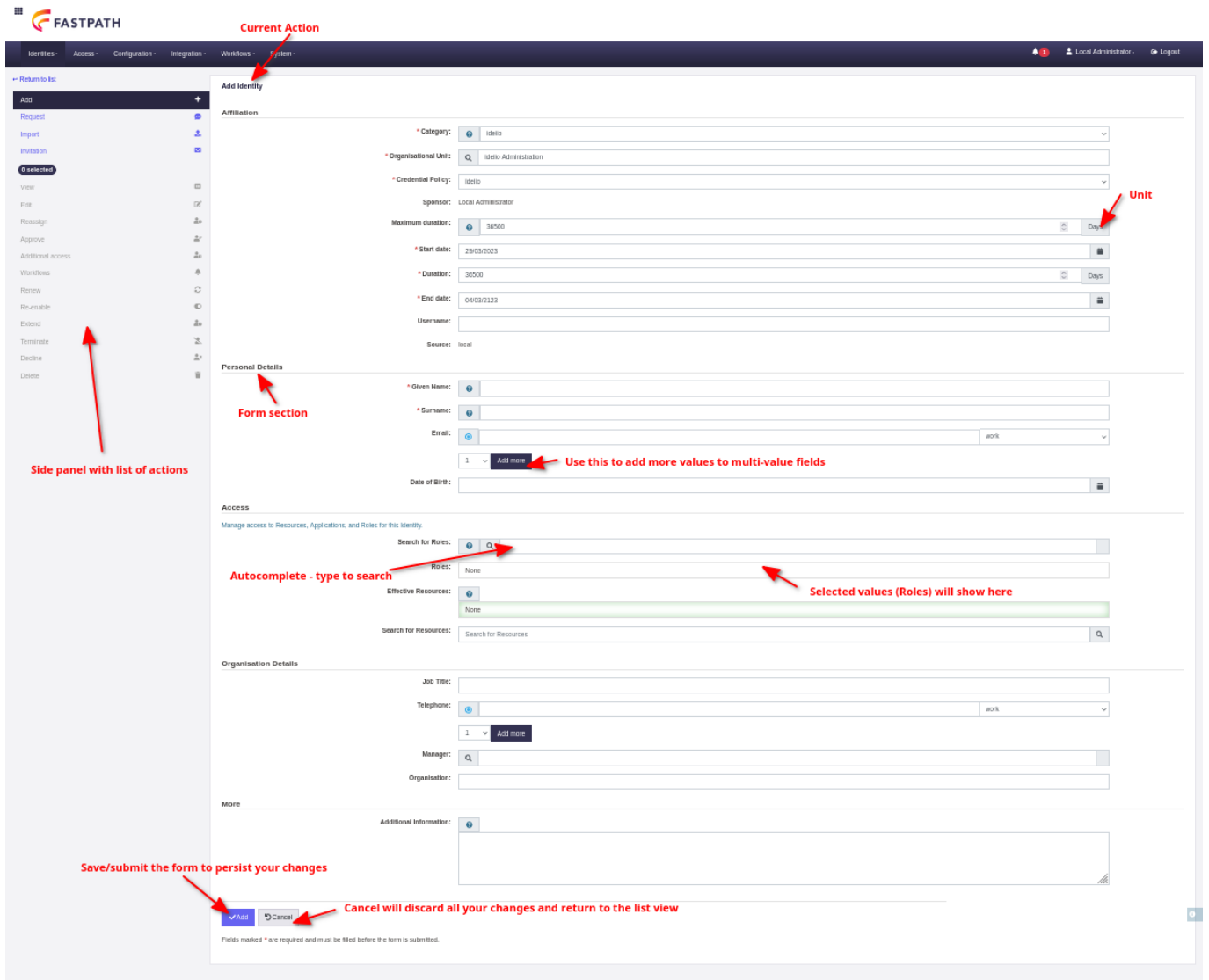


Figure 2.2: Fastpath Lifecycle Form elements

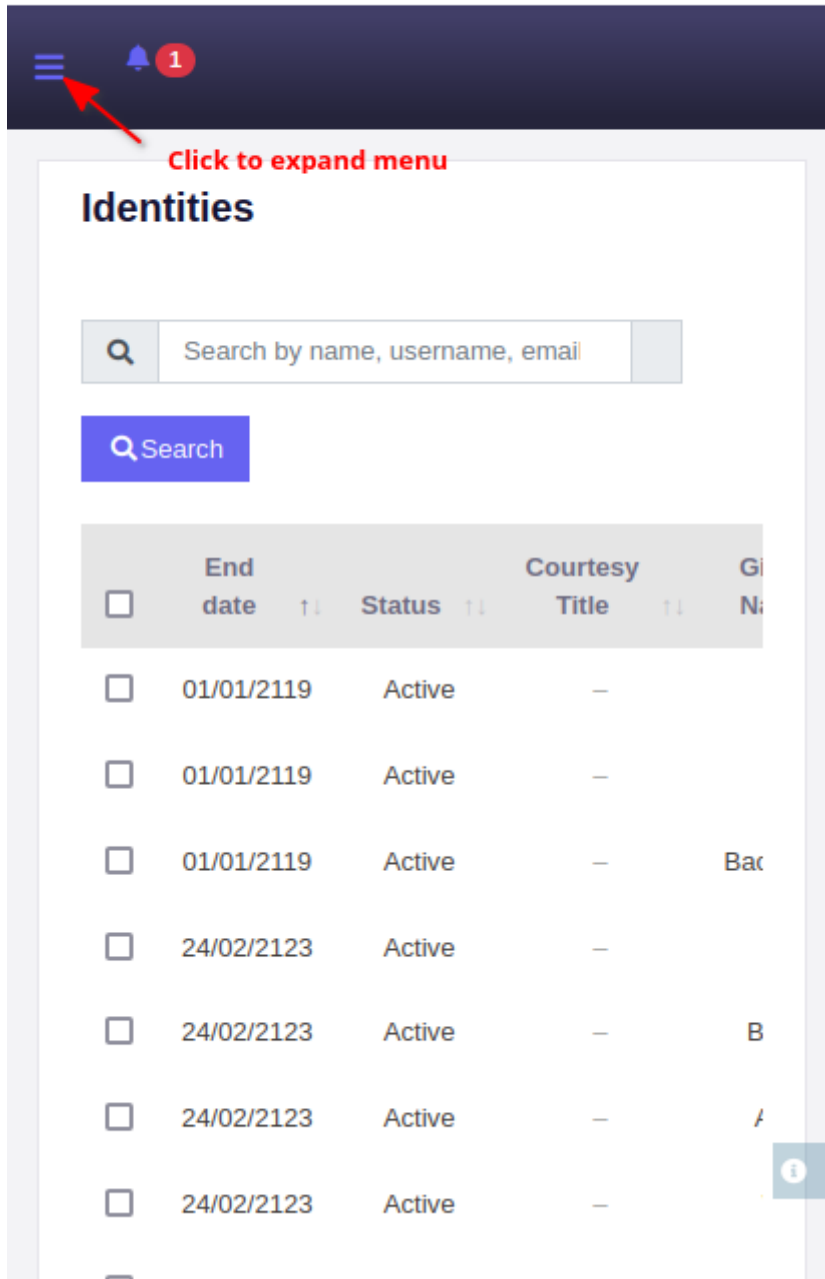


Figure 2.3: Fastpath Lifecycle Mobile Interface, Identity summary view

2.3 Application Access

Administrative Users (Identities with appropriate privileges) can login to Fastpath Lifecycle using Local, LDAP, or SAML2.0 authentication (or even a combination of the above).

Fastpath Lifecycle provides granular access restrictions to administrative features within the product to allow for very flexible control over who has access to each feature.

Access control for Administrative Users is accomplished via membership of one or more Roles. There are over a hundred Privileges that can be individually assigned to Roles and even more Privileges can be created to grant custom restricted access linked to either a Category, a Role, or an Organisational Unit.

Fastpath Lifecycle comes with a default set of system Roles & Privileges which provide enough to get started with Fastpath Lifecycle, but you can create more Roles, and Privileges to extend what is possible and grant very specific Privileges to your Users.

For more information about these features see the [Administrative Users, Roles & Privileges](#) section.

Chapter 3

Getting Started

Tip: See the separate Administrator's guide for assistance installing and configuring Fastpath Lifecycle.

3.1 Logging into Fastpath Lifecycle for the first time

Access the Fastpath Lifecycle URL in your web browser and login with Administrative User credentials. If you chose to authenticate using LDAP during installation this will be a User who is a member of the Fastpath Administrators LDAP Group specified in `idv_admin_group` in your `settings.ini` file. Otherwise, this will usually be 'fastpathadmin'.

Example Fastpath Lifecycle URL: `https://my-server.example.com/ideiio/`

Note: You will be automatically logged out after a period of inactivity however, to protect the information stored in Fastpath Lifecycle, you should manually log out via the link on the menu bar whenever you have finished working with Fastpath Lifecycle.

Note: If you have forgotten your Administrative User password or for some other reason cannot gain access, use another account to login if you have one. Or, see the Troubleshooting section of the Administrator's guide to check LDAP connectivity and/or recover your account.

Note: Fastpath Lifecycle will lockout a device to prevent login in after a certain number of failed attempts with a given period. If you forget your credentials and are affected by this you can:

- Wait for the lockout duration and then try again.
- Reset your password, e.g., using SFPR.
- Ask an administrator who does have access to reset your password for you.
- Login using another device.

3.2 First Steps

Before you can begin managing Identities with Fastpath Lifecycle you will want to configure it to closely match the individual requirements of your organisation. Fastpath Lifecycle does come with defaults for a lot of scenarios, but some information is needed from you too.

3.2.1 Credential Policy

One Credential Policy called 'Default' is provided, but this is not configured to generate usernames and passwords by default. You'll usually want to create and configure your own policy or policies. See [Setting up Credential Policies](#).

3.2.2 Resources & Roles

Create Resources and Roles, link the Resources with Roles in order to configure granular permissions that can be applied to your Identities. See [Setting up Roles](#) and [Setting up Resources](#).

3.2.3 Categories

Fastpath Lifecycle requires at least one Category to be created in order to provide Resource, Role, and life cycle defaults for new Identities. See [Setting up Categories](#).

3.2.4 Organisational Units

Fastpath Lifecycle requires at least one Organisational Unit to be created, every Identity will be associated with an Organisational Unit. See [Setting up Organisational Units](#).

3.3 Next Steps

Now that you have a basic configuration in place, you are ready to further tailor Fastpath Lifecycle to your particular organisational requirements and begin managing Identities.

- Read the section [Administering Fastpath Lifecycle in your Organisation](#) for information about tailoring your Fastpath Lifecycle configuration.
- Read the section [Integration](#) for connections to other software and services.
- Read the section [Administrative Users, Roles & Privileges](#) to provide and control access to Fastpath Lifecycle features for your colleagues.
- Finally, read the section [Managing Identities](#) which has information about the many ways that Fastpath Lifecycle can work with Identities and manage access to Resources.

Chapter 4

Administering Fastpath Lifecycle in your Organisation

Fastpath Lifecycle offers a rich set of configuration settings that allow you to customise it in order to meet all of your Organisation's needs.

4.1 Setting up Organisational Units

Organisational Units in Fastpath Lifecycle provide a hierarchical way of classifying Identities and a way to model your Organisation's structure.

Typically, an Organisational Unit would represent a Division, Department, or Branch, but really it can represent anything to suit your particular needs, for example Partner organisation, Subsidiary, Section.

To configure these, please select **Configuration » Organisational Units** from the menu.

Setting	Possible Values	Purpose
Name	Free text	The name of the Organisational Unit.
Parent Organisational Unit	None / Existing Organisational Unit	To set this Organisational Unit as a child of the parent Organisational Unit chosen here.
Reference	Free text	To set a reference for the Organisational Unit.
Internal Only	On / Off	When checked, the Organisational Unit will not be visible to the Self Service portal.
Delegate OU Administration	On / Off	This option can only be used once and when enabled, it will create a default set of permissions to delegate the current Organisational Unit using a Role, and basic Privileges such as editing an Identity only for this OU, etc.
Delegated Category Template	Existing Category	Select a Category to be used as a template in order to create a newly delegated Category which, along with its Roles, Resources, and Catalogue, will be related with this Organisational Unit. Only available when delegating.
Users	Existing Administrative Users	Add Administrative Users to the corresponding delegated group that will be created for this delegated Organisational Unit.

Setting	Possible Values	Purpose
Delegated Administrative Users list Users	-	Will show a list of selected Users when delegating.
Invite Admin	On / Off	Only available when delegating the OU, and it allows inviting new Administrative Users to Fastpath Lifecycle. An email will be sent to the provided addresses and the new Users will be granted access to the current OU only.
Email	Email address or CSV file containing email addresses	Provide one or more email addresses that will be sent an invitation to gain access to this delegated OU.

You can use the Reference field to include a reference or ID number that you use in other systems and this value will be passed to IDM via the staging table as `orgunit.ref`.

Organisational Units can be nested and there's no restriction on the number of nested levels, but the length of the full name may get unwieldy with deep nesting and Administrative User Privileges will only be checked up to 10 levels deep.

Organisational Units can be created or edited with a delegated Role, Group, and associated Privileges as well as optionally invite an Administrator for that particular Organisation Unit.

4.2 Setting up Fields

Fastpath Lifecycle has a set of built-in Fields that are available for use on an Identity. Some are configured to be used by default and others are available to be enabled if necessary. In addition, Fastpath Lifecycle allows defining Custom Fields that can have any name and type. Fields can also be shown/hidden on the Identity form or made required/optional, depending on an Identity's Category. Furthermore, Fields can be made available only when the Identity has access to a particular Resource by changing the "Use with" field to "Resources" and then attaching the field on a given [Resource](#).

To configure Fields, please select the **Configuration » Fields** menu option.

The following field settings are available.

Setting	Possible Values	Purpose
Field	Field Name	Used by Fastpath Lifecycle and IDM to identify the field, avoid symbols and spaces. ¹
Use with	Select option	Selecting "Identities" will make this Field available for use on the Identity form. Selecting "Resources" will make it available as a Resource Custom field.
Label Data type	Free Text Data Type	The label displayed next to the Field. To set the type of data to be stored by the Field, also affects how the Field is displayed and validated in Forms. ² See Field Data Types .
Autocomplete	On / Off	Whether to autocomplete the Field value whilst typing. ³
Hide value	On / Off	Autocomplete fields show a value as well as a data label, check this option to display the data label only.
Default value	Free Text	Pre-filled, default form Field value.

Setting	Possible Values	Purpose
Mapping table	Select option	Selecting an existing mapping table here will cause it to be used to provide available values to a dropdown or autocomplete field. If the field available values setting already has values, these will be migrated to that Mapping Table.
Maximum length	Number	Set the maximum length of input allowed. ⁴
Available values	Pipe delimited values	A list of values for drop-down fields. ⁵
Help Text	Free Text	Displayed as an icon with a tooltip next to the Field (Currently only displayed in Self Service Forms).
Form Section	Select option	Select a section where this Field will be placed, in the Identity form.
Enforce uniqueness	On / Off	Do not allow a field to hold duplicate values by enforcing uniqueness on every update. When enabling this be sure that the field will be populated with a unique value as form field validation will prevent submission otherwise, even when the field is not displayed on the form.
Read-only	On / Off	When checked, the Field value (if there is one) will be displayed, but the Field will not be editable. If no value is provided either as a default, via SCIM, staging synchronisation or a previous edit, the field will not be shown on the form. Useful for having data populated only via other sources besides the identity form.
Show field in lists	On / Off	When checked, the Field is shown as a column on search results etc.
Include field in export	On / Off	When checked, and when supported by the form, the Field can be included in a CSV export.
Exclude field from filter	On / Off	When checked, the Field will not be shown in the filter form. Excluding fields that you don't need to search makes a simpler filter form.
Generate data format	Free text	Automatically generate data for this field if a value is not manually provided. ⁶ More than one format can be provided, separated by a new line, so that when this field is also set to be unique, all formats will be used in case a format generated a duplicate. Data will be generated regardless of whether this field's configuration is read only or not. However, considering that data is generated when the form is submitted, please note that making the field mandatory via "This field is required" means data will have to be manually provided rather than generated.
Re-Generate Data	On / Off	Re-Generate field data when the Identity is edited and one of the fields in the format rules is modified (except system variables). ⁷
Show field in forms	On / Off	When checked, the Field is shown on forms.

Setting	Possible Values	Purpose
Field is required	On / Off	When checked, the Field is marked as mandatory and must be completed before forms can be submitted.
Self service forms	On / Off	Select which Self Service Forms will have this Field available.

4.2.1 Ordering Fields

Furthermore, besides choosing in which form section a field is displayed (see Form Section above), the order of the fields can be changed from the list view by using the arrows available to move fields up or down. When displayed on the identity form, each field will follow their configured order within the section that they are displayed in.

4.2.2 Field Label translations

The 'Help' and 'Label' can contain one or more language keys in the form `{{example.key}}` which will be replaced with a corresponding language string from the current language.

4.2.3 Field Data Types

Each field is associated with a Data Type, this enforces validation rules upon the field, enables auto-detection of field data during Import, and determines how the field will be displayed on the form.

Once a data type has been chosen for a field it should not normally be changed, since differences between data types may lead to unexpected data loss.

