My1Login Ltd.

Enterprise Identity Management Solution

May 2018

Table of Contents

1 MY1LOGIN G-CLOUD SOLUTION OVERVIEW 4

2 SUMMARY OF PRODUCT SET 4

2.1 User Experience Options 5
2.2 User Portal: Viewing, Searching and Filtering Stored Passwords and Applications 5

3 PRODUCT SET 6

3.1 Single Sign-On for Web & Mobile 6
3.1.1 Overview of SSO for Web & Mobile 6
3.1.2 Web SSO 6
3.1.3 Web SSO - Domain Inclusion/Exclusion List 7
3.1.4 Web SSO - Automatic Detection and Automatic SSO Integration of Web Apps 7
3.1.5 Web SSO - Form Finder, Multi-Step Login Forms and Custom Credential Field Mapping 7
3.1.6 Mobile SSO 8
3.1.7 SSO Without Revealing Credentials for Web and Mobile Web Apps 8
3.1.8 SSO for Web and Mobile: Handling of Multiple Credentials for a Single Web Application 8
3.2 Single Sign-On for "Fat Client" Apps 9
3.2.1 Integrating "Fat Client" Applications that Do Not Have Connectors Available 9
3.2.2 "Fat Client" Applications: Linking Stored Credentials with Other "Fat Client" and Web Apps 9
3.2.3 "Fat Client" Applications: Automatically Integrating Users' Application Credentials 9
3.2.4 "Fat Client" Applications: Examples of Compatibility 9
3.2.5 "Fat Client" Applications: Handling of Multiple Credentials for a Single "Fat Client" Application 10
3.2.6 Handling of Custom Login Windows and Multi-Step "Fat Client" Login Processes 10
3.3 Privileged Password Manager 10
3.3.1 Overview of Privileged Password Manager 10
3.3.2 Issuing Privileged Passwords: Fine-grained Permissions 10
3.3.3 Privileged Password Manager - Temporal Access by Time and Date 11
3.3.4 Privileged Password Manager - Automatic Password Generation for Web Apps 11
3.3.5 Privileged Password Manager - Automatic Password Updates on Web Apps 11
3.3.6 Privileged Password Manager - Password Updates on Thick-client Apps 11
3.4 Multi-Factor Authentication (MFA) 12
3.4.1 Overview of Multi-Factor Authentication 12
3.4.2 MFA: Currently supported MFA Types 12
3.4.3 MFA: On-Boarding Users and Groups 12
3.4.4 MFA: Grace Period 12
3.5 Provisioning Engine 13
3.5.1 Overview 13
3.5.2 Organisational Provisioning 13
3.5.3 Just-in-Time Provisioning 14
3.5.4 Automated De-Provisioning 14
3.6 Self-Service Password Reset (SSPR) 14
3.6.1 Overview of AD SSPR 14
3.6.2 AD SSPR: Configuration 15
3.6.3 AD SSPR: Enrolment 15

4 SECURITY AND SETTINGS 15

4.1 'Shadow-IT' Alerts 15
4.2 Domain Inclusion/Exclusion Lists 16
4.3 IP Filtering Policies (Allow/Deny List) 16
4.4 Password Policy Enforcement for Target Apps 16

5 AUDIT AND REPORTING 17

5.1 System Audit 17
5.2 Application Usage Audit 17
5.3 Application Usage Summary 17

5.3.1 Syslog Integration *18*

6 OFF-PREMISE USERS - AD AND EXTERNAL (NON-AD USERS) **19**

7 OFF-PREMISE AD USERS **19**

8 EXTERNAL (NON-AD USERS) **20**

8.1 Adding Individual Non-AD Users 20
8.2 Bulk Adding Non-AD Users 20

9 BULK IMPORTING LOGIN CREDENTIALS **20**

9.1 Admin Bulk Import of Login Credentials 20
9.2 User Bulk Import of Login Credentials 20

10 SOLUTION ARCHITECTURE **21**

11 DIRECTORY INTEGRATION **21**

11.1 Directory Integration: User Synchronisation with My1Login 22
11.2 Directory Integration: User Authentication with My1Login 22
11.3 Directory Integration: AD Connector 22
11.4 AD Groups 22
11.5 Local Groups in My1Login 23
11.6 Multiple AD Domains / Large Scale AD Structures 23

12 CUSTOM BRANDING / MANAGED SERVICE PROVIDERS **23**

12.1 Custom Branding 23
12.2 Managed Service Providers 23

13 CUSTOMER IMPLEMENTATION OVERVIEW **24**

14 SERVICE MANAGEMENT **24**

14.1 Information Assurance 24
14.2 Data Back Up and Restoration 24
14.3 Service Constraints 24
14.4 On-boarding and Off-boarding 24
14.5 Financial Recompense 24
14.6 Pricing 25
14.7 Service Levels 25
14.8 Ordering and Invoicing 25
14.9 Scalability 25
14.10 Termination Process 25
14.11 Technical Requirements 25

15 SERVICE PLANS FOR SUBSCRIPTION **26**

16 TRAINING AND DEPLOYMENT SERVICES **27**

16.1.1 Training and Deployment Packages *27*

17 BASIC AND PREMIUM SUPPORT **29**

18 MANAGED SERVICES **29**

18.1.1 Professional Services *29*

1 My1Login G-Cloud Solution Overview

Founded in 2007 in the UK, My1Login is a UK leader in protecting against enterprise cyber security threats through its Identity and Access Management (IAM) solutions.

My1Login's IAM solution enables organisations to securely manage access to applications for both internal and external users. My1Login's IAM solution solves the problem of weak passwords and practices, enabling organisations to control user access and centralise identity through Single Sign-On. Its SSO integrates with all app types - web apps, mobile apps, flash apps, virtualised apps, and even legacy, thick-client apps and mainframes.

My1Login's IAM solution supports identity standards such as SAML. Additionally, My1Login can also integrate with target applications that don't have connectors (e.g. legacy, thick-client applications and mainframes), to offer a true Single Sign-On (SSO) experience for end-users. My1Login can also auto-discover the cloud applications being accessed by users, inform IT and enable policies to be set which will automatically integrate these apps with SSO. My1Login can also perform automatic password updates on target applications.