Table 4.3: Field Data Types (part 1)

Data Type	Description
address1	Address line 1.
address2	Address line 2.
affiliate	Lookup for an existing Identity. Stores Fastpath Lifecycle ID.
alphanum	Alphanumeric characters only.
iga_id	Fastpath Lifecycle ID of an existing Identity. This is generated when creating the Identity.
checkbox	A checkbox. The value 0 is used to indicate unchecked and 1 to indicate checked.
country	Country.
courtesytitle	Drop-down list of Courtesy Titles (e.g., Mr, Mrs).
date	Date picker.
datetime	Date and time picker.
db	Database lookup field. ⁸
orgunit	Organisational Unit selection.
dn	A lookup field to select a DN from the LDAP authentication directory.
dob	Date picker. Date of Birth.
dropdown	Drop down list. See the section below about Drop-down fields.

¹It is not possible to change the Field name once set.

²Although it is possible to change the data type of existing Field, it is not recommended as it carries the risk of losing data.

³Applies to courtesytitle, Organisational Unit, and dropdown fields only.

⁴Applies to Text data types only.

⁵Applies to Drop-down data types only.

⁶Please see the [username formats](#) section under Credential Policies for available template variables to generate data. It is not possible to generate data for the Unique ID field as the recommended way of achieving that is via [Credential Policies](#).

⁷When a multi-field is regenerated the new data will be added as a new value, it will not replace an existing value.

Data Type	Description
radiobuttons	A group of radio buttons (only one value can be chosen and all values are visible by default). Available values should be separated with a pipe (i.e.,) and each of these will become a radio button (e.g., Red Green Blue).
email	Email Address.
email_RFC822	Email Address in RFC822 format.
firstname	First Name / Given Name.
fullname	Full Name.
sponsor	Sponsor dropdown. Can also include LDAP entries if configured.
language	Language in the format of an ISO 639-1 two letter language code, followed by an underscore and the ISO 3166-1 country code (e.g., en_GB, en_US).
locale	Locale using the same format as the language data type.
timezone	Olson format time zone, e.g., Europe/London.
user	Administrative User.
slug	URL slug consisting of a URL friendly string where spaces are replaced with dashes. Any other character beside alpha-numeric ones will be removed.
gender	Drop down list. Gender is not available for custom fields.
group	A lookup field to select a Group from the LDAP authentication directory.
integer	An integer. Numeric characters only. Empty values will be stored as 0 (zero).

Table 4.4: Field Data Types (part 2)

Data Type	Description
jobtitle	Job Title
memo	Free text, Multi-line
mobiletelephone	Mobile Telephone number
newpassword	New Password
ninumber	National Insurance Number (UK)
office	Office name
organisation	Organisation name
password	Existing Password
photo	Photo field (JPEG Upload)
postcode	Postal code (e.g., Post code, Zip code)
qualifications	Qualifications (e.g., B.Sc.(Eng), MBA, FRS)
region	Region (e.g., County, State)
surname	Surname / Family Name
telephone	Telephone number
text	Free text, single-line
town	Town or City
url	URL (Hyperlink)
vehicleregistration	Vehicle Registration Number

4.2.3.1 Field Available Values (choices)

Some fields present a selection of choices, the keys and values for these choices on most fields can now be configured using Mapping Tables, whilst the previous manually configured available values method will continue to work for existing fields. If a mapping table is chosen while a manual configuration exists, then those keys and values will be migrated to the mapping table.

If your mapping table contains more than a few dozen entries, for performance and usability reasons, it is strongly recommended using an 'autocomplete' field, either a dropdown datatype configured as

⁸See the section on configuring a Lookup database in the Administrator's guide.

autocomplete or using the autocomplete datatype directly.

4.2.3.2 Manually configured available values

Some fields have choices that are defined in the 'Available Values' setting instead of using a mapping table. The Available Values for these are a pipe (|) separated list of values. Values may also have labels, with the label being separated from the value by a hash symbol (#).

Drop-down example (Values only): The user will be presented with a list containing the choices R, O, Y, B, G and P and these are the values that may be stored in the field.

Available Values: R|O|Y|B|G|P

This example uses single letters for the values, but you can use longer values if you like.

Drop-down example (with labels): The user will be presented with the choices Red, Orange, Yellow, Blue, Green and Purple, but the field will store the single letter rather than the full colour name, which is a label only.

Available Values: R#Red|O#Orange|Y#Yellow|B#Blue|G#Green|P#Purple

Setting a default: When setting a default for Drop-down Fields, you must use the value rather than the label.

Making drop-down and drop-down autocomplete Fields optional: If the Available Values is prefixed with a pipe symbol (|), Fastpath Lifecycle will insert an empty option into the list of choices in the drop-down, making it possible for the user to leave the field blank. Of course, the 'Field is required' setting will also need to be unchecked.

e.g. Available Values: |R#Red|O#Orange|Y#Yellow|B#Blue|G#Green|P#Purple

4.2.4 Per-category Form Field settings

To configure Form Field visibility or to set whether a Field is required to be filled for a specific Category, select the Category from the checkbox list under "Category override" on the field's configuration page (**Configuration** » **Fields** menu option).

When a Category is enabled, any Field that is edited will present the following configuration options.

Setting	Possible Values	Purpose
Default value	Text	To provide a default value for this Field when this particular Category is selected.
Show field in forms	On / Off	When checked the field is shown on forms (for the selected Category).
Field is required	On / Off	When checked the field is marked mandatory (for the selected Category) and must be completed before forms can be submitted.

Please note that if the Category override matches the Field settings, these will not be saved, however, a notification will be shown to indicate so.

4.2.5 Form Field Transformations

You can add a Lua Script to a form field in order to perform transformations on the field data, to set this up click the **Transform** option on a form field and either choose an existing Lua script or select "Create a new Lua Script".

The value that your script returns will be set as the form value. From v5.1.0 onwards, you can set values for multifields by returning a Lua table.

To read about Lua scripting please see [Lua Scripts](#) section.

If later you decide you no longer want the transformation to run, clear the Lua Script field under **Transform**.

4.3 Setting up Credential Policies

Credential Policies define the username scheme and initial password generation rules to apply to a new Identity. To add a new Credential Policy or to edit an existing one use the **Configuration » Credential Policies** menu option.

Setting	Possible Values	Purpose
Name	Credential Policy Name	To set the name of a Credential Policy, which is displayed in the interface and also passed to IDM.
Allow password editing	On / Off	When checked the Identity edit form will allow Administrators to update passwords. Identities will always be able to change their own passwords.
Password Protection	Protection Method	Determine how passwords are to be stored. See password protection below.
Reveal Password	On / Off	Allow a reversible password to be revealed with a click on the Identity page. (Caution: this can pose a security risk). Only available for reversible encryption methods.
Password validity	Number of days	The maximum number of days for which a password will be valid. After this time has passed, Identities will not be allowed to log in, and they will be required to update their passwords. The password will not expire when set to zero (i.e., 0).
Minimum password age	Number of days	The minimum age of a password for changes to be allowed. When a minimum is configured here password changes are prevented until the existing password is this old. When left unconfigured (set to 0 days), password changes are unrestricted.
Generate Password	On / Off	Generate a password when the Identity becomes active.
Allow username editing	On / Off	If enabled, the Identity form will allow updating usernames. Please handle this option with care as it may result with duplicate accounts being created in other integrated systems.
Enforce LDAP Uniqueness	On / Off	When checked LDAP will be searched during username generation to make sure that the username is unique in the directory as well as in Fastpath Lifecycle. (Uniqueness within Fastpath Lifecycle is always enforced) - This option is only available if LDAP is configured.
Initial password prompt	On / Off	An email will be sent to prompt the identity to create (choose & set) a password by following a one-time link. (Requires password generation to be enabled and SFPR URL to be configured, see System Settings)

Setting	Possible Values	Purpose
Allow force password reset	On / Off	A button will be shown on the view Identity page to administrative users with appropriate privileges. This will allow the current password to be invalidated, and an email to be sent, prompting the identity to set a new a password by following a one-time link.
Generate Username	On / Off	Generate a username when the Identity becomes active.
Username Format	Username format strings (one per line)	To control how usernames are generated by Fastpath Lifecycle.
Re-Generate Username	On / Off	Re-Generate a username when the Identity is edited and one of the fields in the format rules is modified (except system variables).
Characters to exclude	List of characters	To specify characters that should be excluded from generated usernames.
Convert to ASCII/Latin1	On / Off	When checked the username characters will be transliterated to ASCII/Latin1.
Convert to lower case	On / Off	When checked usernames will be forced lower case.
Password Characters (Set 1)	List of characters	To define the characters that must be used in Fastpath Lifecycle passwords. The more characters used, the better the passwords will be. If there are too few characters to choose; password generation will fallback to a system default list of characters.
Password Characters (Set 2)	"	"
Password Characters (Set 3)	"	"
Password Characters (Set 4)	"	"
Number of Character sets	1, 2, 3 or 4	To select which character sets are to be included in passwords. A minimum of one character per set is to be included.
Minimum Password Length	Any number	To set minimum password length.
Restrict previous password use	On / Off	When enabled, a history of Identity password changes is kept to prevent re-use. ⁹
Number of passwords to remember	Number	This is the number of passwords to store in the history, and these will be used to prevent re-use.
Enable password blacklist	On / Off	Enable password blacklisting, which provides a number of options to prevent passwords from including certain unwanted content. On its own, this setting simply enables the blacklist options, those must be separately configured.
Word blacklist	List of words	A list of words that are not allowed in passwords, one per line. Leave empty to allow any word.

Setting	Possible Values	Purpose
Sequence blacklist	List of sequences	A list of character sequences that are not allowed, one per line. This differs from the words list by the message that is displayed when a blacklisted sequence is used in a password. Leave empty to allow any sequence.
Number of repeated characters	Number	The maximum number of repeated characters that are allowed in a password. Characters must be repeated adjacent to one after another to be rejected.
Prevent obvious values	On / Off	When enabled this will restrict obvious values such as name, username, phone numbers and email addresses from being used in passwords

Note: The Username Format settings are not available when Username Generation is disabled and Password Format settings are not available when Password Generation is disabled. The Enforce LDAP uniqueness option is only available when LDAP is configured, and The Reveal Password setting is only available when reversible encryption is used to protect the password.

4.3.1 Password Protection

Fastpath Lifecycle offers a choice of methods to protect passwords according to your requirements.

Method	Reversible	Notes
Bcrypt	No	Hashing function derived from Blowfish. Fastpath Lifecycle recommended choice.
SHA-512	No	512bit Digest Hashing function (SHA-2) designed by NSA.
SHA-256	No	256bit Digest Hashing function (SHA-2) designed by NSA.
AES	Yes	Advanced Encryption Standard, also known by its original name Rijndael. Intended for scenarios where Fastpath Lifecycle is providing temporary first-use or initial passwords, and is not recommended for other use cases. CAUTION: Passwords are decrypted automatically before provisioning in plaintext.

Note: Since IGA 3.3.0 passwords are staged in their encrypted form unless configured otherwise. See **System » Settings » Staging** for the option to **Decrypt Passwords**.

4.3.2 Username Formats

Use template strings in the format `{{givenname}}`, see the tables below for a full list of available template strings.

In addition, it is possible to restrict the length of the replacement value using the format `{{variable:<length>}}` where is the number of characters you want to use. e.g., `{{surname:5}}` will use five characters from the surname.

When generating data for usernames, please note that spaces are not allowed. However, if using these formats to generate data for a field, spaces can be used. For example, to generate an Identity's

⁹Password hashes are stored securely in the history in a way that they cannot be freely associated to an Identity except during validation and are only used to prevent re-use. The history is secret and cannot be viewed.

full name, the corresponding field can be set to generate data using a format similar to `{{honsuffix}} {{givenname}} {{surname}}`.

These standard template variables are available:

Table 4.8: Username Formats (part 1)

String	Replacement Value
<code>{{iga_id}}</code>	The Fastpath Lifecycle ID for the Identity, RFC 4122 compliant GUID
<code>{{courtesytitle}}</code>	Courtesy Title/Honorific title (e.g., "Mr")
<code>{{givenname}}</code>	Given name / First name
<code>{{middleinitial}}</code>	Middle Initial
<code>{{surname}}</code>	Surname / Family name
<code>{{fullname}}</code>	Full name
<code>{{preferredname}}</code>	Preferred name
<code>{{previousname}}</code>	Previous name
<code>{{honsuffix}}</code>	Honorary suffix
<code>{{dob}}</code>	Date of birth in ISO format (yyyy-mm-dd)
<code>{{qualifications}}</code>	Qualifications
<code>{{phone}}</code>	Telephone number
<code>{{mobile}}</code>	Mobile (cell) telephone number
<code>{{extemail}}</code>	Personal email address
<code>{{email}}</code>	Internal email address
<code>{{organisation}}</code>	Organisation name
<code>{{jobtitle}}</code>	Job title
<code>{{orgunit}}</code>	Organisational unit
<code>{{gender}}</code>	Gender
<code>{{address1}}</code>	Primary address, address line 1
<code>{{address2}}</code>	Primary address, address line 2
<code>{{town}}</code>	Primary address Town / City

Table 4.9: Username Formats (part 2)

String	Replacement Value
<code>{{region}}</code>	Primary address Region / County / State
<code>{{postcode}}</code>	Primary address Postal code / Zip code
<code>{{country}}</code>	Primary address Country
<code>{{password}}</code>	Initial account password
<code>{{credential_policy}}</code>	Fastpath Lifecycle Credential Policy
<code>{{uniqueid}}</code>	Unique ID / Username
<code>{{previousid}}</code>	Previous Unique ID / Username
<code>{{context}}</code>	DN of Identity eDir context
<code>{{status}}</code>	Identity Status Code
<code>{{reqtime}}</code>	The request time in ISO format, yyyy-mm-dd HH:mm:ss
<code>{{asstext}}</code>	Additional Information
<code>{{sponsor}}</code>	DN of Sponsor
<code>{{createdby}}</code>	Created by
<code>{{rejectreason}}</code>	Reject reason

These special system template strings are also available. Unlike the variables above - these will not cause re-generation even if that option is enabled.

String	Replacement Value
<code>{{appshortname}}</code>	The short name of the application
<code>{{yyyy}}</code>	The current year as four digits (e.g., 2012)
<code>{{yy}}</code>	The current year as two digits (e.g., 12)

String	Replacement Value
{{mm}}	The current month as two digits
{{dd}}	The current day as two digits
{{increment}}	An incrementing number - if used must be placed as the last (right-most) string in your username format. The number of digits can be controlled via the length parameter (e.g., {{increment:3}} will count up to a maximum of 999).

More than one format can be configured per Credential Policy when separated by new lines and each format will be tried in turn to try to find a unique username.

e.g.

```
{{appshortname}}.{{increment:2}}
{{appshortname}}.{{surname}}.{{increment:3}}
```

This example will first create usernames in the format 'Fastpath.00' to 'Fastpath.99' and will then begin generating usernames in the format 'Fastpath.higgins.000' after the first format has been exhausted.

To append incrementing numbers without prefixes that go beyond a single digit of 9 you can use multiple rules, with each rule introducing more digits up to the number of digits you'd like to limit to.

e.g.

```
{{givenname}}{{increment:1}}
{{givenname}}{{increment:2}}
{{givenname}}{{increment:3}}
{{givenname}}.{{surname}}
```

4.3.3 Password Complexity

Use the Password Character Set fields to define up to four lists of characters that must be included in generated passwords. For example, Set 1 uppercase letters, Set 2 lowercase letters, Set 3 numbers and Set 4 symbols.

Enter 1, 2, 3 or 4 under **Number of Character sets** to include, 1, 2, 3 or 4 sets. Sets will be included, in ascending order, from Set number 1 through to Set 4 so if you set the number of sets to include to be 3 this will use set 1, 2 and 3. At least one random character from each included set will be used to generate the password, the rest of the characters in the password will be chosen randomly from all the included sets.

Note: If you leave Set 1 blank, Fastpath Lifecycle will use defaults for all password character sets.

4.4 Setting up Acceptable Usage Policy (i.e., AUP)

The Acceptable Usage Policy should contain information about the implications of using the system and possibly data collection policy. If enabled, it will be presented as a checkbox, with a link to be viewed, and will require acceptance when using the Self Service Form or when accepting an Invitation.

To edit the AUP, please select **Configuration » Acceptable Usage Policy** and then select **Edit** from the left-hand side menu.

Setting	Possible Values	Purpose
Title	Free text, maximum 255 characters	To set a title for the AUP. The title will then be used as a page title and heading when the AUP is viewed by potential Identities.

Setting	Possible Values	Purpose
Enabled	Checkbox	If checked, the AUP will be displayed as a required field in the Self Service Form, as well as in the form where Invitations are accepted, and Fastpath Lifecycle Identities will have to abide to it.
Content	Free text editor	Outline the Acceptable Usage Policy using various text editor features such as bold, italic, strike through, indentations, and external links.
Date	Read only date field	Shows the date at which the AUP was last updated.

Once the content has been provided, please use the **Save** button to store the content and make the AUP immediately available, if enabled.

4.5 Workflow Configuration

There are a number of Workflows that can be configured to control when Fastpath Lifecycle should send emails, and where emails should be sent. Workflows can be configured to require manual actions to be performed by Administrators.

Workflows can be viewed or configured by selecting **Workflows » Configuration**.

Click **View** next to the Workflow you are interested in to view more details.

Click **Edit** to change the name, description or to disable the entire Workflow.

Field	Possible Values	Purpose
Workflow Name	Name	The Workflow name is a human-readable label for the Workflow.
Description	Description	The description is free text that provides information to Administrators about the Workflow.
Triggered after	Trigger actions	When set, the workflow will start automatically immediately after the selected action is complete (e.g., after the form is saved).
Entity	Fastpath Application object	The object type of workflow must match that of its trigger and parameters and is used to evaluate workflow step conditions.

Each Workflow has a name and description that explains the circumstance that causes it to trigger. These range from an Identity being created to a duplicate being detected. The Workflows themselves are comprised of a number of steps, each step describing an action that should be taken. The actions that the Steps describe are executed, in order, when a Workflow is triggered.

To configure the Steps that comprise a Workflow, first click **Edit** next to the Workflow and then click **Edit** or **Delete** next to the Step you would like to change or **Add Step** to create a new Step for the current Workflow.

Field	Possible Values	Purpose
Workflow Name	Name	The Workflow name is a human-readable label for the Workflow.
Order	Step number	Steps can be moved up or down in the order of execution by setting the step number here.

Field	Possible Values	Purpose
Action	Workflow Action	What will happen when this Step is executed.
Email Template	Template	When the action is to send an email you can choose a template here (this can also be a custom template, see Email Templates). ¹⁰
Recipient	Recipient	Who is to receive the email or be prompted for action.
Group	Admin Group	The Group to send the associated email to. This option is only available when Recipient is set to "Group".
Workflow	Existing Workflow	Choose another Workflow to be started. This option is only available when Action is set to "Start another workflow".

Due to restrictions which may be enforced by an Identity's Category or Credential Policy, some attributes are not available when choosing to "Update an Identity attribute automatically". Namely, the Credential Policy and the Category themselves as well as the password, start date, end date, duration, username, Organisational Unit, and the IGA ID. Furthermore, fields that store binary data (e.g., photos) can not be updated via Workflow actions either.

4.5.1 Assure SOD Risk Assessment

Assure can be used to provide a Risk Assessment of Additional Access requests, which is displayed on the approval page. (Also known as the User Workflow Event page).

A connection to Assure is required, this section explains how to configure that.

You may configure a connection to assure either via system settings or workflow parameters. If a workflow parameters is left blank, the relevant system setting will be used instead.

4.5.1.1 To configure Assure connection via System Settings

Navigate to **System » Settings » Application** and provide a value for each of the Assure settings.

4.5.1.2 To configure Assure connection via workflow action parameters

Navigate to **Workflows » Configuration » "An additional access request for risk assessment." » Step 1** (or another step if this has been modified). Edit the step with the action '**Perform Assure SOD Risk Assessment on requested Additional Applications and Entitlements.**' and provide a value for each of the Assure settings.

¹⁰The Email Template field will only display when the action is to send an email.

4.5.1.3 Assure settings

Setting	Description
Assure Base URL.	URL for the Fastpath Assure API endpoint. e.g. https://abc.fastpathassure.com/api/identitymanager/
Assure Token Endpoint URL.	URL for the OAuth2 Endpoint that provides access tokens for use with the Assure API.
Assure Tenant ID.	The Fastpath Assure Tenant ID (A GUID) to use.
Assure Client ID.	The Fastpath Assure Client ID to use for API Authentication.
Assure Secret.	The Fastpath Assure Client Secret to use for API Authentication.
Assure Mapping Table	A mapping table to map Lifecycle resource names to Assure Product ID's (optional). Resource (application) names are mapping table keys, while assure names are values.

All of the above Assure connection settings are required, except for mapping table, which is optional.

4.5.1.4 Viewing SOD Risk Assessments

A user with approve app/role request privilege can view a risk assessment, if available, through the normal approval page. The risk assessment appears below the first access item for approval.

The Bell Notification Icon appears in the menu bar at the top of the page to approvers when there is a request for approval.

Navigate to **Bell Notification Icon** » (browse to the row of interest) » **Approve or Decline Request**. This will display the approvals page along with a risk assessment, where one is available.

4.5.1.5 Troubleshooting SOD Risk Assessment

Little in the way of troubleshooting information is displayed in the UI so as not to interfere with the approval process except error messages that are returned from Assure in the place of a risk assessment are shown as warning messages at the top of the approval page. The system log provides the most useful information, especially with the debug level. See the Administrators Guide for more information the log and log levels.

4.5.2 Workflow step conditions

NOTE: An entity must be set on the Workflow in order to set conditions on the Workflow Steps.

Workflow steps can be run or skipped according to either a set of Rules or a Lua Script (when Lua scripting is enabled). Rules are evaluated based on the object set in the workflow 'Entity' field. Where the rules (or the lua script) produces a true result, the workflow step will be run; a false result will in turn skip the workflow step.

To configure Workflow Step Conditions, navigate to the Workflow Step you would like to place conditions, then select the **Conditions** panel.

A set of simple conditions can be configured, or for more advanced requirements, a Lua script can be provided.

Simple conditions currently operate on a subset of fields, with some data types not yet available to evaluate - for conditions using these a Lua script can be configured.

A hierarchy of conditions can be made by adding groups that may return true for a success against **all** rules (where every condition inside the group must be true) or **any** rule (where just one condition evaluating to true inside the group will return true for the whole group) according to your requirements.

The operators that are available to use in conditions are **Equal to**, **Not equal to**, **Greater than**, **Less than**, **Contains**, **Does not contain**, **Starts with**, and **Ends with**.

A Lua script that returns true, or a value that evaluates to true such as a non-empty string will cause the Workflow Step to run. A Lua script that returns false, an empty value, or nil will cause this Workflow Step to be skipped.

Either a set of conditions or Lua Script can be configured, not both. Configuring a Lua script will always override any existing conditions and cause them to be removed.

4.6 Administer Pending Workflow Events

Some workflows can pause their execution pending a manual action from an Administrative User. For example a workflow may prompt an admin to approve something. For each of these events an entry is displayed under this section in order that they be managed centrally for all users.

Administrators can view and manage pending workflow events by going to **Workflows » Pending**. All workflow events awaiting action can be seen here along with the admin users that have been notified to deal with the event.

There is a number of actions that can be performed against a workflow event by an admin. These actions will trigger another workflow, the following actions are available.

Action	Default Workflow	Description
Add User	add_user	This allows a new admin user to be added to a workflow event. The default workflow will email the admin to make them aware they have been added.
Remind User	remind_user	This allows an admin on a workflow event to be reminded. The default workflow will email the admin to remind them they have a pending event.
Remove User	remove_user	This allows an admin on a workflow event to be removed. The default workflow will email the user to let them know they have been removed from an event.
Delete Event	delete_event	This allows an admin to delete a workflow event completely. The default workflow will email all admins originally notified to make them aware the event has been deleted.

The default behaviour can be modified by editing the default workflows. You can also define custom actions to be run for a specific workflow that contains a prompt step by checking **Custom Admin Actions** when creating/editing the step.

4.7 Setting up Self Service Forms

Self Service Forms offer access to existing Identities or external Identities to manage their details or to register for access. By default, Self Service is disabled until at least one form is created. In order to create or manage Self Service Forms, please navigate to **Configuration » Self Service Forms** via the menu.

When creating or updating a Self Service Form, the following fields are available.

Setting	Possible Values	Purpose
Name	Free Text	The name of the form which will be displayed as a heading on the self service form when it will be accessed by Identities.

Setting	Possible Values	Purpose
URL Title	Alpha Numeric field (may contain dashes)	The URL Title will act as a unique identifier and be part of the Self Service Form's URL. If not provided, one will be generated using the Form's name.
Existing Identities only	On / Off	If checked, the Form will only be accessible for existing Fastpath Lifecycle Identities in possession of the unique URL. Please note that only Identities within the selected Categories and Organisational Units will have access to this form.
Require email confirmation	On / Off	If checked, Administrators will not be prompted to Approve Fastpath Lifecycle Identity requests until they have confirmed their email address after submitting the form, by following a unique link sent to them via email.
Use captcha	On / Off	Protect the Self Service Form against spam using captcha. The Fastpath Lifecycle domain will have to be added to the domain list for the corresponding site and secret key.
Captcha site key	On / Off	After registering for an account with Google's captcha service, please provide the site key here.
Captcha secret key	On / Off	Please provide your account's secret key here.
Additional Info	Free text	The additional info field, if provided, can be used to show information for, or greet, the Identities that will access the Self Service Form as it will be displayed below the heading, on the form.
Logo	Image	If provided, the logo image will be displayed above the form heading (i.e., the form name) on the Self Service Form.
Fields	On / Off	Provides the ability to specify which Fields the Identity will be able to add values for when accessing the form. Please use the search field located above the Field list to search for existing Fields and use the Field settings to configure form Fields or add new ones.
Organisational Units	Organisational Unit	The available Organisational Units from which the Identity can choose when filling in the form.
Categories	Existing Categories	Similar to the Organisational Unit, the Category field denotes which Categories are available when viewing the form.
Credential Policy	Credential Policy	A Credential Policy to be used when generating a username/password if the self-service request is approved.

Please note that selecting one Organisational Unit, or a single Category, will make these selected by default on the Self Service form. Selecting a single item for each of these (i.e., one Organisational Unit and one Category) will eliminate the Affiliation details step completely, and these options will be selected as defaults for any Identity registered using this form.

4.8 Pending Invitations View

Fastpath Lifecycle users can view the pending Invitations which are sent to Identities. To view the pending Invitations please select **Configuration » Pending Invitations**. Please note that this list will only show Invitations for which the related task has completed, and the Invitations have been sent. Once accepted, it will no longer be shown in this list.

4.9 Email Templates

Fastpath Lifecycle sends notification emails using pre-configured templates. These templates can include information about the Identity that they refer to and information provided by workflow parameters. There is a wide choice of template variables that you can use to customise the content of the email.

4.9.1 Setting up Email Templates

To add an email template or to modify an existing template please navigate to **Workflows » Email Templates**.

Setting	Possible Values	Purpose
Name	Free Text	The name of the email template.
Workflows	Workflows list	Select the Workflows for which this email template is available.
Language	Language dropdown	Select from the configured languages for which language to use this particular template.
Subject	Free text	Enter the subject for this email.
Message	Free text editor	Outline the content of the email. Variables can be used to include dynamic content. Please see below for available options.

In order to determine which template has been used to send out a particular email, please enable debug mode and this information will be shown in the email's body.

For most email templates (those relating to an Identity) the full list of Fields on the Identity are available as template variables (e.g., %givenname%) - in some cases extra template variables are available as well.

Table 4.18: Email template variables (part 1)

Template variable	Replacement Value
%iga_id%	The Fastpath Lifecycle ID for the Identity, RFC 4122 compliant GUID
%courtesytitle%	Courtesy Title/Honorific title (e.g., "Mr")
%givenname%	Given name / First name
%middleinitial%	Middle Initial
%surname%	Surname / Family name
%fullname%	Full name
%preferredname%	Preferred name
%previousname%	Previous name
%honsuffix%	Honorary suffix
%dob%	Date of birth in ISO format (yyyy-mm-dd)
%qualifications%	Qualifications
%phone%	Telephone number
%mobile%	Mobile (cell) telephone number
%email%	Internal email address
%extemail%	Personal email address
%organisation%	Organisation name

Template variable	Replacement Value
%jobtitle%	Job title
%orgunit%	Organisational Unit name
%orgunitref%	Organisational Unit reference
%gender%	Gender
%address1%	Primary address line 1
%address2%	Primary address line 2
%town%	Primary address Town / City
%region%	Primary address Region / County / State

Table 4.19: Email template variables (part 2)

Template variable	Replacement Value
%postcode%	Primary address Postal code / Zip code
%country%	Primary address Country
%password%	Initial account password
%credential_policy%	Fastpath Lifecycle Credential Policy
%uniqueid%	Unique ID / Username
%previousid%	Previous Unique ID / Username
%context%	DN of Identity eDir context
%status%	Identity Status Code
%reqtime%	The request time in ISO format, yyyy-mm-dd HH:mm:ss
%asstext%	Additional Information
%sponsor%	DN of Sponsor
%sponsorname%	Name of Sponsor
%createdby%	Created by
%rejectreason%	Reject reason
%viewbutton%	A link to view details about the Identity.
%url%	The base URL of the Fastpath Lifecycle application. This can be overwritten via Workflow parameters.
%loginurl%	The URL of the Fastpath Lifecycle Login page.
%template%	The name of the template that is currently being used.
%photo%	JPEG Photo (see below for instructions)

4.9.2 Embedding photos

To embed a photo in an email template use syntax like this:

```

```

4.9.3 Available Templates

These are the templates that are available in Fastpath Lifecycle by default and what they are used for in the out-of-the box configuration.

Table 4.20: Default Email templates

Template	Description
accessrequest	Sent to Fastpath Lifecycle Administrators when a User requests access to a feature they currently have no Privileges for. Identity template variables not available. Additional variables available: %accessrequest% and %username%.
accountactivated	Sent to an Identity home email address when his/her record is made Active.

Template	Description
accountandpass	Sent to an Identity's home email address when a record is created for them, and the Category has the 'Notify Identity via email' option checked. A home email address and a username (uniqueid) is also required.
accountcreated	Sent to an Identity's home email address when Fastpath Lifecycle receives a uniqueid (Username) from IDM.
accountterminated	Sent to an Identity's home email address when the Identity's account is terminated.
application	Sent by Self Service to an Identity's home email address to confirm that their request has been received. Additional variables available: %url%.
approver	Sent to Approvers of the Identity recorded Organisational Unit.
approverrequest	Sent to Approvers of the Identity recorded Organisational Unit when a Sponsor adds an Identity.
confirmemail	Sent to Identities after submitting a Self Service Form which requires email confirmation.
dailyroleapprequestnotification	Sent daily to Administrators (owners of Identity Roles or Applications) and it contains a summary of the requests made during the day.
expirynotify	Email notification about Identities due to expire soon sent to Administrators every X days where X is the amount of days configured on the Identity's Category.
extendnotice	Sent to the Identity after their access has been extended and will contain the new termination date.
invitation	Sent to an external person when a new Identity invitation is sent.
invitationadmin	Sent to an external person when a new Administrative User Invitation is sent.
othernotify	Sent to notification email addresses associated with the Identity Category when an Identity request is added.
rejected	Sent to an Identity's home email address when a request (other than a Sponsor request) is declined.
report	Sent to the current Fastpath Lifecycle User when requesting a report by email. The report will be attached to the email.
roleapprequestapprovedecline	Sent to Identities after an Application or Identity Role request which has been managed by an Admin and contains a summary of the approved and declined items.
sponsornotify	Sent to a Sponsor when an Identity record is made Active. Additional variables available: %sponsorname%.
sponsorrejected	Sent to a Sponsor when a Sponsor request is declined.
sponsorrequest	Sent to a Sponsor to confirm a Sponsor request has been received. Additional variables available: %sponsorname%.
temporaryassignuser	Sent to an Admin User after choosing to temporary assign their permissions to another Administrator.
temporaryassignuserreceiving	Sent when an Admin temporary assigns their permissions to another Administrator, as a notification for the receiving Administrator.
weeklynotify	Sent to Approvers weekly to list the number of outstanding requests. Additional variables available: %details%, %htmlDetails%.
weeklynotifyadmin	Sent to Fastpath Lifecycle Administrators weekly. Additional variables available: %requests%, %leavers%.

Tip: When debug mode is turned on, the ID of each template is included in the footer of each email sent (when using the default footer). This may help discover which template requires changes.

4.10 Compliance Policies

Compliance policies define regular automatic checks that should be made against Identities in order to enforce certain rules. For example to check for Identities that have never logged in.

To manage Compliance Policies select **Configuration » Compliance Policies** from the main menu.

Setting	Possible Values	Purpose
Name	Free text	The name of the Compliance Policy.
Compliance Policy Rules	List of Rules	Search for Compliance Policy Rules and relate these with the Compliance Policy.
Run Every	Number of days	Specify the run frequency for automatic compliance checking for each associated provisioning endpoint.
Run a workflow for each identity anomaly	Checkbox	Run a Workflow for each identity anomaly is that is detected. Be aware that this can create a very large number of Workflow events.

4.11 Setting up Roles

Roles define the grouping and dependencies of Resources and optionally Fastpath Lifecycle privileges. To manage Roles please select **Access » Roles** from the main menu.

Setting	Possible Values	Purpose
Name	Alphanumeric	Name of the Role.
Description	Free Text	Human readable description of the Role.
Can be added	On / Off	Denotes whether the Role can be added by an Identity (via Fastpath Self Service) or by an Admin via Fastpath Lifecycle. Adding it involves the Identity inheriting the Role without going through an Approval process. ¹¹
Managers	Identities	Optionally select Identities who have the system role 'Managers' to be a Manager for the Identities who have this Role.
Distinguished Name	DN	To allow the Role to be mapped to an LDAP Group, the DN may be changed here. Identities who are members of the LDAP Group specified in the DN will be granted membership to the local Role when they log in. ¹²
Owner	Administrative User or Role	Select the Administrative User(s) to receive and manage the Requests made for this Role. This option is only available if Can be added is turned off.
Reason is mandatory	On / Off	When an owner is provided and a request is made for this Role, a reason will have to be provided in order to make the request.

Setting	Possible Values	Purpose
Resources	Set / Not Set	To set the Resources that will be assigned to Identities with this Role. Please use the provided search field to find Resources and attach them to the current Role. This field also enables selecting Entitlement defaults for the Resources in this list by clicking the Entitlements icon next to the Resource name (double tick). The selected Entitlements will be granted by default for Identities that have this Role, and these will not allow disabling. However, further Entitlements besides the Role defaults can be added for each Identity within this Role.
Administrative Privileges	Set / Not Set	To set the Privileges that will be assigned to Identities with this Role. Please use the provided search field to find Privileges and attach them to the current Role.

To make a Role available for Identities to request via the Portal or for other Administrators to request it on behalf of an Identity via the “Additional access” panel, either make it “Addable” or add an owner for the Role. If the Identity does not already have the respective Role, it will be made available to be requested or added via Fastpath Self Service - by the Identity - as well as via the Identities’ Additional access panel - by an Administrative User.

By default, Fastpath Lifecycle contains a small selection of system Roles to define the basic Privileges required to manage Fastpath Lifecycle itself, and new Roles can be added.