Critical applications can be protected by auto-generated, strong, unique passwords that can be hidden from users, eliminating phishing. My1Login's auto-detection of application usage further reduces the attack surface by removing the blindspots created by Shadow IT.

My1Login was named the Identity and Access Management Solution of the Year at the 2017 Computing Security Awards.

2 Summary of Product Set

My1Login's enterprise IAM product set comprises the following: -

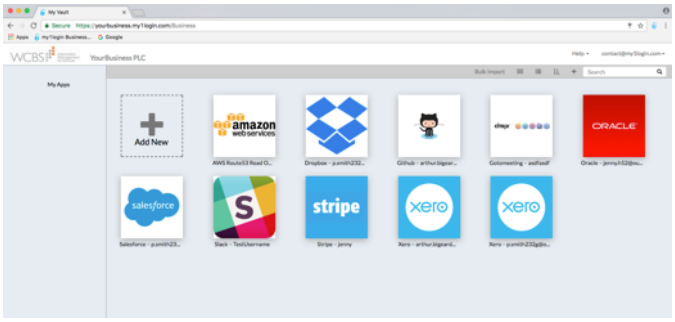
My1Login can dynamically detect the login structure of most web-pages meaning that even if the structure of the target application page changes the Single Sign-On process will still work. For sites that do not work with the automated 'form finder' functionality, exception scripts can be created centrally by My1Login and these will be detected and used by the browser plug-ins on specific domains.

My1Login can also perform credentials-based SSO for Flash-based login forms, basic-authentication login forms and Java login forms using password vaulting and forwarding. My1Login's browser plug-ins and desktop connector jointly perform this functionality.

2.1 User Experience Options

My1Login can be deployed to work in two ways for end users:

A/ Portal Access: The My1Login user portal and login page can be custom branded with the customer's business name and logo. The user portal displays a list of users' applications and, where required, credentials for these applications. **The user portal can be used to launch web and thick-client applications.**

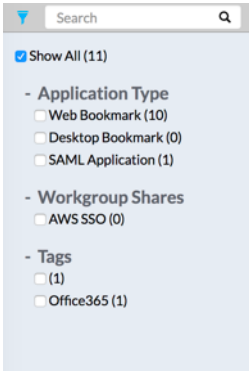


B/ Seamless Access: My1Login can be deployed to work in the background so the user does not have to log into a portal. The user simply launches the required **'fat-client' application or web application** and My1Login detects this, confirms if they have credentials available for that application and signs them in. **This provides seamless Single Sign-On to applications without having to access via a portal.**

Once set-up, users never have to access or log into My1Login – access is seamlessly linked to their AD profile.

2.2 User Portal: Viewing, Searching and Filtering Stored Passwords and Applications

Within the user portal, SAML applications and stored login credentials and passwords can be viewed as 'tiles' or as a list. These details can be further sorted, filtered and searched to make it more user friendly for users that have access to large numbers of passwords and applications.



3 Product Set

3.1 Single Sign-On for Web & Mobile

3.1.1 Overview of SSO for Web & Mobile

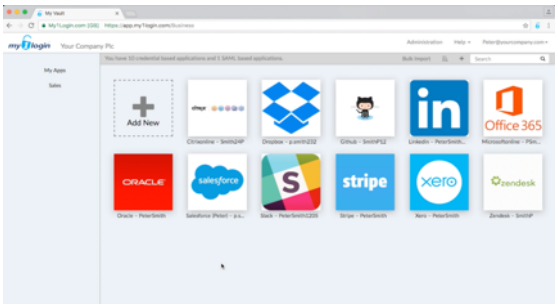
My1Login can dynamically detect the login form for most web-pages meaning that even if the structure of the target application page changes the Single Sign-On process will still work. For sites that do not work with the automated 'form finder' functionality, exception scripts can be created centrally by My1Login and these will be detected and used by the browser plug-ins on specific domains/apps. The 'form finder' works on web and mobile applications.

My1Login can also perform credentials-based SSO for Flash-based login forms, basic-authentication login forms and Java login forms. My1Login's browser plug-ins and desktop connector jointly perform this functionality. My1Login can also use both IdP and SP initiated SAML to authenticate users with apps.

In terms of mobile, My1Login supports SAML-based SSO for native apps and SSO for mobile web-apps via the My1Login app which users access with their AD credentials or a PIN Code once set-up.

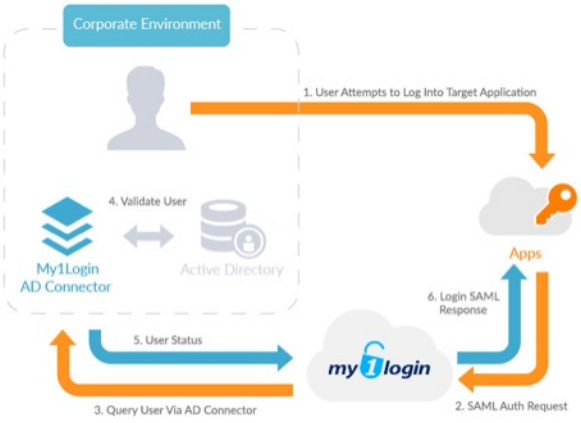
3.1.2 Web SSO

My1Login Single Sign-On for web applications works with either SAML or credentials-based applications. SAML applications can be configured to use My1Login as the IdP enabling My1Login to authenticate the user. My1Login can validate the user against the AD to log the user in seamlessly to the target application.



My1Login supports:

- IdP Initiated SAML Authentication
- SP Initiated SAML Authentication
- Credentials-based Authentication



The diagram on the left shows an example of an AD user undertaking SP initiated SSO i.e. a user within the corporate network, who is authenticated on the AD attempting to access a web application by visiting the URL.