4.11.1 Role Policies

Roles can be granted or removed according to either a set of Rules or a Lua Script (when Lua scripting is enabled). Rules are evaluated against active Identity data and where the Rules (or the lua script) produces a true result the Role will be granted to the Identity, or removed from the Identity where a false result was obtained.

To configure Role Policies select **Access » Roles** from the menu, select **View** beside the Role you wish to edit and then navigate to the **Role Policy** panel.

A set of simple conditions can be configured, or for more advanced requirements, a Lua script can be provided. Either way - when the conditions are met, the group will be granted.

Simple conditions currently operate on a subset of fields, with some data types not yet available to evaluate - for conditions using these a Lua script can be configured.

A hierarchy of conditions can be made by adding groups that may return true for a success against **all** rules (where every condition inside the group must be true) or **any** rule (where just one condition evaluating to true inside the group will return true for the whole group) according to your requirements.

The operators that are available to use in conditions are **Equal to, Not equal to, Greater than, Less than, Contains, Does not contain, Starts with,** and **Ends with.**

A Lua script that returns true, or a value that evaluates to true such as a non-empty string will cause the Role to be granted. A Lua script that returns false, an empty value, or nil will cause this role to be denied.

Either a set of conditions or Lua Script can be configured, not both. Configuring a Lua script will always override any existing conditions and cause them to be removed.

¹¹This feature is disabled by default for system Roles that have privileges. It’s available for other Roles, or you can re-enable the feature via **System » Settings » Application » Allow Roles with Privileges to be Added.**

¹²Group DN’s are generated automatically and set read-only (they cannot be edited) unless LDAP Authentication is enabled and the User has ‘Modify Group DN for a Role’ privilege.

Role Policies are evaluated on each change and also when an Identity is added or edited. There is also a cron task available (“ProcessRolePolicies”) which will evaluate role policies for all active Identities and this can be configured to run periodically, if required. See the section on [Tasks](#).

4.11.2 Default Roles

Fastpath Lifecycle comes with a set of system default Roles as follows:

Approvers Only have the ability to log in. Other Privileges are required in order to manage Identities, and these should be added explicitly.

Managers Only have the ability to log in. Other Privileges are required in order to manage Identities, and these should be added explicitly.

SelfService Required for the Self Service Forms and no changes should be made to this Group nor its related Roles.

Sponsors Have the ability to create Identity requests and in order to do so, Sponsors will have access to view Categories and Organisational Units. Additionally, members of this Group will appear in the ‘Sponsor’ autocomplete field.

Unrestricted Fastpath Administrators Please use sparingly and with caution as this Group provides unrestricted access to the entire Fastpath Lifecycle installation.

4.12 Setting up Resources

To configure Resources select **Access » Resources** from the menu.

Tip: You can import Resources from a Provisioning Endpoint connection, see the section on [Provisioning](#).

The Resources screen lists all the Resources. From here it is possible to add new Resources, edit existing Resources, and delete inactive (unused) Resources.

Setting	Possible Values	Purpose
Name	Alphanumeric	The unique name of the Resource.
Friendly Name	Free Text	An optional alternative name that is useful for humans rather than machines, intended to be more readable, recognizable, and memorable. This will be displayed to users when requesting through the self-service portal.
Description	Free Text	A description of the Resource. This will also be displayed to users when requesting through the self-service portal.
Custom field	Resource Custom Field	Allows attaching a Custom Field to a Resource in order to store extra data for these. Please note that only Resource Custom Fields will be available here. To add or edit a Resource Custom Field please navigate to Configuration > Fields.
Email Message	Free Text	If provided, this text will be included in the “accountactivated” email template (variable %resource_email_messages_html%). This can be used to provide additional instructions or information for the user (e.g., a URL to access the Resource or a welcome message).

Setting	Possible Values	Purpose
Application	On / Off	Enabling this option will allow adding extra details as well as make this Resource available for Identities, so they can request access to it.
Can be added	On / Off	Denotes whether the Application can be added by an Identity (via Fastpath Self Service) or by an Admin via Fastpath Lifecycle. Adding it involves the Identity inheriting the Application without going through an Approval process.
Owner	Administrative User/Group	The type of owner to add for this Resource. Selecting either of the two will enable choosing the User/Group by using the revealed User/Group field.
User	Administrative User	If User was selected as an Owner, this field will become available to choose the owner as the Administrative User to receive notifications regarding access requests made for this Resource.
Group	Administrative Group	If Group was selected as an Owner, this field will become available to choose the owner as the Administrative Group to receive notifications regarding access requests made for this Resource. Therefore, requests will be received and can be approved by any User found within the selected Administrative Group.
Label	Label	Choose a Label to categorise similar Resources.
Logo	Image	The logo will be displayed when Identities will request this particular Resource.
Access URL	URL	If the Application has a URL which allows access to it (SSO), please provide it here, and an Open button will be shown in Fastpath Self Service for this particular Application.
Catalogues	List of Catalogues	Placing the Resource in a Catalogue will make it available for Identities that belong to a Catalogue's Category.
Set existing Categories to	On (mandatory) / Off (mandatory) / On (optional) / Off (optional)	The default value for existing Categories. ¹³
Identity Roles	On / Off	Relate this Resource with Identity Roles.
Entitlements	On / Off	Attach Entitlements to this Resource.
Workflow Added	List of Workflows	A workflow set here will be triggered after a Resource has been added to an Identity.
Workflow Removed	List of Workflows	A workflow set here will be triggered after a Resource has been removed from an Identity.

Tip: If the Application checkbox is enabled and the Resource “Can be added” or it has an Owner provided, Identities will be able to request access to it via Fastpath Self Service or Administrative Users will be able to make Additional access requests on behalf of an Identity. The Resource will have to be added to a [Catalogue](#) which will have to be related with the Identity’s [Category](#) for it to show up in Fastpath Self Service or in the Additional access Identity panel.

¹³This will set the default for existing Categories, and Identities will be updated to set the Resource state (On (mandatory)/Off (mandatory)/On (optional) etc.) automatically after the Resource is saved.

Note: For a new Resource to be provisioned, the IDM system must be configured to recognise it.

4.13 Setting up Entitlements

To manage Entitlements, select **Access » Entitlements** from the menu.

Entitlements are used for configuring fine-grained access within Resources and can be attached to more than one Resource. As an example, a Resource named “HR Application” could use Entitlements to define access within that Application. Therefore, having “Add Users”, “Edit Users”, and “Update Salary” could be permissions that are available for Administrators within that particular Application. On the Identity panel, the [Effective Resources](#) field can be used to attach Entitlements to an Identity by selecting which of the three Entitlements are available for a given Identity.

Setting	Possible Values	Purpose
Name	Alphanumeric	The unique name of the Entitlement.
Friendly Name	Free Text	An optional alternative name that is useful for humans rather than machines, intended to be more readable, recognizable, and memorable. This will be displayed to users when requesting through the self-service portal.
Description	Free Text	A description of the Entitlement. This will also be displayed to users when requesting through the self-service portal.
Search for Resources	Resource	Allows selecting Resources that have this particular Entitlement attached to it.
List of Resources	Resources	Shows the Resources that have this Entitlement attached to them as well as allows detaching Resources.

4.14 Setting up Labels

Labels can be accessed from the **Configuration » Labels** menu.

Labels offer a way of grouping similar Resources, when “Application” is turned on for the latter, so that Identities can easily recognise them when making requests.

Setting	Possible Values	Purpose
Name	Alphanumeric	The Label’s name, used to group Resources. This will be shown for Identities when performing Requests.
Applications	List of Resources	The Resources/Applications available via this Label.

4.15 Setting up Catalogues

Catalogues offer a way of grouping Resources so they can be Requested by Identities that belong in the same Category as the Catalogue.

Setting	Possible Values	Purpose
Name	Alphanumeric	The Catalogue’s name, used to group Resources. This will be shown for Identities when performing Requests.

Setting	Possible Values	Purpose
Category	Category	Choose a Category to relate this Application Catalogue with. Only Identities in this Category will be able to Request Applications from within this Catalogue.
Resources	List of Resources	The Resources/Applications available via this Catalogue.

4.16 Setting up Categories

To configure Categories, please select **Access » Categories** from the menu.

The initial Categories screen will list all the Categories. From here it is possible to add new Categories, edit existing Categories, and delete unused Categories.

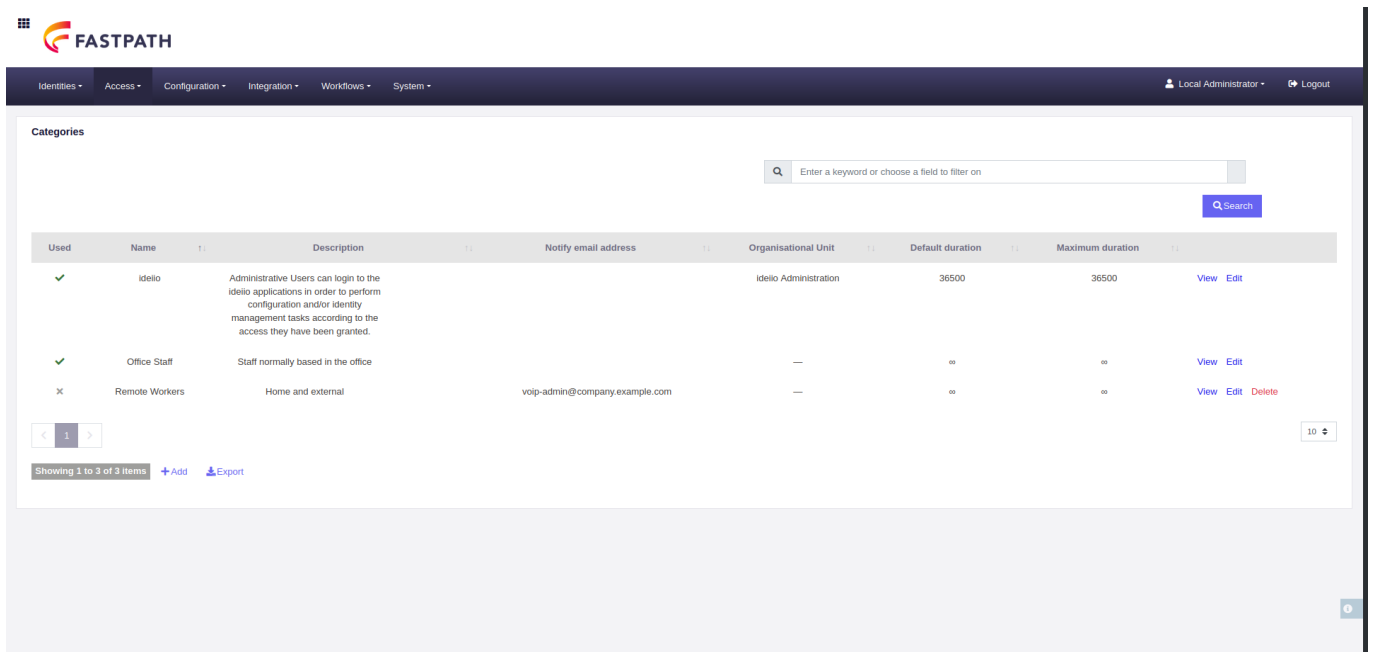


Figure 4.1: List of Categories

Note: A change made to a Category, Credential Policy, Organisational Unit, or a Category's duration will not affect any existing Identities until a specific change is made to their Identity record. However, some changes will be processed in the background and applied to the Identities as well as potentially be provisioned to external systems via Endpoints (e.g., Resource changes).

Setting	Possible Values	Purpose
Name	Alphanumeric	Name of the Category.
Description	Free Text	Human readable description of the Category.
Notify Fastpath Identity via email	On / Off	If checked, Fastpath Lifecycle Identities will receive an email using template accountandpass when their status changes to Active.
Notify email address	Email address	When completed, an email using template othertofify will be sent when an Identity record is added.
Credential Policy	None / Credential Policy	The username and password generation rules to apply to Identities in this Category.

Setting	Possible Values	Purpose
Organisational Unit	None / Organisational Unit	The default value for the Organisational Unit field for Identities added to this Category.
Default Duration	0 - 36500 (days)	The default initial duration of the Identity record.
Maximum Duration	0 - 36500 (days)	The default maximum number of days that an Identity record can stay active.
Days before termination to notify	1 - 150 (days)	The amount of days to notify before an Identity's end date is reached. The notification will consist of an Extend Workflow being raised as well as an email summary being sent out to Administrators to notify about the Identities account termination.
Resources	List of Resources	Search for Resources and relate these with the Category. Only these Resources will be made available along with the selected defaults when managing an Identity in this Category.
Roles	List of Roles	Search for Roles and relate these with the Category. Only these Roles will be made available along with the selected defaults when managing an Identity in this Category.

Note: If Credential Policy is set to 'None' the user will be prompted to enter a Credential Policy at the time the Identity is added, or the request is approved.

The screenshot shows the 'Add Category' form in the FASTPATH system. The form is titled 'Add Category' and includes the following fields and options:

- Name:** A text input field.
- Description:** A larger text input field.
- Notify Identity via email:** A checkbox that is currently unchecked.
- Days before termination to notify:** A numeric input field with a value of 7 and a 'Days' unit selector.
- Identity default values:**
 - Default Credential Policy:** A dropdown menu set to 'None'.
 - Organisational Unit:** A search input field.
 - Default duration:** A numeric input field with a value of 7 and a 'Days' unit selector.
 - Maximum duration:** A numeric input field with a value of 7 and a 'Days' unit selector.
- Birthright Resources:**
 - Search for Resources:** A search input field.
 - Resources:** A list box showing 'None'.
- Available Roles:** A section at the bottom of the form.

Figure 4.2: 'Add Category' Form

If configured, a list of Resources will be available at the bottom of the Category form via the dedicated search field, and the default provisioning of Resources for members of the Category can be set here. Please note that changing Resources on an existing Category will affect Fastpath Lifecycle Identities as it will trigger a background task in order to provision these.

For each Resource the following options are available.

Setting	Possible Values	Purpose
Resource	On (mandatory) / Off (mandatory) / On (optional) / Off (optional)	To set the mandatory and optional Resources available to Identities added to the Category.

Note: The preferred way to confer Resources to Identities is via Identity Roles.

4.17 Administrative Users, Roles & Privileges

Fastpath Lifecycle Administrative Users are Identities that have been granted Privileges (via Roles) which provide access to the Fastpath Lifecycle features that they need, while restricting access to other areas.

4.17.1 Administrative Users

Administrative Users can be added and managed locally, or they will be added automatically by the system as users login via LDAP or SAML2.0. The source of each user (Local, LDAP, SAML) is displayed on the Identity page and on the User's own profile page.

See the section on [Managing Identities](#) to learn how to add and manage Identities.

4.17.1.1 Profile page

Any user can view their own profile page, which displays information about the User, a list of Roles, and Privileges, and forms to temporary assign privileges to another Administrator and (if enabled) to change their password.

To access your own profile page, click your own username/name from the menu (next to Logout, in top right-hand corner) and then click "Profile".

Field	Notes
Username	To provide the username which will be used when logging in.
Email address	The Admin's email address.
Full name	Optional full name.
Password	Enter the password which will be used when authenticating.
Temporary Assign Permissions	Allows assigning an Admin User's permissions to another Admin User, for a period. If enabled, it will allow selecting the User as well as the period for which the permissions will be assigned. Please note that Administrators also have this option available via their account's profile.
Assign to	Visible when "Temporary Assign Permissions" is enabled, and it allows selecting the Administrator which will inherit the permissions of the User currently being edited / added.
Assign period	Visible when "Temporary Assign Permissions" is enabled, and it provides the ability to select a period of time for which the permissions will be assigned by choosing a start and end date.
Roles & Privileges	The Roles that the Administrative User will be a member of and inherit Privileges from.

4.17.2 Administrative Roles

Administrative Roles are Roles with a collection of Privileges.

See [Setting up Roles](#) for information on setting up Administrative Roles.

4.17.3 Administrative Privileges

Privileges define the permissions required to administrate Fastpath Lifecycle, ranging from the permission to log in to the ability to manage Identities, Categories, Credential Policies, to view the Audit log, etc. Each feature of Fastpath Lifecycle that can have access restricted to it has a Privilege defined.

For the purpose of granularity, Privileges can also be added to provide access to certain Fastpath Lifecycle features by Category, Role, or Organisational Unit.

Adding a Privilege that is linked to a Category, Role, or Organisation Unit will restrict the ability to use the respective Privilege only with Identities which are related with the corresponding Category, Role, or Organisation Unit. You can create as many of these as you like.

Setting	Possible Values	Purpose
Administrative Privilege	Dropdown list of privileges	To select a Privilege that you would like to further restrict with this Privilege.
Entity	None / Category / Role / Organisational Unit	The entity type that you would like restrict by.
Object	A Category / A Role / An Organisational Unit	The object that you would like to restrict by.

Note: Remember, after creating a Privilege you will need to assign it to a Role, and that Role must be linked to a Group that has members before the Privilege will take effect.

4.18 Lua Scripts

Lua Scripts provide advanced logic to extend Fastpath Lifecycle capabilities programmatically beyond those provided out of the box.

“Lua” (pronounced LOO-ah) means “Moon” in Portuguese and it’s the name of a fast, powerful, and lightweight programming language with a simple procedural syntax. Fastpath Lifecycle can execute the scripts that you create inside a safe, sandboxed, Lua 5.1 environment in to provide your own complex field transformations and more.

Lua scripting is an advanced feature and is disabled by default, if it is required it can be enabled by navigating to **System » Settings » Application** and using the “Enable Lua Scripts” setting.