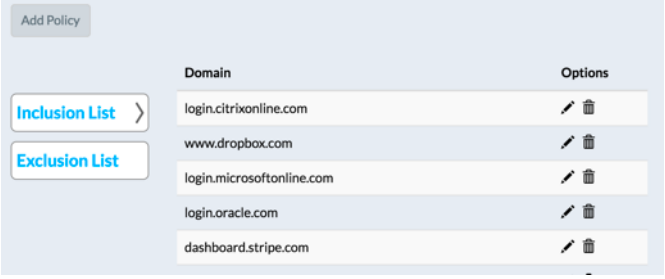
This is SP initiated, in that the user goes directly to the application. My1Login then authenticates the user at this point, checking that they are AD authenticated and are entitled to access that target application. IdP initiated SSO is initiated when the user clicks the application within their My1Login portal.

Diagram: On-Premise, Active Directory User, Service Provider-Initiated Login

3.1.3 Web SSO - Domain Inclusion/Exclusion List

Administrators can create policies that either include or exclude specific web applications (or domains) from being automatically integrated with My1Login's SSO.

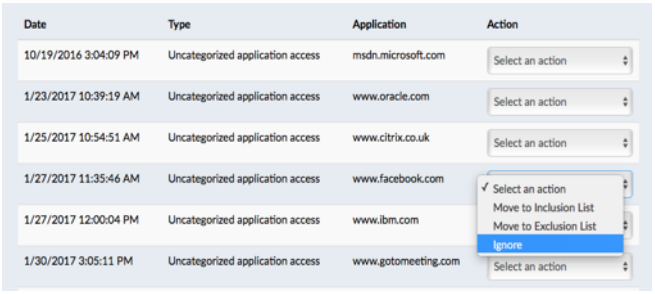
So, for instance, login.oracle.com could be added to the Inclusion List and this would set a policy to ensure that any users logging into login.oracle.com had their credentials automatically integrated with My1Login's SSO. This would mean the next time the user visited login.oracle.com they would be automatically signed in by My1Login's SSO.



Conversely, www.airbnb.co.uk could be added to the Exclusion List which would mean that any users logging into AirBnB would not have their credentials integrated with My1Login's Single Sign-On.

3.1.4 Web SSO - Automatic Detection and Automatic SSO Integration of Web Apps

My1Login can be configured to detect "Any Web App". Whilst this is activated, My1Login will detect the login forms of applications that users are logging in to. IT administrators will receive notifications of these applications and can then make a simple policy decision as to whether these become integrated with Single Sign-On (for each user) or are excluded from Single Sign-On.



Excluding **does not** prevent the user from accessing a web app or domain, but it does exclude their login credentials from being automatically integrated with the My1Login SSO.

This functionality enables IT to determine whether newly detected applications should be integrated with SSO and can help identify 'Shadow-IT' i.e. cloud applications being used for business that IT may be unaware of.

3.1.5 Web SSO - Form Finder, Multi-Step Login Forms and Custom Credential Field Mapping

My1Login can dynamically detect the login form for most web-pages meaning that even if the structure of the target application page changes the Single Sign-On process will still work. For sites that do not work with the automated 'form finder' functionality, exception scripts can be created centrally by My1Login and these will be detected and used by the browser plug-ins on specific domains/apps.

Where there are non-standard login forms (e.g. 3 fields, or a two-step login form) My1Login can write exceptions to allow for seamless SSO to these applications. The exceptions are deployed centrally and do not require updates to locally installed My1Login components.

3.1.6 Mobile SSO

My1Login enables Single Sign-On to native mobile apps that support SAML and to mobile web apps either using SAML or credentials-based authentication via My1Login's mobile application.

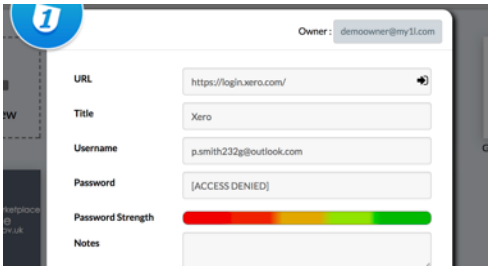
Native mobile apps can be configured to use My1Login as the IdP, enabling the user to log into the target application using their AD credentials.

For mobile web apps, these can be accessed via My1Login's native mobile app. The user logs in using their AD credentials (or a pin number once set-up) and can then launch their required applications. When an application is launched My1Login will authenticate the user with the target application using either SAML or the user's credentials for that app depending on configuration.

My1Login's mobile application is available for iOS, Android and Windows Phone.

3.1.7 SSO Without Revealing Credentials for Web and Mobile Web Apps

Where credential-based authentication is being used for Web Apps, My1Login provides the functionality for administrators to hide the application passwords from end users. Users can therefore log into the applications without having view permissions of the passwords.

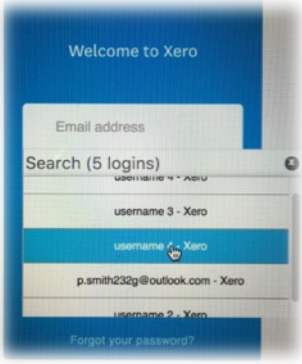


3.1.8 SSO for Web and Mobile: Handling of Multiple Credentials for a Single Web Application

If a user has access to multiple login credentials for one web application, there are two options for selecting which set of credentials that are to be used for Single Sign-on. The user can:

1/ Within their My1Login portal, click the application tile that contains the selected credentials

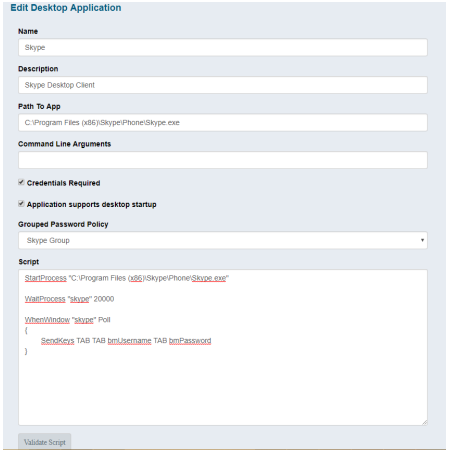
2/ Navigate directly to the target application website, where My1Login will present a list of the available credentials for that application adjacent to the login fields. If there are five or more sets of credentials available, a search box will also appear to enable rapid selection of the relevant credentials.



3.2 Single Sign-On for “Fat Client” Apps

3.2.1 Integrating “Fat Client” Applications that Do Not Have Connectors Available

Administrators can create templates (see picture) for “fat client” apps which can then be made available to specific users and groups.