4.18.1 Setting up Lua Scripts

To manage Lua Scripts please select **Configuration » Lua Scripts** from the main menu.

Setting	Possible Values	Purpose
Name	Free text	The name of the Lua Script.
Lua Script	Lua Script (code)	Valid Lua code.

The syntax of your code will be checked as it is added (or edited) but please test your script before putting into production use as errors can also occur at runtime.

Lua scripts can be added as transformations to form fields, and these will run for any Identity form action (e.g., Add/Edit), including those made via the API. The return value of your script will become the new field value.

Lua Scripts can also be run to transform provisioning data.

4.18.2 Getting started with Lua programming

This section provides an introduction to scripting with Lua and describes some of the major features of the language. While this is enough to get you started it's not a complete guide, for that we recommend reading the [official documentation](#).

Syntax

Statements are separated by new lines or Semi-colons (;). Unlike some languages Lua does not require Semi-colons after every line. Semi-colons should be used to separate multiple statements on a single line and can also be used where there may be ambiguity.

Comments

Lua supports both single line and block comments.

Comments begin with double-hyphen

```
-- This line is a comment
```

and block comments are enclosed with double square brackets.

```
--[[  
    This line is a comment  
    and so is this one  
--]]
```

Variables

Lua variable names can be letters, digits, and the underscore character. Names can begin with either letters or underscore but cannot begin with a digit. Lua is case-sensitive so upper and lower case letters are distinct.

Variables are dynamically typed and are scoped either Global or Local. Unlike most languages all variables are global unless explicitly declared as local.

Types

Lua is a dynamically-typed language, so variables and function arguments have no type. Only the values assigned to variables have a type, and all values have a type.

nil

nil represents the absence of a value. Nil may not be used as a key in a table. When converted to a string the result is "nil" and when converted to a boolean, nil is considered false.

Boolean

Boolean values are true and false. Unlike most other languages, boolean values can not be directly converted to numbers.

Strings

Strings are encoded as UTF-8 and may contain up to 4 bytes per character.

String Literals are enclosed in single or double quotes, they're both treated equally.

```
string = 'single quoted'  
another_string = "or double quoted"
```

Multi-line String Literals start with double square brackets.

```
string = [[
Programming is fun.
If you want to have more fun,
program in Lua!
]]
```

Strings can be concatenated with .. (two dots).

```
combined_string = 'Hello ' .. 'World!'
```

The following escape sequences are recognized:

```
\b backspace
\t horizontal tab
\n newline
\r carriage return
\" double quote
\' single quote
\\ backslash
```

Tables

Tables are associative arrays and are defined with a pair of braces (curly brackets). Thus, an empty table is {}.

Any value except nil may be stored in a table, and an attempt to store nil has the effect of removing the key from the table. Accessing any key that has not been set will result in nil.

A comma separated list of field specifiers may be included inside the braces in order to populate a table on creation.

```
fruit_table = {
  [raspberry] = 'red',
  [orange] = 'orange',
  [banana] = 'yellow',
}
```

Fields in a table are accessed using bracket notation.

```
color = fruit_table['raspberry']
```

Other forms of field specifiers are available.

Arithmetic Operators

Operator	Description	Example
+	Addition	a + b
-	Subtraction	a - b
*	Multiplication	a * b
/	Division	a / b
%	Modulus	a % b
^	Exponent	a^10
-	Unary minus	-a

Comparison/Relational Operators

Operator	Description	Example
==	Equal to	a == b
~=	Not equal to	a ~= b

Operator	Description	Example
>	Greater than	a > b
<	Less than	a < b
>=	Greater than or equal to	a >= b
<=	Less than or equal to	a <= b

Logical Operators

Operator	Description	Example
and	Logical AND	a and b
or	Logical OR	a or b
not	Logical negation (NOT)	not b

Other Operators

Operator	Description	Example
..	Concatenate two strings	a .. b
#	Unary Length (of a string or table)	#a

Loops

Four types of loop are available: while loop, repeat loop, and two styles of for loop.

While loop

Repeats statement(s) while a given condition is true, with the condition tested before each iteration of the loop is executed.

```
while (x > 20) do
  x = y - a
  a = a + 1
end
```

Repeat loop

Repeat loops are identical to while loops except that the condition is tested after each iteration of the loop.

```
repeat
  result = result .. i .. '\n'
  i = i + 2
until i > 10
```

For loop (traditional)

Declare a local variable, and repeat the block for values from value 1 to value 2 adding value 3 on each iteration. The expression list is evaluated once before iteration starts.

```
for v = 0, 1, .5 do
  a = a + v
end
```

For loop (iterator)

Declare a local variable, and repeat the block for values from value 1 to value 2 adding value 3 on each iteration. The expression list is evaluated once before iteration starts.

```
for v = min, max, increment do
    a = a + v
end
```

Abort

You can break out of any loop with a break statement, which will terminate the loop and begin executing the next statement following the loop.

```
for variable = 1, -1, -.5 do
    if variable == 0 then
        error = 'SNAFU'
        break
    end
    log.debug(error)
end
```

Conditional Statements

Lua treats any combination of boolean true and non-nil values as true, and it's worth noting that Lua **treats zero and an empty string as true**.

Conditional statements can be nested.

if statement

Statements inside the if block will be executed only if the boolean expression evaluates to true.

```
if x > 10 then
    result = 'Success'
end
```

if ... else statement

Similar to the if statement. An optional else block will execute statements inside the only if the boolean expression evaluates to false.

```
if x > 10 then
    result = 'Success'
else
    result = 'Failure'
end
```

Functions

A function is a named section of a program that combines multiple statements to perform a specific task.

Functions in Lua are global in scope by default (unless explicitly defined as local) and are usually defined like this

```
local function transmogrify(argument1, argument2, argument3)
    local a = argument1 + argument2 + argument3
    local b = argument1 * 5
    return a,b
end
```

Functions are called much like they are in most other languages, that is, a function name followed by a list of arguments in parentheses.

```
transmogrify(temperature, speed, mass)
```

As you can see it's possible to return multiple values by passing them as comma separated values after the return keyword.

Native Lua Functions and Variables

Fastpath Lifecycle supports most of the Lua functions and variables that are native to Lua. This section lists the features that are available.

_G Table Variable

A table variable that holds a reference to the global variables currently in memory.

```
a = 10
b = _G[a]
c = _G.a
```

The global variable a may be accessed as `_G.a` or `_G[a]`

_VERSION Variable

A string with the currently running Lua version.

assert

Throws an error if the given value is false or nil . Returns the value that was passed into the function if the assertion succeeds.

```
assert(value, string "assertion failed!")
```

collectgarbage

Fastpath Lifecycle supports only the "count" operation which returns the total memory in use by Lua (in kilobytes).

```
collectgarbage("count")
```

getfenv

Returns the current environment in use by the function. The parameter can be a Lua function, or a number that specifies the function at that stack level: Level 1 is the function calling getfenv. If the given function is not a Lua function, or if the parameter is 0, getfenv returns the global environment. The default is 1.

```
getfenv(1)
getfenv('foo')
```

getmetatable

Returns the metatable of the specified object. If the object does have a metatable, but the metatable has a `__metatable` field set, the value of `__metatable` will be returned instead, otherwise nil will be returned.

```
getmetatable(obj)
```

ipairs

Returns three values: a function, the table `t`, and an iterator.

```
f, t, i = ipairs(fruit_table)
```

next

Iterating over the keys in a table. If the key is `nil` or unspecified, it returns the “first” key in the table and its value; otherwise, it returns the “next” key and its value. When no more keys are available, it returns `nil`. It is possible to check whether a table is empty using the expression `next(t) == nil`.

Note: the order in which the keys are returned is not specified, even for tables with numeric indexes. To traverse a table in numerical order, use a numerical `for` or `ipairs`.

The function behaviour is undefined if, when using `next` for traversal, any non-existing key is assigned a value. Assigning a new value (including `nil`) to an existing field is allowed.

```
next(table, key)
```

pairs

Returns the next function, and the passed table, so that the construction will iterate over all key/value pairs of that table. See the function `next` for the caveats of modifying the table during its traversal.

```
f, t = pairs(fruit_table)
```

pcall

Calls the function `func` with the given arguments in protected mode. This means that any error inside `func` is not propagated; instead, `pcall` catches the error and returns a status code. Its first result is the status code (a boolean), which is `true` if the call succeeds without errors. In such case, `pcall` also returns all results from the call, after this first result. In case of any error, `pcall` returns `false` plus the error message.

```
bool, Variant = pcall(function func, Tuple args)
```

rawequal

Returns a boolean to indicate whether parameter one is equal to parameter two, without invoking any metamethod.

```
b = rawequal(v1, v2)
```

rawget

Gets the real value of `table[index]`, without invoking any metamethod.

rawset

Sets the real value of `table[index]` to a given value, without invoking any metamethod.

select

Returns all parameters after parameters number `index`.

setfenv

Sets the environment to be used by the given function.

setmetatable

Sets the metatable for the given table.

tonumber

Attempts to convert the parameter into a number with an optionally specified base to interpret the value in. If it cannot be converted, this function returns nil. The base may be any integer between 2 and 36.

```
num = tonumber('24')
num = tonumber('24', 12)
```

tostring

Receives an argument of any type and converts it to a string in a reasonable format.

type

Returns a string with the type of the object passed as a parameter.

```
t = type(foo)
```

unpack

Returns the elements from the given table.

```
e = unpack({1,2,3})
```

xpcall

This function is similar to pcall, except that you can set a new error handler. xpcall calls function f in protected mode, using err as the error handler. Any error inside f is not propagated; instead, xpcall catches the error, calls the err function with the original error object, and returns a status code. Its first result is the status code (a boolean), which is true if the call succeeds without errors. In this case, xpcall also returns all results from the call, after this first result. In case of any error, xpcall returns false plus the result from err.

Fastpath Lifecycle Lua Library

message

Print a notification message at the top of the page.

```
message.success('A success')
message.info('Some information')
message.warning('A warning')
message.error('An error')
```

Note, these functions only make sense when your script is executed interactively as the message will only be sent to the user that is currently signed in and has begun the action that led to your script being run.

identity

Get information about the Identity that is currently being processed.

Form Field Transformations

To set the value of the field that called your Lua Script simply return a string.

```
return string.upper(identity.form('surname'));
```

To retrieve the original value of a field you can use `identity.original`, e.g.

```
identity.original('fieldname');  
identity.original(identity.fieldName());
```

Where 'fieldname' is the name of a Fastpath Lifecycle identity field. For example to check whether a field changed you could use:

```
if identity.form('jobtitle') ~= identity.original('jobtitle') then  
    message.success('Job title changed from ' ..  
        identity.original('jobtitle') .. " to " .. identity.form('jobtitle'))  
end
```

To retrieve a list of Identity form fields, use `identity.fields()`, e.g.

```
log.info('List of fields: ' .. table.concat(identity.fields(), ", "));
```

Read the value of any form field using `identity.form`, e.g.

```
identity.form('fieldname')
```

Where 'fieldname' is the name of a Fastpath Lifecycle identity field. See **Configuration » Fields** for a list of field names.

For example:

```
identity.form('address');  
identity.form('surname');
```

To retrieve the name of the form field that is running the transformation script.

```
identity.fieldName()
```

To retrieve identity fields relating to the manager of the current identity (if set), e.g.:

```
identity.manager('uniqueid')  
identity.manager('fullname')
```

To retrieve identity roles:

```
identity.roles()
```

For example to display role names along with ID's for each that are granted to the Identity:

```
for i, v in pairs(identity.roles()) do  
    message.info(v .. ' (ID: ' .. i .. ')')  
end
```

To retrieve identity resources:

```
identity.resources()
```

For example to display resource names along with ID's for each that are granted to the Identity:

```
for i, v in pairs(identity.resources()) do  
    message.info(v .. ' (ID: ' .. i .. ')')  
end
```

To retrieve identity entitlements:

```
identity.entitlements()
```

For example to display entitlement names along with ID's for each that are granted to the Identity:

```
for i, v in pairs(identity.entitlements()) do
    message.info(v .. ' (ID: ' .. i .. ')')
end
```

log

Make an entry in the Fastpath Lifecycle log file.

```
log.alert("This is an alert to indicate that action must be taken immediately.")
log.fatal("This is a fatal error, my Lua script has gone badly wrong.")
log.error("This is an error, something's not quite right with my Lua Script.")
log.warn("This is a warning, I'm pretty sure it's not supposed to do this.")
log.debug("This is a debug message, useful while developing your script.")
log.notice("This is a significant informational notice.")
log.info("This is a normal informational notice.")
```

plugin

Call a function provided by a Fastpath Lifecycle plugin.

Note: This will only be available if you have a plugin that supports it installed and enabled. Refer to your Plugin documentation for full instructions.

```
plugin.somefunc(param1, param2, param3)
```

action

Get information about the action that called the Lua script. This can be useful to make your script act differently depending on how it has been called. For example, to run a form field transformation on when an identity is added but not later when it is edited.

With `action.type()` you can get the type of action that called the Lua script.

```
action.type()
```

This will return the type of action, which can be one of the following values:

- validation - Called while validating the script on save.
- workflow - Called from a workflow action.
- provisioning - Called from a provisioning task.
- panel - Called from a form panel.
- role - Called from a role policy.

For more granular information about what called your script you can use `action.trigger()`, for example:

```
action.trigger()
```

The return value of `action.trigger()` varies depending on the action type.

If this is the provisioning type it will return the endpoint id.

The panel type will return the calling panel set, for example it would return `identity` when making a change to an identity in the Fastpath Lifecycle application.

The validation type will contain the current scripts name.

For a workflow type it will return the ID of the workflow step.

For a role (role policy) type it will return the ID of the Role being evaluated.

Tip: You can see the return value for your use case by logging the output.

```
log.debug('Triggered by:' .. action.trigger())
```

To return the name of the action itself, use `action.get()`:

```
action.get()
```

Again the return value varies depending on the action type.

If this is the provisioning type this will return `provision`.

The panel type will contain the panel name. For example if editing an identity, this will return `edit`; adding will return `add`, etc.

The validation type will return `validate`. When a script is run from a workflow action or a role policy the value returned will be the name of the script.

Tip: You can see the return value for your use case by logging the output.

```
log.debug('Triggered by:' .. action.get())
```

workflow

Get workflow parameters. Available when the Lua Script was run from a Workflow Action.

Return a single parameter value.

```
workflow.parameter('stepid')
```

Return a table containing the parameters of the running workflow.

```
workflow.parameters()
```

Trigger a workflow to run.

When the workflow starts it will inherit parameters from the original workflow, these can be overridden from Lua by passing a table of parameters as the second argument.

Tip: You can see the names of parameters required by workflow actions by viewing a workflow step for the action you are interested in, the step edit form shows the names underneath each parameter form field.

```
workflow.trigger(workflowid, params)
```

This example form field transformation uses `workflow.trigger()` to start a workflow that will send an email and passes two parameters that the email template will display to the user (using `%contact_point%` and `%contact_number%`). The workflow will be triggered only if the field value contains one of the job titles from the script.

```
-- An example form field transformation script to send a welcome email to new
-- Identities with certain job titles using a workflow trigger.

local wflow_id = '6A48E991-780A-4348-A70F-9FFFF0C95D72'
local wflow_params = {contact_point = "Boston", contact_number = "+1 3812 128771"}
local titles = {"Trainer", "Technician", "Clerk", "Mechanic"}
local field_value = identity.field();

local function contains(haystack, needle)
    for key, value in pairs(haystack) do
        if value == needle then return key end
    end
    return false
end

if contains(titles, field_value) then
```

```

    workflow.trigger(wflow_id, wflow_params)
end

-- Store the form field data as-is without any changes.
return field_value

```

mappingTable

Retrieve mapping table information from Fastpath Lifecycle.

Tip: See the section [Mapping Tables](#) to learn about mapping tables and how to set one up.

Return a Mapping Table's row value by providing a dot notation string. For example, if the table's identifier is `identityMap` and it contains a row key `example`, this method will be called as `mappingTable.getValue('identityMap.example')`. The return will be a string containing the actual table key's value.

```
mappingTable.getValue('table.row')
```

Return an entire Mapping Table along with its rows by providing the table's identifier. Continuing from the example above, the table's identifier will be `identityMap`. The table will contain an `id` (string), `tid` (IGA tenancy ID as a string), `identifier` (the same string provided to find the table), `description` (string), `created_at` (string), `modified_at` (string), `rows` (an array containing tables of key and value pairs - the key's name under `key` as well as its value under `value`).

```
mappingTable.get('identifier')
```

Return only the rows of a Mapping Table using its identifier. The rows will consist of an array containing tables of key and value pairs - the key's name under `key` as well as its value under `value`.

```
mappingTable.getRows('identifier')
```

This example form field transformation script sets the value of a form field by finding the key from another form field and looking that up in a mapping table.

The mapping table for this example looks like this:

Table 4.36: cityCodeMap Mapping Table (example).

Key	Value
101	New York
102	Paris
103	Tokyo

The script appends the value of the 'citycode' custom field to the `mappingTable.getValue()` parameter in order to look up and return the value.

```
return mappingTable.getValue('cityCodeMap.' .. identity.form('citycode'));
```

The result will be that when the 'citycode' custom field has a value of 103, our field will receive a value of 'Tokyo'.

generate

Generate data using Fastpath Lifecycle.

Obtain a valid GUID (globally unique identifier) using the same means as Fastpath Lifecycle:

```
generate.guid()
```

Get a random string of characters. The parameter is an int to indicate the length. The method used to generate the string is cryptographically strong but note that since it uses a fairly small pool of

characters using these strings as passwords will require quite a long string for reasonable security.

```
generate.randomString(25)
```

session

Get the username of the current administrative user.

```
session.username()
```

Get the IGA ID (Identity ID) of the current administrative user.

```
session.igaId()
```

Lifecycle

Miscellaneous functionality exposed for Lua by the Fastpath Lifecycle application.

Verify if a string consists of a valid GUID by calling the following function:

```
Lifecycle.isGuid('YOUR_STRING_HERE')
```

Get the version number of the current installation. Use this to check that your script is running on the expected software version.

```
Lifecycle.version()
```

JSON

Convert data to a JSON string and back again.

This will encode Lua data as a JSON string.

```
JSON.encode(items)
```

This will encode Lua data as a more readable JSON string.

```
JSON.encode_pretty(items)
```

This will decode a JSON string and return lua data.

```
JSON.decode(person)
```

str

Transliterate a UTF-8 string to an ascii/Latin1 string.

```
str.ascii('€')
```

Trim. Strip whitespace from the beginning and end of a string.

```
str.trim(' hello world. ')
```

Left Trim. Strip whitespace from the beginning of a string.

```
str.ltrim(' hello world.')
```

Right Trim. Strip whitespace from the end of a string.

```
str.rtrim('hello world. ')
```

4.18.3 Differences from standard Lua

Fastpath Lifecycle provides a Sandboxed Lua Environment, and some functions are not available; print(), error(), dofile(), loadfile(), newproxy() and the package 'io', the package 'io' including require() and module(), load(), loadstring(), and others.

Some useful extra functions are made available, e.g., identity.form() and log.error(). These extra functions may vary slightly between application versions, check the release notes carefully when upgrading.

4.19 Mapping Tables

Mapping Tables, also referred to as Lookup Tables, provide a way of mapping keys with values. They can contain multiple key value pairs in the form of rows.

Using a table's identifier, a key's value can be retrieved via Lua scripts.

A mapping table can also provide a list of items for a dropdown or autocomplete field, with field data from keys and data labels from mapping table values.

4.19.1 Setting up Mapping Tables

To manage Mapping Tables please select **Configuration » Mapping Tables** from the main menu.

Setting	Possible Values	Purpose
Identifier	Alphanumeric text	A table's unique identifier.
Description	Free text	A table's optional description.
Rows	Alphanumeric key / Free text value	Add rows for the mapping table by providing key value pairs.

A mapping table's values can be retrieved in Lua by using the table's identifier along with the required key, using dot notation (e.g., tableIdentifier.rowKey). Please see the mappingTable section inside [Lua Scripts](#) for more details.

4.20 Bulk Import

At this point you may wish to import some Identities from a CSV file to manage with Fastpath Lifecycle. See the section on [Importing Identities](#).

4.21 Tasks

Some actions, particularly those that may take some time to run, are executed in the background as a 'task'. You can view the status of tasks that are pending, are running and that are complete via **System » Tasks**.

From this section you also clear the list of tasks that have finished.

See the section on Configuring cron in the Administrator's guide for more information.

4.22 Email Configuration

Fastpath Lifecycle sends email notifications to identities and to Fastpath Lifecycle users as part of workflows and as reminders. To configure Fastpath Lifecycle mail server settings select **System » Settings » E-mail** from the menu.

4.23 Auditing Fastpath Lifecycle Usage

A list of security sensitive actions performed whilst using Fastpath Lifecycle, along with details of who performed them and when, is available to Fastpath Lifecycle Administrators via the menu option **System » Audit**.

The information displayed in the Audit Log is as follows: Date & Time, User (Shown in DN format or full name), Audited Action, Object (Name/Description of the object the audited action was performed on), Result (Either Success or Failure), and Notes which can contain extra details such as the new and the old value when an edit has been performed or the email address where an Invitation has been sent to, etc.

4.23.1 Exporting the Audit Log

The audit log entries can be exported in CSV (Comma-separated values) format which can be imported in spreadsheet, database, or reporting software using the **Export** link shown below the list of Audit log entries.

4.23.2 Limiting the size of the of Audit Log

By default, audit entries are kept forever, but you will likely want to configure how long to keep these, as they will consume a large amount of storage over time.

You can configure the maximum number of entries to keep and/or the maximum age of entries via the Application section of **System » Settings » Application**.

When `cron-daily.php` is configured to run (as it is by default), the older Audit entries will be deleted daily and consequently will not be displayed on this page.

4.24 Fastpath Lifecycle Reporting

The Reports system area of Fastpath Lifecycle is where reports created by automated compliance checking will appear. Once configured, compliance checking will run periodically to compare the state of identities against a set of rules. Each rule may produce a report listing the names and IDs of anomalous identities.

Chapter 5

Integration

5.1 Connecting Fastpath Lifecycle to your Identity Management System

Fastpath Lifecycle provides several options for connecting to onward Identity Management systems.

- Provisioning via SCIM (for example to PingFederate or PingOne Directory)
- Staging

5.2 Provisioning

Fastpath Lifecycle provides a flexible provisioning solution that enables:

- Provisioning and de-provisioning of Identities
- Provisioning of Resources as Groups with managed User Group Membership
- Provisioning of Identity updates
- Real-time provisioning status
- Connections to SCIM

5.2.1 Setting up Provisioning Endpoint Connections

To set up connections to Provisioning Endpoint Connections for SCIM, please go to the **Integration » Provisioning** menu option.

5.2.1.1 Endpoint Connection

Setting	Possible Values	Purpose
Name	Free text	The unique name of the Endpoint connection.
Enabled	On / Off	This will enable or disable the Endpoint connection.
User endpoint	URL	The remote Endpoint URL for user operations.
Group endpoint	URL	The remote endpoint URL for group operations.
Verify Certificate	On / Off	When this option is enabled, Fastpath Lifecycle will verify the authenticity of the server's certificate. Disabling verification of the certificate is insecure.
Authentication	Dropdown	Only HTTP Basic Authentication is supported.

Setting	Possible Values	Purpose
Client ID	Username	Client ID is the username used for accessing the Endpoint.
API Key	Password	API Key is a password used for authentication when accessing the Endpoint.
Use PATCH	On / Off	Using PATCH is recommended, although not all Endpoints support it. When this is set to Off several operations will be much less efficient and provisioning will be slower as a result.
Resource	Select from existing Resources	If a Resource is selected it will provision that Resource to the Endpoint.
Delete or make inactive	Dropdown	Select what happens at the remote endpoint when a resource is removed, or an identity is deleted. You can choose to delete the user, set the user to inactive, or do nothing which will only remove the group membership relating to the endpoint connection resource.
Custom field (External ID)	Select from existing Custom Fields	Select a Custom Field to receive a unique identifier from the Endpoint application. This Field may not be shared by multiple Endpoints.
Compliance Policy	Dropdown	Select an existing compliance policy in order to run the policy against Identities related to this endpoint connection.
Provision groups for	Dropdown	Select whether to provision all resources, no resources, those selected on this form, or all except those selected on this form.
Search for Resources	Select from existing Resources	When the 'Provision groups for' setting is not all or none, here you can set the resources that will be provisioned to the remote endpoint. Either as a whitelist or as a blacklist depending on the above.
Selected Resources	Resources	The selected resources to use with the 'Provision groups for' setting.
Create groups	On / Off	When set to On new Groups will be created at the remote endpoint where required. Otherwise, only existing groups will be used. Without this option group provisioning will fail if the group does not already exist at the endpoint.
Enable Readback	On / Off	When readback is enabled we will read the user data returned from the endpoint, as the user is provisioned, and write that back into the Identity record. This means that any generated data or transformations made at the endpoint will be incorporated back into the Identity (and potentially then provisioned out to other endpoints!). This feature normally requires the endpoint to provide user data in its responses, but if it doesn't (not all do) then tasks will be created to fetch the data separately.

Setting	Possible Values	Purpose
SCIM Core Schema	On / Off	SCIM Core schema (enabled by default and readonly).
Enterprise Schema	On / Off	The SCIM Enterprise User Schema Extension defines attributes commonly used in representing users that belong to, or act on behalf of, a business or enterprise. Available for SCIM Endpoints only.
Fastpath Schema	On / Off	It defines attributes for Fastpath Lifecycle fields not already covered by SCIM core or enterprise schema and for Fastpath Lifecycle Custom Fields. Available for SCIM Endpoints only.
Fastpath Custom Schema	On / Off	Whether to include Fastpath Schema in the output. (It is always accepted as input, if present). Available for SCIM Endpoints only.
unicodePwd	On / Off	Fastpath Lifecycle can encode passwords in Unicode-16 format before sending them through SCIM. You should not enable this option for any system other than Microsoft Active Directory. Available for SCIM Endpoints only.
Millisecond precision	On / Off	If checked, datetime values will be sent with millisecond precision. Available for SCIM Endpoints only.
Enable SCIM Roles attribute	On / Off	When checked the SCIM Roles attribute is populated and returned with user API responses.
Force birthright resources	On / Off	When checked this will force birthright resources to be always granted even though they may be configured on the Category to be optional (on) and not included as Groups in the API user request. This means that you can pass Identity information via the User API and let Fastpath Lifecycle decide whether to grant the resource initially in a similar way to form defaults when adding an Identity via the UI.
Send a work email	On / Off	This option ensures an email of type "work" is sent to the endpoint even if one is not available for a given Identity. An attempt will be made to mark the first email of type "other" as "work" and if one is not found, an email of type "home" will be sent as "work". Leave unchecked for normal use.

5.2.1.2 Transformations

If you have enabled Lua scripting in your Application settings, you can create provisioning transformations. Select a field to transform and then pick a Lua Script to run. The result of the Lua script will be applied to the field before it is mapped to the SCIM Schema and then sent to the remote endpoint.

It's important to note that any field transformations here affect only the data sent to the endpoint and will not affect any data retained in Fastpath Lifecycle.

5.2.1.3 Field/Attribute Mapping

You can make adjustments to the field/attribute mapping that Fastpath Lifecycle uses for a SCIM connection by adding mappings here. Select a field to map and then select the SCIM attribute that should receive its value.

5.2.1.4 Provision

Normally, Identities will be provisioned to the Endpoint automatically as necessary, but there may be times when you wish to force this process manually. For example after a network failure. You can use the button on this form to create a new provisioning task for this Endpoint Connection.

5.2.1.5 Apply Compliance Policy

Compliance policies are usually applied automatically according to the frequency you have configured on the policy itself. If you've applied a Compliance Policy to this Endpoint Connection you can force a manual application of the Compliance Policy with this form.

5.2.1.6 Import Identities

This will start a one-off task to import Identities from the remote Endpoint and begin managing them locally. Local Fastpath Lifecycle Identities will be created for any remote Users that do not have a matching Identity locally.

Note: Where the ID is identical local and remote the Identity will not be imported, all other Identities will be imported. Be careful when you have existing Identity data in Fastpath Lifecycle as this feature can very easily lead to duplicates.

5.2.1.7 Import Resources

This will start a one-off task to import Resources from the remote Endpoint and begin managing them locally. Local Fastpath Lifecycle Resources will be created for any remote Groups that do not have a matching Resource locally.

5.3 Fastpath Connect status

If Fastpath Connect is configured, details about its status will be available for viewing under **Integration » Fastpath Connect status** menu option. Fastpath Connect will make regular requests to Fastpath Lifecycle in order to provide information about its status including its ID, version, uptime information as well as its listeners, provisioners, and configuration. The majority of the information is displayed in JSON format. A history of previous status updates is also available, and the number of items to keep in history can be configured by going to **System » Settings » Application** and updating the "Fastpath Connect status history amount".

5.4 Staging

Staging is an interface to connect to your Identity Management System through a set of database tables using a published schema.

By configuring your Identity Management Connector or Driver to read and write data to the Fastpath Staging Schema, as per the documentation below, you can have Identities published to your IDM System when they are made active. Your IDM system can also return information back to Fastpath Lifecycle, for example an email address for a mailbox created by your IDM system.

Fastpath Lifecycle is able to provide connectors/drivers for many Systems, ask your account manager for more details.

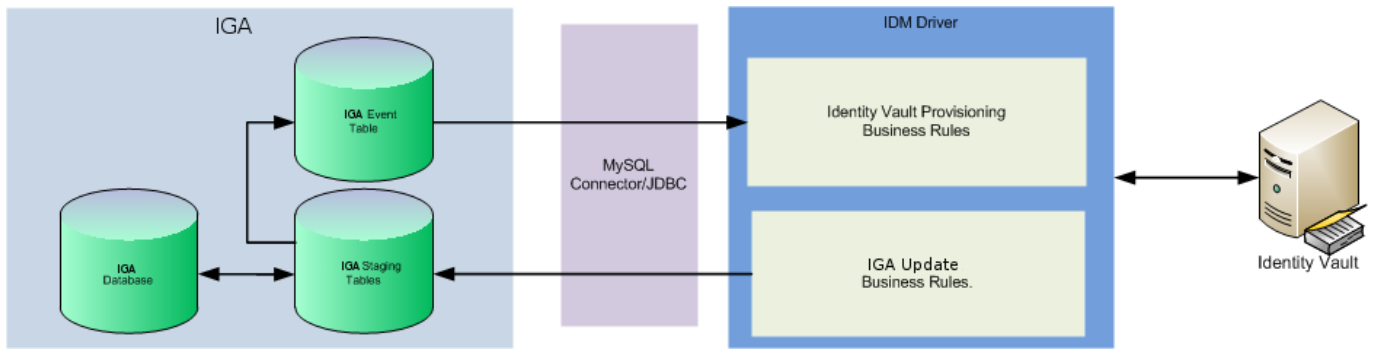


Figure 5.1: Connecting Fastpath Lifecycle to NetIQ IDM

5.4.1 Fastpath Staging Schema

When the status of an Identity changes to Active, the Fastpath Lifecycle Identity will be staged to make it available to the Identity Management System (IDM). A number of database tables are made available to the Identity Management System so that it can read this data. It is also possible for the Identity Management System to return information to Fastpath Lifecycle by updating these tables.

Your Identity Management Connector or Driver should connect to the MySQL database (typically running on the same host as Fastpath Lifecycle) with the database user 'idm' which was created by the Fastpath Lifecycle setup script. This database user has appropriate permissions for working with the Fastpath Lifecycle staging schema without compromising the integrity of the Fastpath Lifecycle database. It is important not to use the 'iga' database user for your IDM connector or driver so that Fastpath Lifecycle can distinguish where any changes to the staging data are coming from.

5.4.1.1 Encoding

All characters within Fastpath Lifecycle and the Fastpath Lifecycle database will be handled with UTF-8 encoding, up to 4 bytes per character. Therefore, any data imported staging, via CSV, via the REST API or from any other external systems has to be provided in UTF-8 encoded format too.

5.4.2 Database Table: staging

This table stores the main details about Identities.

Table 5.2: Database Table 'staging'

Column	Type	Description	Sync Direction
tid	varchar(36)	Tenancy ID	Fastpath ↔ IDM ¹
iga_id	varchar(36)	RFC 4122 compliant GUID	Fastpath ↔ IDM ²
courtesytitle	varchar(20)	Courtesy Title/Honorific title (e.g., "Mr")	Fastpath ↔ IDM
givenname	varchar(255)	Given name / First name	Fastpath ↔ IDM
middleinitial	varchar(255)	Middle Initial	Fastpath ↔ IDM
surname	varchar(255)	Surname / Family name	Fastpath ↔ IDM
fullname	varchar(255)	Full name	Fastpath ↔ IDM
preferredname	varchar(255)	Preferred name	Fastpath ↔ IDM
previousname	varchar(255)	Previous name	Fastpath ↔ IDM
honsuffix	varchar(255)	Honorary suffix	Fastpath ↔ IDM
dob	date	Date of birth	Fastpath ↔ IDM
qualifications	varchar(255)	Qualifications	Fastpath ↔ IDM
organisation	varchar(255)	Organisation name	Fastpath ↔ IDM
managerid	varchar(36)	Manager GUID	Fastpath ↔ IDM
jobtitle	varchar(255)	Job title	Fastpath ↔ IDM
orgunit	varchar(255)	Organisational Unit	Fastpath ↔ IDM ³
orgunitref	varchar(255)	Organisational Unit ref	Fastpath → IDM ⁴

Column	Type	Description	Sync Direction
orgunitid	varchar(255)	Organisational Unit GUID	Fastpath → IDM ⁵
site	varchar(255)	Reserved for future use	Fastpath ↔ IDM
gender	char(1)	Gender	Fastpath ↔ IDM
password	varchar(255)	Initial account password	Fastpath ↔ IDM
password_protection	varchar(255)	Password protection method	Fastpath ↔ IDM
password_modified	datetime	Date password was last changed	Fastpath ↔ IDM
password_expired	datetime	Date password expired	Fastpath ↔ IDM
credential_policy	varchar(40)	Fastpath Credential Policy	Fastpath ↔ IDM ⁶
uniqueid	varchar(255)	Unique ID / Username	Fastpath ↔ IDM
previousid	varchar(255)	Previous unique ID / Username	Fastpath ↔ IDM
status	int(11)	Identity Status Code	Fastpath ↔ IDM
reqtime	datetime	Date & Time of request	Fastpath ↔ IDM ⁷
asstext	text	Additional Information	Fastpath ↔ IDM
sponsor	varchar(255)	DN of Sponsor	Fastpath ↔ IDM
approver	varchar(255)	GUID of Approve	Fastpath ↔ IDM ⁸
createdby	varchar(255)	Created By	Fastpath ↔ IDM
rejectreason	varchar(255)	Reject reason	Fastpath ↔ IDM
startdate	date	Start Date	Fastpath ↔ IDM
termdate	date	End Date	Fastpath ↔ IDM
category	varchar(255)	Fastpath Category	Fastpath ↔ IDM ⁹
categoryid	varchar(255)	Fastpath Category ID	Fastpath → IDM ¹⁰
photo	longblob	JPEG Photo (Binary data)	Fastpath ↔ IDM
nickname	varchar(255)	A nickname, pseudonym	Fastpath ↔ IDM
profileurl	varchar(255)	Profile URL	Fastpath ↔ IDM
preferred_language	varchar(255)	IETF Language tag	Fastpath ↔ IDM
timezone	varchar(255)	Time zone	Fastpath ↔ IDM ¹¹

5.4.2.1 Database Table: affiliatecustomfields

This table is responsible for storing any Custom Fields used in Identity data entry. If the value field exists and is of type longtext or longblob then its contents will mirror textvalue or binaryvalue respectively. If the Custom Field value is not printable then the textvalue field will contain a BASE64 encoded version.