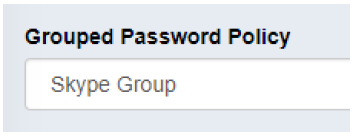
Once set up, users can launch the target application and My1Login will provide SSO for the user based on their stored credentials.

The target “fat client” application can be launched either:-

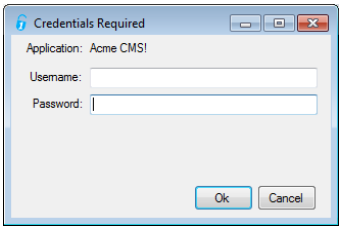
1/ From the user’s web portal
2/ Directly from the user’s desktop (where configured)

3.2.2 “Fat Client” Applications: Linking Stored Credentials with Other “Fat Client” and Web Apps

Some “fat client” applications also have web-client versions of their software that use the same credentials, for instance Skype or SAP. Creating a “Grouped Password Policy” on My1Login ensures that if one of these sets of credentials is changed, the other also changes i.e. if the Skype web app password changes, My1Login will automatically update the Skype desktop app password as well.



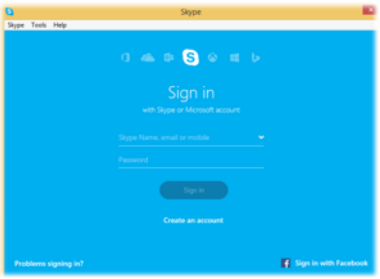
3.2.3 “Fat Client” Applications: Automatically Integrating Users’ Application Credentials



Credentials for the fat client applications can be manually entered via the users’ My1Login portal. Alternatively, where the “fat client” app has been launched directly, without using the portal, My1Login can be configured to prompt the user for the app credentials so they can be stored in My1Login and used to provide SSO for the application.

3.2.4 “Fat Client” Applications: Examples of Compatibility

My1Login’s “fat-client” connector is able to perform credentials-based SSO to almost any application that runs as an executable on the desktop i.e. Remote Desktop Programs, Citrix, Mainframe Emulators, Cisco Jabber, Skype.



Functionality of My1Login’s “fat-client” connector can also be combined with the browser plug-ins to provide SSO into Citrix applications and Flash-based login forms.

3.2.5 "Fat Client" Applications: Handling of Multiple Credentials for a Single "Fat Client" Application

If a user has access to multiple login credentials for one "fat client" application, there are two options for selecting which set of credentials that are to be used for Single Sign-On.

The user can:-

1/ Within their My1Login portal, click the application tile that contains the required credentials

2/ Launch the target "fat client" application directly from the desktop, where My1Login will present a list of the available credentials for that application. The user can then select the set of credentials to be used and My1Login will use these to perform SSO into the application.

3.2.6 Handling of Custom Login Windows and Multi-Step "Fat Client" Login Processes

In the circumstances where a target fat-client application utilises a non-standard login form (e.g. 3 login fields or a two-step or two-page login form), My1Login provides the capability for exception scripts to handle this scenario, providing seamless SSO to these applications.

My1Login's desktop connector can also handle SSO to multi-step, fat-client login forms by detecting 'child' windows of fat-client applications and text within these 'child' windows.

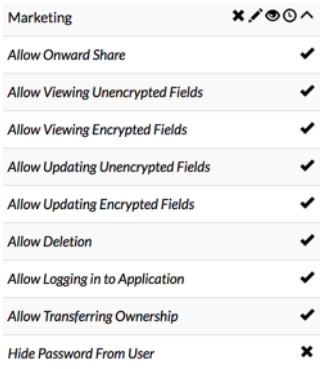
3.3 Privileged Password Manager

3.3.1 Overview of Privileged Password Manager

My1Login's Privileged Password Manager provides users with access to sensitive and/or shared credentials they need to perform their role. It ensures that appropriate access is granted to specific users and groups and that access is only available during specific periods of time and/or within specific days and times. My1Login provides a full audit trail around this activity so it can be determined who used, or even viewed, specific credentials at any given time.

Access to and removal of shared credentials works in real-time with no need for the user to refresh the My1Login user portal.

3.3.2 Issuing Privileged Passwords: Fine-grained Permissions



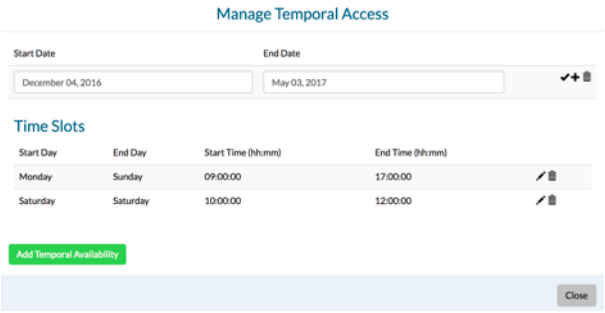
Where permitted, the Privileged Password Manager enables the sharing of credentials with users and groups together with the ability to hide the password for recipients of those shared credentials allowing them to use but not view the password on My1Login.

A variety of fine-grained permissions provide more granular control of the access rights that are delegated to the recipients of any shared credentials. This includes read/write/execute and whether they have permission to share the credentials on to additional users.

3.3.3 Privileged Password Manager - Temporal Access by Time and Date

Further access controls can be provided by only allowing users and/or groups to access specific credentials between specific dates and within specific timeslots during these dates.

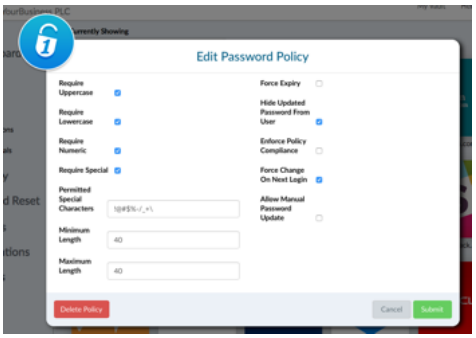
Access to the permitted credentials will become available to appropriate users within the defined times and dates in real time, without the need to refresh the user's My1Login portal page. Conversely, outside of the defined times, access will be revoked in real-time with no need for the user to refresh the user's My1Login portal page.