¹Tenancy ID must be set to 'Default' unless you are running a multi-tenant installation in which case it must always be set to the correct tenancy ID on create and then never changed. You should never attempt to move an Identity from one tenancy to another.

²iga_id is an RFC 4122 compliant UUID/GUID that uniquely identifies the Identity. This column will sync in either direction, but the inbound sync (Fastpath ← IDM) will only occur for newly created Identities. i.e., Records created first by IDM will sync to Fastpath Lifecycle and include data from these fields. You should avoid any subsequent changes to these fields in staging, as changes may be overwritten by Fastpath Lifecycle or may cause a sync problem. To be clear, these fields will only sync in an outbound direction (Fastpath → IDM) after an Identity has synchronised once.

³If the Organisational Unit is set or changed by IDM, Fastpath Lifecycle will attempt to look up the Organisation Unit and set the ID based on the name from the staging.orgunit column. Sync will fail if the OU is not recognised.

⁴Fastpath Lifecycle will set the orgunitref based on OU matched using the orgunit column.

⁵Fastpath Lifecycle will set the orgunitid based on OU matched using the orgunit column.

⁶If a Credential Policy is set on the Category then that will be used and this column will be ignored for inbound sync.

⁷If reqtime is not set by IDM during creation of the Identity, Fastpath Lifecycle will set it to the current date/time.

⁸Fastpath Lifecycle will accept a DN here, if set by IDM, Fastpath Lifecycle will attempt to look up the Approver and set a GUID here.

⁹If the Category is set or changed by IDM, Fastpath Lifecycle will attempt to look up the Category and set the ID based on the name from the staging.category column. Sync will fail if the Category is not recognised.

¹⁰Fastpath Lifecycle will set the categoryid based on Category matched using the category column.

¹¹Time zone is assumed to be in TZ Database format. e.g., Europe/London or America/New York.

IDM may update any of the value fields. The other field(s) will be updated on the next cron execution.

Column	Type	Description	Sync Direction
userid	varchar(36)	Link to the staging table iga_id column.	Fastpath ↔ IDM
customfieldname	varchar(255)	Custom Field name	Fastpath ↔ IDM
datatype	varchar(255)	Fastpath data type	Fastpath ↔ IDM
value	varies	Custom Field value	Fastpath ↔ IDM
textvalue	longtext	Custom Field value	Fastpath ↔ IDM
binaryvalue	longblob	Custom Field value	Fastpath ↔ IDM

5.4.3 Database Table: resources

This table is responsible for storing Resources.

Column	Type	Description	Sync Direction
id	varchar(36)	Unique ID for this Resource	Fastpath → IDM
name	varchar(255)	A name	Fastpath → IDM
description	varchar(255)	A human readable description.	Fastpath → IDM

5.4.4 Database Table: affiliateresources

This table links the Resources table to the staging table.

Column	Type	Description	Sync Direction
userid	varchar(36)	Links to the staging table iga_id column.	Fastpath ↔ IDM
resourceid	varchar(36)	Links to the Resources table id column.	Fastpath ↔ IDM
status	int(11)	Resource status 0 = off, 1 = on	Fastpath ↔ IDM

5.4.5 Database Table: event

This table stores a log of staging events. Fastpath Lifecycle uses MySQL triggers to populate this table automatically as records are changed or added in the staging tables.

Column	Type	Description	Data Source
record_id	int(11)	Record ID	Fastpath or IDM
table_key	varchar(64)	Table Key	Fastpath or IDM
status	char(1)	Event Status	Fastpath or IDM

Column	Type	Description	Data Source
event_type	tinyint(4)	Event Type	Fastpath or IDM
event_time	datetime	Event Date/Time	Fastpath or IDM
perpetrator	varchar(64)	Perpetrator	Fastpath or IDM
table_name	varchar(64)	Table Name	Fastpath or IDM
column_name	varchar(64)	Column Name	Fastpath or IDM
old_value	varchar(64)	Old Value	Fastpath or IDM
new_value	varchar(64)	New Value	Fastpath or IDM

The status column indicates the state of a given row.

Status	Interpretation
N	New
S	Success
W	Warning
E	Error
F	Fatal

The Perpetrator column identifies the database user who instigated the event.

The Event Type column is an integer that describes the type of event that has occurred.

Event Type	Interpretation
1	Insert field
2	Update field
3	Update field (remove all values)
4	Delete row
5	Insert row (query-back)
6	Update row (query-back)
7	Insert field (query-back)
8	Update field (query-back)

5.4.6 MySQL Data Types Explained

These are the MySQL data types used in the staging tables with an explanation of each.

Data type	Explanation
char	Fixed length text strings.
varchar	Variable length text strings.
text	Large variable length text strings.
int, smallint	Integer numeric values.
datetime	Date and time values. YYYY-MM-DD HH:MM:SS
date	Date values. YYYY-MM-DD

Data type	Explanation
longblob	Large binary data.
longtext	Large text data.

5.5 Fastpath Lifecycle API

Fastpath Lifecycle has a RESTful API based on SCIM (System for Cross-Domain Identity Management) version 1.1,¹² which helps integrate Fastpath Lifecycle with other applications or cloud based services.

The API uses JSON as a data format, and the schema used is as per the SCIM core schema¹³. The SCIM Enterprise User Schema Extension is also used. While the SCIM core and Enterprise User schema provide a fixed set of default attributes for the user object, Fastpath Lifecycle has its own Schema Extension which defines attributes that Fastpath Lifecycle supports that are not covered in either SCIM Schema.

The API requires `mod_rewrite` to be loaded within Apache to function.

The API requires HTTP Basic authentication using a local Fastpath Lifecycle Administrative User, which must be created in advance. The User should be a member of the 'API' Group. See the section on Local Administrative Users.

The REST API can support a tenancy ID in the URL and although multiple tenancy is not enabled by default, it can be enabled via **System » Settings » API**.

Important: When API Multitenancy is enabled, the Endpoint URLs require the Tenancy ID to be specified in the path after the API version, see the examples below.

Please visit Fastpath Lifecycle using `/scim/v1` in your browser and expand the Documentation section for more details such as API documentation and the available REST Resources.

Further information about using a SCIM API can be found online at <https://web.archive.org/web/20230219102236/http://www.simplecloud.info/specs/draft-scim-api-01.html>.

5.5.1 Field/Schema attribute mappings

The following tables list the schemas and attributes that Fastpath Lifecycle supports and stores, and the fields used to store the data.

The SCIM Specification has more details about these Schemas and their attributes.

5.5.1.1 urn:scim:schemas:core:1.0

Table 5.10: API attribute mapping for SCIM Core Schema.

Fastpath Field	API Attribute
iga_id	id
uniqueid	userName
fullname	name.formatted
surname	name.familyName
givenname	name.givenName
middleinitial	name.middleName (initial character only)
courtesytitle	name.honorificPrefix
honsuffix	name.HonorificSuffix
nickname	nickName
profileurl	profileUrl
emails	emails (email.value, email.type, email.primary)
phone	phoneNumbers (phoneNumber.value, phoneNumber.type, phoneNumber.primary)

¹²<https://web.archive.org/web/20230219102236/http://www.simplecloud.info/specs/draft-scim-api-01.html>

¹³<https://web.archive.org/web/20230219102236/http://www.simplecloud.info/specs/draft-scim-core-schema-01.html>

Fastpath Field	API Attribute
address (value)	addresses.address.streetAddress
address (town)	addresses.address.locality
address (region)	addresses.address.region
address (postcode)	addresses.address.postalCode
address (country)	addresses.address.country
address (type)	addresses.address.type
address (primary)	addresses.address.primary
category	userType
jobtitle	title
preferredlanguage	preferredLanguage
locale	locale
timezone	timezone
active	(True when status is Active)
password	password
roles	roles
entitlements	entitlements

5.5.1.2 urn:scim:schemas:extension:enterprise:1.0

Table 5.11: API attribute mapping for SCIM Enterprise Schema.

Fastpath Field	API Attribute
organisation	organization
orgunit	department
employeenumber	employeeNumber
manager	manager.managerId

5.5.1.3 urn:scim:schemas:com_ideiiio:1.0

Table 5.12: API attribute mapping for Fastpath Schema.

Fastpath Field	API Attribute
credentialpolicy	credential_policy.id, credential_policy.name
preferredname	preferredname
previousname	previousname
previousid	previousid
dob	dob
qualifications	qualifications
site	site
gender	gender
status	status
orgunitref	orgunitref
countryname	country
asstext	asstext
rejectreason	rejectreason
lastlogin	lastlogin
startdate	startdate
termdate	termdate
openEnded	openended
sponsor	sponsor.dn
approver	approver.id
createdby	createdby.dn
category	category.id

Fastpath Field	API Attribute
password	password.original, password.protection, password.plaintext, password.modified, password_expired_at
authentication_source	authentication_source
authentication_dn	authentication_dn

5.5.1.4 urn:scim:schemas:com_ideiio_custom:1.0

Table 5.13: API attribute mapping for Fastpath Custom Field Schema

Fastpath Field	API Attribute
custom_field_name	custom_field_name

Please also visit Fastpath Lifecycle using **/api/v1/Schemas** to view all available Endpoints, Methods, and Schemas.

5.5.2 API Configuration.

Navigate to **Integration » API**.

Multiple API Configurations are allowed for compatibility with other applications. The 'default' configuration is the one used when a custom API path is not used, and it is also the configuration used for SCIM provisioning.

To access an API with a custom configuration insert the ID before the method in the URL, like this:

<https://example.com/ideiio/api/5B1C14CB-D92D-4A12-B83E-358E1D8F089F/users/>

5.6 OAuth Clients

OAuth Clients provide configuration for Identities to authenticate and access to identity information using their Fastpath Lifecycle credentials.

For each client to perform OAuth requests, a client needs to be created. Fastpath Lifecycle creates JWT formatted access tokens.

A JWKS endpoint is provided at /jwks to list the keys used to validate the JWT.

Authentication is normally performed locally, and a login form is displayed; SAML will be used instead if it is configured and enabled. You can set a query parameter of 'acr_values' to 'idp:local' to override this behavior and login locally, but only if the SAML Login Recovery setting `idv_saml_recovery_login` has been enabled.

Setting	Purpose
Client ID	The name of the Client, effectively the username.
Client Secret	The secret of the Client, effectively the password.
Redirect URL	Where to redirect Identities after successful logins.
Accepted Grant Types	The grant types that this Client accepts.
Allowed scopes	The scopes that will be valid for this client.
Access Token Algorithm	The algorithm that will be used to sign the JWT access token, RS256 uses asymmetric encryption using public private keys, HS* use symmetric encryption using the Client secret.
Access Token Lifetime	How many seconds the access token is valid for.
(Re)create Keys?	Should the public/private keys be recreated and the old ones deactivated.

5.7 Fastpath Self Service Configuration

Fastpath Self Service is a separate application from Fastpath Lifecycle (not to be confused with self-service forms Lifecycle feature). Fastpath Self Service can be used by Identities to manage their access to Roles and Applications as well as update their personal details. Fastpath Self Service requires an OAuth connection to Fastpath Lifecycle in order to authenticate Identities as well as an API connection in order to exchange information. To find out more how to set up an OAuth Client please go to the [OAuth Clients](#) section and to set up an API User for Fastpath Self Service please visit the [Administrative Users](#) section as well as the [Fastpath Lifecycle API](#) section.

Setting	Purpose
Client ID	The name of the API username, effectively the username.
API Key	The API User's password.
Access URL	The URL where the API can be accessed. (e.g., https://my-server.example.com/ideiio/api).
Verify Certificate	When enabled, Fastpath Self Service will verify the certificate's authenticity.
Client ID	The OAuth Client ID as added in Fastpath Lifecycle.
Client Secret	The OAuth Client secret, effectively the password.
Endpoint URL	The URL that Fastpath Self Service has to access to authenticate Identities.
Token URL	The URL that Fastpath Self Service will use to validate access tokens, after Identities have authenticated.
API key	A local path or a URL where the OAuth public key can be found. If a local file path is provided, the public key's content must be found in that particular file.
Verify Certificate ID attribute	Denote whether to verify the OAuth issuer's certificate. Optional attribute for Fastpath Self Service to look at when requiring an Identity's ID.
Logout redirect URL	Fastpath Self Service can redirect to a particular URL when Identities choose to log out. Please provide it here.

5.7.1 Applications and Roles in Fastpath Self Service

Please note that any Application or Role that the Identity already has access to will not be available to request via Fastpath Self Service.

Only the Applications and Roles that are related to the Identity's Category will show in the portal as available to request or add.

5.7.1.1 Roles

In order for Roles to be requestable/addable in Fastpath Self Service, please ensure that the Role is related to the Identity's Category. After doing so, also ensure that it has either of the two options available/set on the Role:

- Can be added - will make the Role available to Add by the Identity directly.
- Owner - if the Role is not addable, this denotes the Admin that will approve the requests made for this Role.

In order to add Roles and configure them for Fastpath Self Service, please go to the [Setting up Roles](#) section.

5.7.1.2 Applications

Applications offer more options in order to be made available to be requested via Fastpath Self Service. Besides being addable or having an owner, Applications also have to be added in a Catalogue which in return must be related with the same Category as the Identity. Optional Labels can be added in order to group Applications. Any Applications that do not have a label will show up as "Uncategorised".

Please visit the [Setting up Resources](#) section in order to find out more and add Applications for Fastpath Self Service.

Chapter 6

Managing Identities

6.1 Adding / Requesting an Identity

Any user with appropriate Privilege can add an Identity by choosing **Identities » Add** from the menu. If the User has a Role of Sponsor the record will be created with a status of 'Sponsor Request' to indicate that it is a request.

The Add Identity form requires that you select a Category, this will determine the Resources that are available to the Identity (you may be able to configure these further, depending on the Category settings) as well as other defaults like maximum duration, Organisational Unit, and Credential Policy.

The fields that are shown on the Add / Request Identity form are controlled by your particular Field settings and may vary depending on the Category that you select at the top of the form.

Certain Fields are always displayed, these are described below.

Field	Possible Values	Purpose
Category	Existing Category	To set the Category of an Identity we are adding. The rest of the form is dynamically adjusted to request information appropriate for the Category chosen.
Sponsor	Sponsor DN	This field is pre-populated with the DN of the current User but can be set to any User inside the Search Base for Sponsors from the authentication directory if desired.
Organisational Unit	Organisational Unit	To associate the Identity with a particular Organisational Unit.
Maximum Duration	Number of days	The maximum number of days that the Identity can be active. It will not be possible to extend the duration past this.
Start Date	Date	The date at which the Identity will be made Active.
Duration	Number of days	The number of days that the record should remain Active.
End Date	Date	The date after which the Identity should be automatically disabled.
No End Date	On / Off	Denote if the Identity requires an end date (i.e., does not expire), if the Category allows it (i.e., maximum duration is set to infinite).

After adding an Identity, it is made active straight away (if the start date is today or in the past), or it is held with a status of 'Awaiting start date' and made Active automatically once that date is reached. The latter is dependent on changing the "Start Date Event" setting to "Set status" under **System »**

6.2 Invite external people

Invitations provide an easy way of inviting external people to become Identities with the use of their email address alone. Unlike Requests, Invitations are pre-approved accounts that will not require manual approval as these will inherit the details which have been provided during the invitation process.

To begin inviting external people, please select **Identities » Invite** from the menu. Please complete the form fields with details that will apply to all the Identities that will be invited in this operation. The Invitations will be sent to the provided email addresses, and they will each contain a unique link. The link will provide access to a form in order for the invitation to be completed by providing extra details such as name, date of birth, etc.

The email addresses can be provided using the email inputs on the Invite form or by uploading a CSV file that contains one column, with email addresses. These can be provided separately or concomitantly but at least one is required in order to send the invitation.

To create more input fields and add more than one email to invite, please select the number of required fields using the drop-down menu located below the email input and then click 'Add more'. This action can be repeated until a satisfactory number of email inputs is reached.

Regarding CSV files, please take the following as an example:

```
Email
john@example.com
doe@example.co.uk
jane@example.net
```

Setting	Possible Values	Purpose
Category	Category	To select the Category to apply to this batch of invitation Identities.
Organisational unit name	Organisational Unit	To select the Organisational Unit.
Credential Policy ¹	Credential Policy	To select Username and Password generation rules.
Sponsor	Sponsor DN	This field is pre-populated with the DN of the current User but can be set to any User inside the Search Base for Sponsors from the authentication directory if desired.
Start Date	Date	The date at which the Identity will be made Active, after accepting the invitation.
End Date	Date	The date after which the Fastpath Lifecycle Identity should be automatically disabled.
Roles	Existing Category Roles	Add Roles that will be added to the Identities once they accept the invitation.
Resources	On / Off	To review the Resources that are to be provided to these Identities.
Email	Email address	One or more email addresses that will inherit these affiliation settings and will receive the Invitation.
File	CSV File	Upload a list of email addresses to send Invitations to.