3.3.4 Privileged Password Manager - Automatic Password Generation for Web Apps

When a new account for a target application is created, My1Login can automatically generate a long, strong, high-entropy password on behalf of the user in-line with the password policy set in My1Login for that application.

3.3.5 Privileged Password Manager - Automatic Password Updates on Web Apps



My1Login can automatically generate long, strong, high-entropy passwords and pro-actively update these passwords on target applications.

My1Login Administrators can set policies to proactively update target application passwords: -

1/ After a defined period of time
2/ The next time users log in to the target application
3/ If a user visits the password change page of the target application

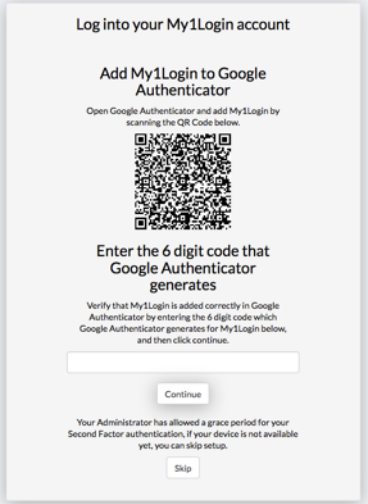
My1Login Administrators can also choose to hide updated passwords from end-users. End-users can still seamlessly access the application via My1Login, but are unable to view the password for that application in the My1Login portal. This can mitigate phishing risks since users would not necessarily know the passwords for the applications they access and therefore cannot succumb to a phishing attempt.

3.3.6 Privileged Password Manager - Password Updates on Thick-client Apps

My1Login can also be configured to update the passwords being used for fat-client applications. Administrators can set a password policy for the fat-client application. Then, when the user is prompted with a password change window by the fat-client application, My1Login will automate the process and create a new strong password that complies with the password policy set for that application.

3.4 Multi-Factor Authentication (MFA)

3.4.1 Overview of Multi-Factor Authentication



My1Login can be configured to enable external AD users to log into the system via a custom, public URL specific to each customer account.

A Multi-factor authentication policy can be applied to these external logins for additional security enabling the user to log into the system with their AD credentials and their MFA.

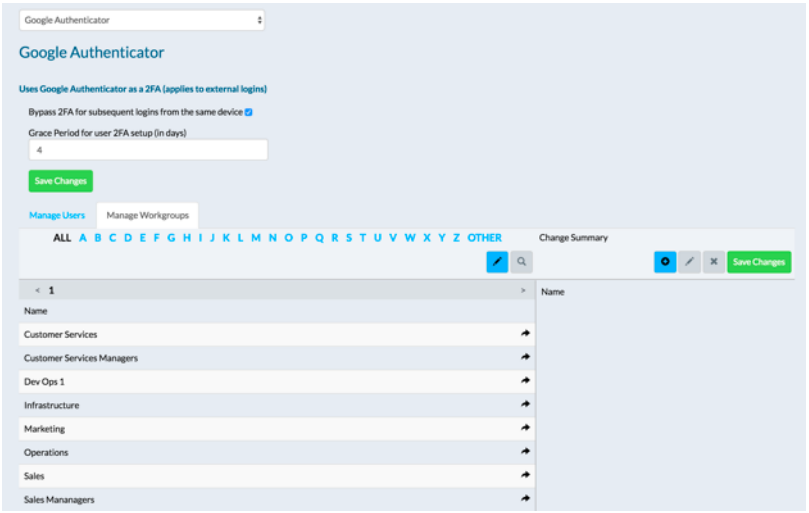
3.4.2 MFA: Currently supported MFA Types

My1Login supports Google Authenticator and Universal Second Factor (U2F) Devices e.g. Yubikey and Nitrokey. My1Login is also a signed-up technology partner with RSA.

3.4.3 MFA: On-Boarding Users and Groups

The MFA policy can be applied to:-

1/ Individual Users
2/ Specific AD Groups
3/ My1Login Groups (groups created locally within My1Login)



3.4.4 MFA: Grace Period

A ‘grace’ period can be applied to the set-up of MFA providing users with a window of time where they will still be able to access the system without being ‘forced’ to set up their MFA token.

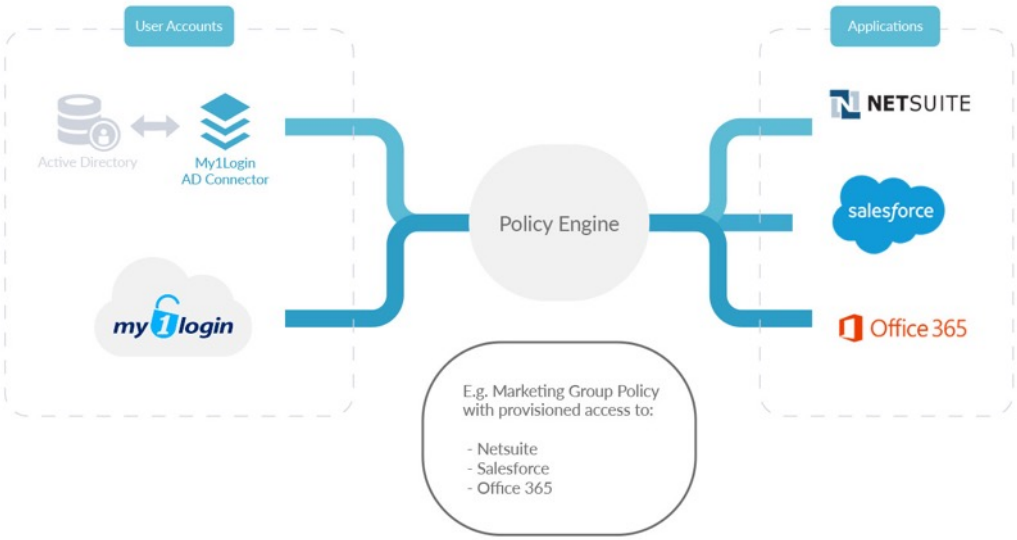
3.5 Provisioning Engine

3.5.1 Overview

My1Login's Provisioning Engine enables user accounts in My1Login to be provisioned, suspended and deleted automatically based on changes that occur within the Active Directory.

In addition, My1Login can enable policies to be set that provision users with access to target applications and/or specific privileged accounts depending on the AD Groups or My1Login Groups they are members of.

For applications that support Just-in-Time provisioning, My1Login can be used to provision the user with an account on the target (SP) application. Provisioning in this way can also be linked to AD Groups or My1Login Groups.



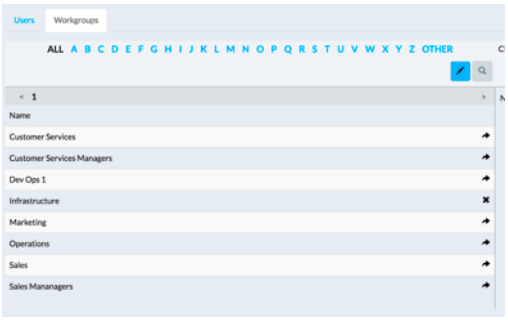
3.5.2 Organisational Provisioning

Organisational Provisioning enables policies to be set at group and user level, automating the provisioning of users' access to applications. So, for instance when a new employee joins the marketing team and is added to Active Directory, the policies for their group membership can automatically provision them with access to applications specified for that role. For example, if a user is part of the 'Marketing Group' within Active Directory My1Login can auto-provision access to the relevant marketing applications determined by the administrator.

As organisational provisioning is synchronised with the directory service (e.g. Active Directory) administration is vastly reduced, saving the admin team time and effort.

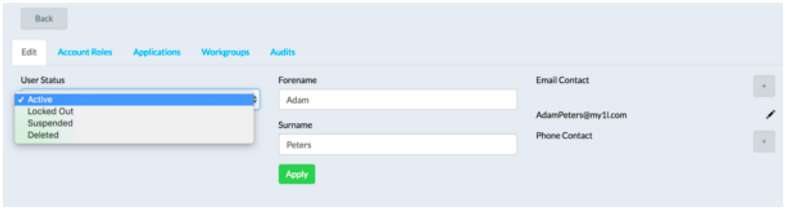
3.5.3 Just-in-Time Provisioning

With Just-in-Time (JiT) provisioning the user's access to an application is provisioned at the moment the user first tries to access the target application. Admins simply set a policy for a user or group to access a particular target application and when that user attempts to log into the app, their account is automatically provisioned. JiT provisioning, where supported by target applications, reduces admin effort as there's no need to provision the user manually; the user simply has to be authorised to access a particular SP's target application.



3.5.4 Automated De-Provisioning

Automatic de-provisioning ensures ex-employees' access to corporate systems is ceased when they leave the organisation. My1Login's user synchronisation means that when a user is suspended or deleted from the Active Directory, their ability to access applications via My1Login is automatically removed.



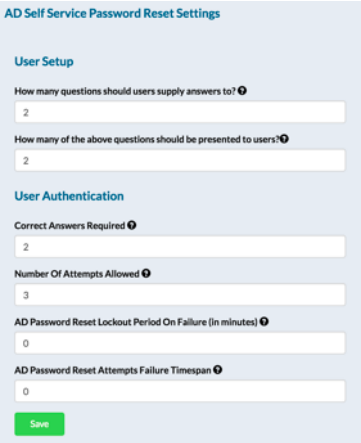
Alternatively, external (Non-AD) users can be manually suspended or deleted by Administrators directly within their Admin portal.

3.6 Self-Service Password Reset (SSPR)

3.6.1 Overview of AD SSPR

My1Login's Active Directory Self-Service Password Reset (AD SSPR) service enables users to self-reset their AD password, via challenge-response security questions on a web page, without the need to call the IT help desk. New passwords are validated against the AD password policy before being set.

3.6.2 AD SSPR: Configuration

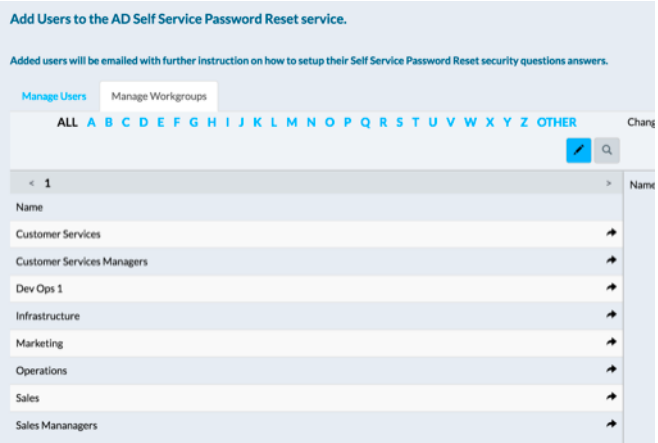


Administrators are able to configure a number of security questions in the system, then select which, and how many of these, are presented to users. Administrators can also define how many correct answers are required for the subset of questions presented, and how many attempts the user may have at answering before lockout.

3.6.3 AD SSPR: Enrolment

User roll out of AD SSPR can be staged by AD Groups, local My1Login Groups or individual users if required.

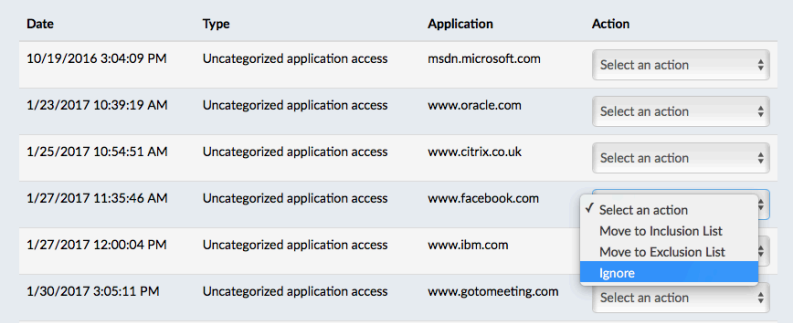
Users will receive a self-service set-up email requesting them to provide answers to the security questions. Once complete they will be able to use the SSPR via any device /web browser.