After the emails have been provided via a CSV file or simply entered in the email field, please use the invite button in order to send the Invitations. Please note that these will be processed as background

¹The Credential Policy field will be unavailable if the Credential Policy has already been fixed by the Category that you have chosen.

tasks and therefore, they will not be sent immediately. Please select **System » Tasks** from the menu in order to view the status and progress of the newly created task.

6.3 Importing Identities

The import facility allows bulk import of a number of Identities from a CSV (Comma-separated values) text file. The file should be organised with one record per row. You can choose which columns in the file to import and which Fastpath Lifecycle fields they will match to, after uploading the file. In addition, the import form allows you to configure some defaults which will apply to all the rows.

The columns of data in the file to be imported can be provided in any order.

Hint: You can improve the auto-matching of columns to fields by including field names as the first row of your CSV file (i.e., headers) - see the 'First line contains headers' setting below.

For example, the file might look like this:

```
Given Name,Surname>Password,Email,Organisational Unit
Alan,Dellon,NewPass09,adellon@example.com,Law School
Brian,Smith,Pass12345,bsmith@example.com,Biological & Biomedical Sciences
Daniel,Brown,Secr3t,brownd@example.net,Finance Department
Janet,Jones,Passw0rd,janetj@example.com,School of Applied Sciences
```

In this example we import passwords, but you can just as easily leave it to your Credential Policy to generate new passwords.

CSV files can be created by exporting data from a spreadsheet application (for example Microsoft Excel or LibreOffice Calc).

Hint: To create a CSV file from Microsoft Excel select **File » Save As » Other Formats** and choose CSV (Comma Delimited).

All the Identities that are imported in a single operation must be of the same Category and Credential Policy.

To import a CSV file of Identities select **Identities » Import** from the menu. The import process will first prompt you to enter a few details that will apply to all the Identities that you import in this operation.

Setting	Possible Values	Purpose
File	CSV File	To select the plain text CSV file to import.
First line contains headers	On / Off	Specifies if the first line in the CSV file contains column headers rather than an Identity.
Category	Category	To select the Category to apply to this batch of imported Identities.
Organisational unit	Organisational Unit	To select the Organisational Unit to apply to this batch of imported Identities.
Credential Policy ²	Credential Policy	To select username and password generation rules.
Sponsor	Sponsor DN	This field is pre-populated with the DN of the current User but can be set to any User inside the Search Base for Sponsors from the authentication directory if desired.
Start Date	Date	The date at which the Identity will be made Active.
End Date	Date	The date after which the Fastpath Lifecycle Identity should be automatically disabled.
Roles	Roles list	Add Roles for the imported Identities.
Resources	On / Off	To review the Resources that are to be provided to these Identities.

After setting Import details and choosing a file click the **Upload** button.

You will now be presented with some sample data from the uploaded CSV file and prompted to set the field for each column of the CSV source. Fastpath Lifecycle will examine the data itself and try to guess the correct field for the values. However, please check carefully to make sure the mappings between fields and the uploaded data is correct.

Note: A maximum of one column can be imported into each field, so take care to set field mappings carefully so that each field is mapped only once to avoid unexpected results.

After confirming the data type mappings click the **Continue** button to begin the import. The import will be created as a 'Task'. Therefore, the Identities will be imported as a background process. To view the status and follow the progress of the import batch task, navigate to **System » Tasks** from the menu.

Each Identity created by the import process will receive an email to their home email address using the accountandpass template.

Note: The order in which Identities are imported from the CSV file will not be the order that these are in the source file. Fastpath Lifecycle processes the rows in an unpredictable order, and the import may be processed over several executions of the cron script, depending on the size of the import file and the performance of the server.

Furthermore, Identities can also be imported from an endpoint. Please visit [Setting up Provisioning Endpoint Connections](#). After setting up an endpoint, when viewing it, choose **Import Identities** from the left-hand side menu. Please note that Fastpath Lifecycle will attempt to match imported Identities with local Identities and new ones will be created if no match is found. This action should only be performed once.

6.4 Finding Identities

To find and manage Identities, choose **Identities » Manage** from the menu.

The manage Identities page, by default, shows all Identities the logged-in user has permission to view, in a tabular format with one record being shown per row. Typically, this will include the Identities they are set to be the Sponsor of and all Identities in a Category or Organisational Unit that specifies a view or approval Group where the User is a member. Users in the Fastpath Lifecycle Administrators Group can see all Identities.

The list of Identities can be sorted by any visible column (excluding the checkbox and actions columns since they do not contain data) by clicking the column header. The columns visible here are dependent on the [field settings](#). The checkbox and actions columns are always visible regardless of the field settings. The number of returned records may exceed the number of displayable records (10 by default). In this situation, navigation arrows will be enabled at the bottom of the table in order to scroll through the results. Page numbers will also be displayed so that different pages can be accessed directly. To change the number of rows visible per page, please use the dropdown menu located in the bottom right-hand corner of the table.

6.4.1 Identity actions

The details for an individual record can be shown by clicking the **View** link which will then provide the ability to manipulate these based on the permissions of the logged-in user. Alternatively, the checkbox on each row allows the Identity to be selected for use in a bulk action. Below the table are buttons for performing a specific bulk action on the selected records. These buttons are only available if the logged-in User has permission to perform that particular action on all the selected Identities.

6.4.2 Quick filters

Above the list of Identities are a few quick filter links. Each quick filter link shows the number of matching records. Selecting one of the quick filters will show only those matching records.

²The Credential Policy field will be unavailable if the Credential Policy has already been fixed by the Category that you have chosen.

6.4.3 Export to CSV

The current list of records can be exported as a CSV (Comma-separated values) file suitable for importing into a Spreadsheet application or Database by selecting the **Export** link shown below the list and then choosing which columns the CSV file will contain. The encoding of the file is UTF-8.

6.5 Requests

Requests are Identities that have either submitted an application online via a Self Service Form or have been added by a Sponsor.

6.5.1 Listing

To list requests select **Identities » Manage** from the menu and select the 'Requests' quick filter. Note that the quick filter is only displayed if there are records with a status that requires approval.

For Fastpath Lifecycle users not in the Fastpath Lifecycle Administrators Group, this list is limited to Identities the user has sponsored, that are requesting to join an Organisational Unit that the user is an Approver for, or in a Category that the User is an Approver for.

Click **View** next to an Identity to view details of the Request and to perform actions on a single Identity or use the checkbox to select multiple records and use one of the batch action buttons (**Approve** or **Decline**) below the listing to apply an action to multiple records in a single operation.

6.5.2 Edit

To edit a request use the **Edit** button. Identity details can be updated from this page, including the 'Additional Information' field.

6.5.3 Reassign

To reassign a Self Service Request to another Organisational Unit, select an Organisational Unit from the 'Reassign' section and then click the **Reassign** button.

6.5.4 Approve

To approve a Request, use the 'Approve' section to specify Category, Credential Policy, Start Date, End Date, Sponsor and Organisational Unit (for sponsor requests). Configure any Resource and Role assignments as appropriate and then click the **Approve** button. This changes the status of the Identity to 'Active' and sends email notifications.

6.5.5 Decline

To decline a Request, use the **Decline** button. This changes the status of the Identity to 'Declined request' and sends an email (Template: rejected) to the Identity to let them know the Request has not been approved. If this is a Sponsor Request, an email is also sent to the Sponsor (Template: sponsorrejected).

6.5.6 Self Service Requests

Self Service Forms allow configuration of multiple Forms, each with its unique link. The Forms can be configured to be accessible by existing Identities only, and the Form Fields available per Form can also be configured. Furthermore, titles, descriptions, and logos can be added for each Form.

When Self Service Forms exist, it is possible for anybody with access to a web browser, in possession of the Form URL and internet, to request access via an easy to use web form which was previously configured. The Self Service pages require a home email address so that emails can be sent to the requester about the status of their Request.

After creating a Self Service Form, please visit the Fastpath Self Service URL in your web browser to begin the registration process.

Example Fastpath Self Service url: <https://my-server.example.com/ideiio/selfservice/RegisterNew> where RegisterNew is the URL title which has been configured for this particular Self Service Form.

The first step of the registration process is to enter an email address, this is usually an email address which is external to the organisation (for example a personal webmail address). After clicking 'Next', please choose a new password, or in the case of an existing registration, enter the previously chosen password to update the Request.

The registration process will then request any information which has been configured for the Self Service Form being viewed (this may be altered by a Fastpath Lifecycle Administrator via Self Service Forms - see the section on [Setting up Self Service Forms](#)).

Default Self Service Fields:

Field	Notes
Email Address	Personal/home Email Address (Required)
Password	Must include both upper and lower case letters plus a number (Required)

6.5.7 Identity Statuses

Every Identity is assigned a status according to its position within the life-cycle. This table lists each possible status along with the status code that is used when staging the Identity to the Identity Management System.

Status	Meaning	Code
Request	A completed Self Service Request.	-7
Awaiting Activation	Approved but not yet made automatically active.	-6
Possible Duplicate	There may be pre-existing Identities that match this one.	-5
Sponsor Request	A request made by a Sponsor.	-4
Declined Request	A request that has been declined.	-2
Awaiting start date	Approved but start date not yet reached.	-1
Active	Active Identity.	0
Disabled (manual)	Disabled by an Administrator.	1
Disabled (auto)	Disabled automatically (at the end of the day when the end date is reached).	2
Disabled (expired)	Disabled and Expired after passing end date and expiry period elapsed.	3
Resynchronising	Used by IDM.	4
Migrated	Fastpath is no longer authoritative for this Identity.	5
Deleted	Considered to mean deleted completely.	99

6.6 Active Identities

Active Identities are records that have been staged for IDM and can be renewed (if the renewal limits have not been reached and the user has permission to do so) or terminated.

6.6.1 Listing

To list active Identities select **Identities » Manage** from the menu and select the 'Active' quick filter.

For Fastpath Lifecycle Users not in the Fastpath Lifecycle Administrators Group, this list is limited to Identities the user has sponsored, associated with an Organisational Unit that the User is an Approver for, or in a Category that the user is an Approver for.

Click **View** next to an Identity to view their details and to perform actions on the record.

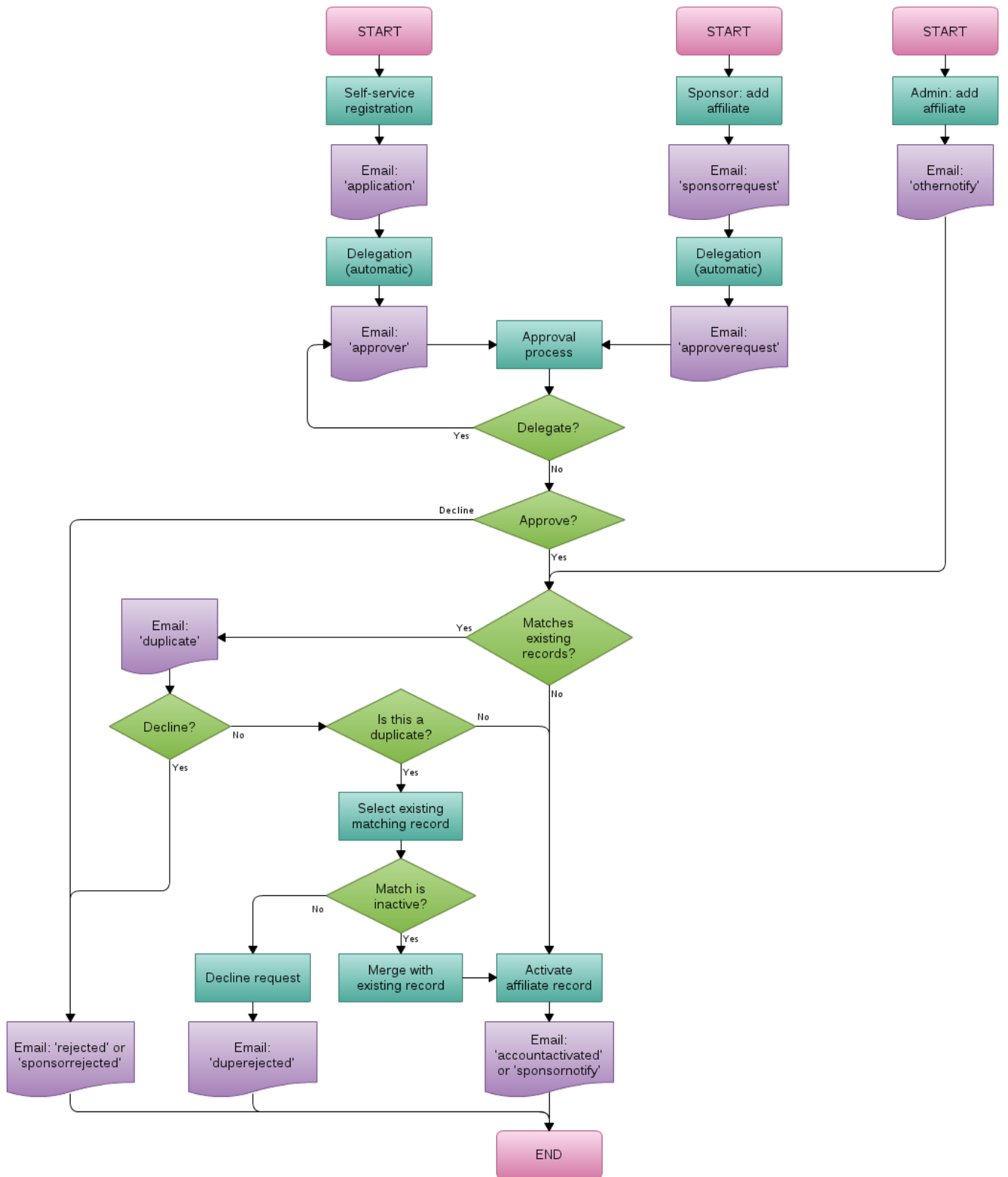


Figure 6.1: Add Identity / Request / Self Service Request Workflow

6.6.2 Additional access

If there are Applications (i.e., Resources) or Identity Roles which can be requested on behalf of this Identity or added, this panel will become available. This panel enables Administrative Users to request access to Roles or Applications that are made available via the Identity's Category. Please note that some Applications or Roles may require a reason to be provided in order to support the request and if that is the case, the reason field will show up underneath the respective Role or Application and the field will be marked with the red asterisk indicating it is required. After the form is submitted, any Roles or Applications that were 'addable' will be attached to the Identity immediately whilst the remainder will have to go through an Approval process by their corresponding owners.

6.6.3 Renewing

If the Identity can be renewed the 'Renew' section will become available on the 'View Identity' page. In the 'Renew' section, select the new end date and click the **Renew** button.

Note: The renewal form will not be available once the renewal limit has been reached.

6.6.4 Extend

Active Identities which are close to their expiration date may be extended using this panel. If this option is not used, a notification will be sent to the Identity's approver prior to their expiration date. The number of days before the end date when the notification is sent can be set on the Identity's Category by using the "Days before termination to notify" option.

6.6.5 Terminating

Select 'Terminate' to immediately disable the Identity. The termination will be applied to the Identity as well as potentially be provisioned to external systems via Provisioning depending on the Endpoints setting for any of the Identity's Resources which may be related to the Endpoints.

6.7 Inactive Identities

Inactive Identities are records that have been manually terminated, have been automatically disabled due to passing their end date or Requests that have been declined.

6.7.1 Listing

To list inactive Identities select **Identities » Manage** from the menu and select the 'Inactive' quick filter.

For Fastpath Lifecycle Users not in the Fastpath Lifecycle Administrators Group, this list is limited to Identities the user has sponsored, are associated with an Organisational Unit that the User is an Approver for or in a Category that the User is an Approver for.

Click **View** next to an Identity to view their details and to perform actions on the record.

6.7.2 Re-enabling

If the Identity has been terminated and can be re-enabled the 'Re-enable' option will become available on the 'View Identity' page.

Click the **Re-enable** button to change the status of the Identity to 'Active'.

6.8 Editing Identities

To edit a Request, use the **Edit** button on the 'View Identity' page. You can update details from this page including the 'Additional Information' field.

6.8.1 Identity Bulk Edit

Fastpath Lifecycle comes with Identity Bulk Edit feature where you can select multiple Identities and by clicking **Multi-select** you can edit their Fields at one time. When you click on **Multi-select** you will find the 'Edit' option on left with which you can edit the Fields of your choice by clicking the Field's respective edit checkbox. When you are viewing multiple Identities and editing the Fields which contain different data, it will show you a warning message that your previous data could be overwritten.

6.9 Effective Resources

Please note that on some Identity panels (e.g., view, edit, approve), a Field labelled **Effective Resources** may become available. This Field will show the final Resources inherited from the Category Resources, and the associated Identity Roles as well as Resources inherited from Additional Access Requests made via Fastpath Lifecycle or Fastpath Self Service. Each Resource will be labelled accordingly to denote its provenance.

As well as showing the names of the resources themselves, this feature will also display some additional related information. The source of an effective Resource will be displayed on the right. Icons with further information about Entitlements (double tick icon) and provisioning (cloud icon) are displayed beside the name; hovering the cursor over the icons will provide details or further actions. In the case of Entitlements, depending on the context, you may also be able to click the icon to set the Entitlements too. The Entitlements will be opened and allow choosing which of the available items are granted for this Identity. Some Entitlements may be disabled if they are inherited from other sources which prevents them from being disabled as they may be set as Role defaults or may have been requested from Fastpath Self Service or via the Additional access panel.

Note: When there is a Category Resource that is set to Mandatory Off on the Category but there is a Role attached to the Identity which contains that particular Resource, the Effective Resources will show the final outcome i.e., that Resource will be enabled as Roles Resources override Category Resources.