4 Security and Settings

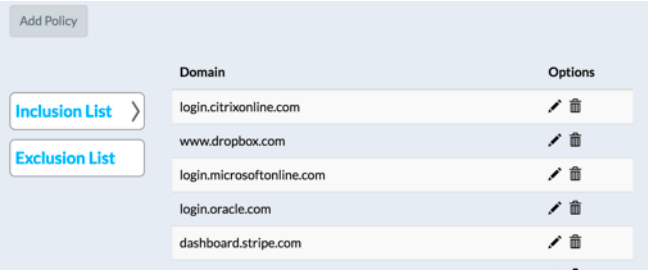
4.1 'Shadow-IT' Alerts

My1Login can be set to alert IT Administrators of 'unknown' web applications that are being accessed by end-users. This enables IT to determine whether these applications should be integrated (included) with SSO.



4.2 Domain Inclusion/Exclusion Lists

For web applications that utilise login credentials rather than a 'connector' such as SAML, My1Login can be configured to automatically include or exclude specific web apps (domains) being integrated with the IAM.



If an application is 'included', My1Login will automatically integrate each user's login credentials for that application and use these to provide Single Sign-On to the application the next time the user visits the web application.

If an application is 'excluded', then My1Login will not integrate users' login credentials for that application. My1Login can be configured to 'exclude' all applications other than those explicitly stated on the 'inclusion' list.

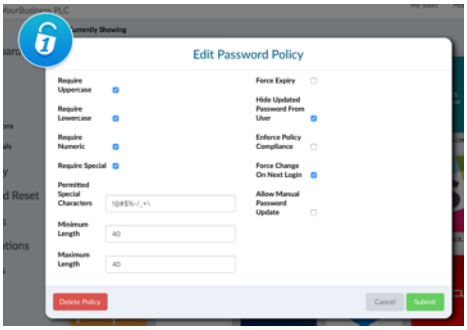
4.3 IP Filtering Policies (Allow/Deny List)

My1Login enables external (public) access to the user's Single Sign-On portal to be restricted only to specific IP addresses or ranges. So, for example, the finance department might not be permitted to access their applications from outside the corporate environment.

Specific IP Filtering Policies can be configured to apply to AD Groups, local My1Login groups or individuals.

4.4 Password Policy Enforcement for Target Apps

My1Login enables an organisation to enforce password security policies by pro-actively updating user passwords for target applications where required. This functionality is further described in sections 3.3.5 and 3.3.6.

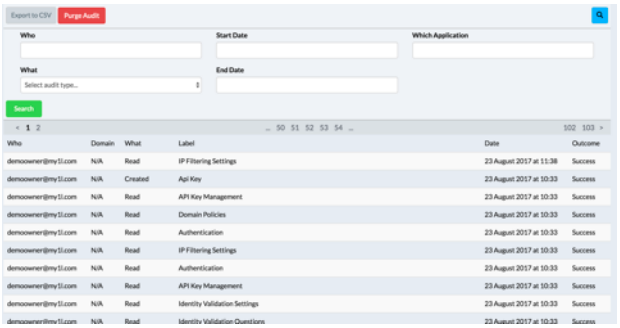


5 Audit and Reporting

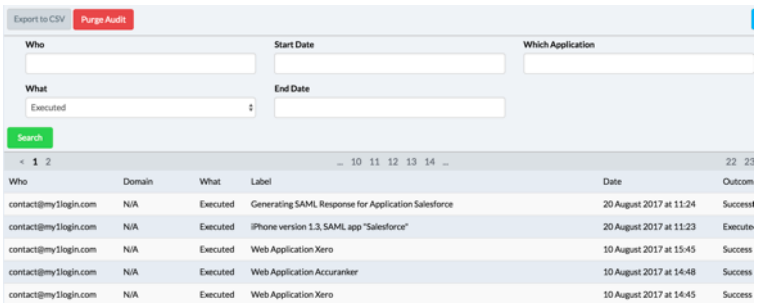
My1Login provides a variety of reports that can assist with audit, governance and alerting.

5.1 System Audit

The system audit report provides administrators with an audit trail of all activities logged on the system, this comprises actions performed on the system by users and/or administrators. These reports are fully exportable and searchable.



5.2 Application Usage Audit



Subset of the System Audit showing who accessed what and when. The application usage reports detail all instances of users logging into applications, whether these are SAML or credentials-based apps. It also provides details of where users have simply viewed a password stored on the system to provide auditing around privileged access management. These reports are fully exportable and searchable.

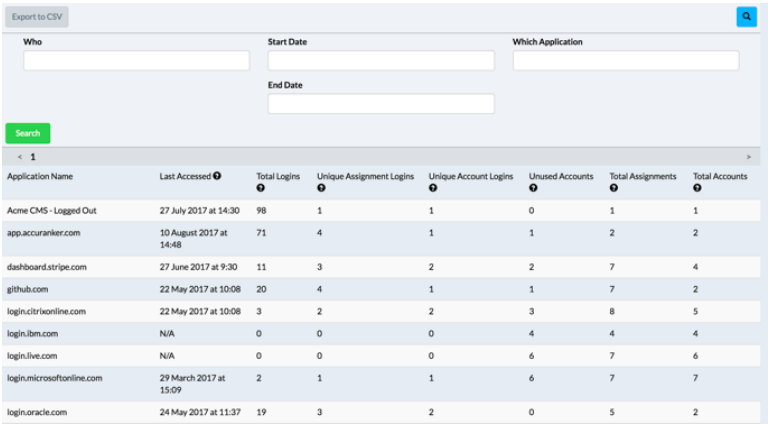
5.3 Application Usage Summary

The application usage summary report is derived from the system audit and provides summary counts, for a given period, of application identities (credentials or SAML) in use and being stored on the system. These reports are fully exportable and searchable.

Assertion 1:-
Users have Assignments to Accounts for applications so they can log in.

Assertion 2:-
An Account is an identity used to log into application and can be either credentials-based i.e. username and password or token-based i.e. using SAML.

Assertion 3:-
A User may have Assignments to more than one Account for a single application.

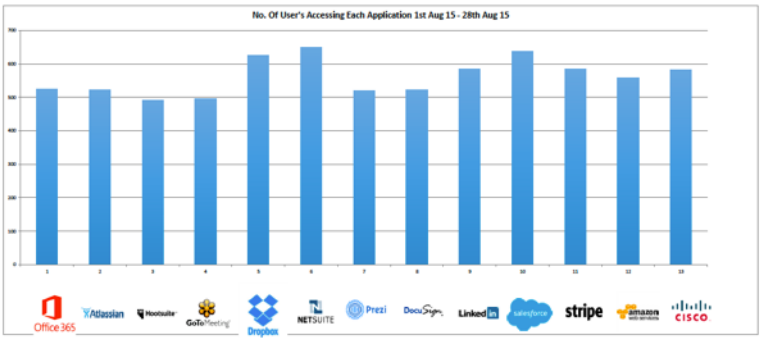


Last Accessed: The last date and time that My1Login detected any user logging in to (executing) this application within the stated time period. If no users have logged in to (executed) the application within the time period this will show as "N/A"

Total Logins: The total number of times the application was logged in to (executed) by all users within the stated time period.

Unique Assignment Logins: The number of individual (i.e. unique) users that have been assigned with access to this application and have logged in to (executed) the application within the stated time period.

Unique Account Logins: The number of unique identities (either login credentials or token-based) that have been used to log into the application within the stated time period.



For example, if some users have access to more than one identity (either login credentials or token-based) for a single application, this would potentially display a higher number than the number of users on the system. Conversely, if many users are sharing access to one set of login credentials (i.e. 10 users sharing access to the same company Twitter account), this number would appear lower than the number of users.

Unused Accounts: The number of unique identities (either login credentials or token-based) that exist on the system (irrespective of when they were created) but have not been used to login to the application (executed) within the given time period.

Total Assignments: The total number of users that have access to identities (either login credentials or token-based) for this application irrespective of time.*
For example, if 50 users share one login for this application, the report will show 50 total assignments i.e. 50 users have been assigned access to this application.
Also, if 50 users each had access to 5 sets of credentials for this application the total number of users who had been assigned access to this application would still be 50 since there are still only 50 users assigned access to this application.

Total Accounts: The total number of unique identities (either login credentials or token-based) stored in the system for this application irrespective of time.*

* "Total Assignments" and "Total Accounts" are calculated for all time, however all other data is calculated within the Start Date and End Date defined in the "Refine Search" area.

5.3.1 Syslog Integration

My1Login's AD Connector can act as a Syslog client to publish the full System Audit entries to the customer's Syslog server for analysis and alerting.

6 Off-Premise Users - AD and External (non-AD Users)

My1Login defines an On-Premise user as one who directly authenticates their session against the domain controller on the same sub-net as the domain controller. I.e. this includes users who may be outside the corporate office but are connected over a VPN. Off-Premise users are those users who do not have direct access to the domain controller.

On-premise AD users can be seamlessly authenticated with their My1Login account by the My1Login AD Connector.

AD users can authenticate with My1Login from outside the AD using their AD credentials to sign in to the Mobile app or the web-site (where permitted).

External (non-AD) users, can access their My1Login service from the My1Login mobile app or any browser using their email address and chosen passphrase.

7 Off-Premise AD Users

Off-Premise AD User Undertaking IdP Initiated SSO - Example of a user who is outside of the corporate environment logging into the My1Login portal, launching, and being authenticated with an application. This user logs into the My1Login portal using their Active Directory credentials and MFA if required. The user is then authenticated by My1Login and can utilise SSO to access permitted applications and stored credentials.

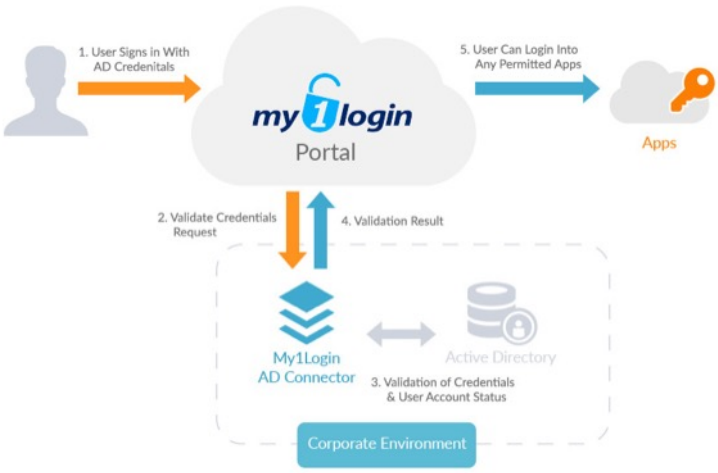
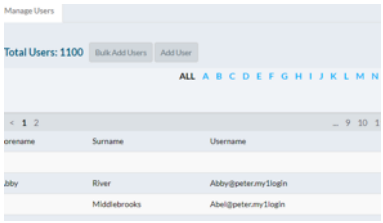


Diagram – Off-Premise, Active Directory User, IdP-Initiated Login

8 External (Non-AD Users)

Admins can provision My1Login accounts for non-AD users by adding their email address to the system. For users who are not part of Active Directory, these users can sign directly into the My1Login portal using their registered email address and pass-phrase. From inside the portal, IdP initiated SSO can be utilised to be authenticated with any SAML applications, or with credentials applications using the plug-in.



8.1 Adding Individual Non-AD Users

External users that are not listed in the Active Directory can be added individually using their email address.

8.2 Bulk Adding Non-AD Users

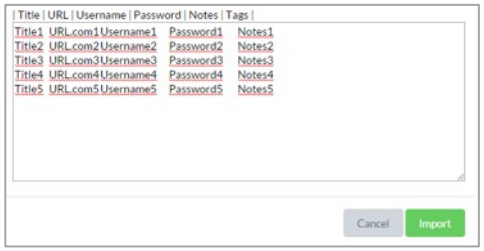
External users that are not listed in the Active Directory can be bulk imported to the system.

9 Bulk Importing Login Credentials

Login credentials can be bulk imported to My1Login, details that can be imported include; Title, URL, Username, Password, Notes and Tags.

9.1 Admin Bulk Import of Login Credentials

Administrators can bulk import login credentials from cells in a spreadsheet. These can then be distributed to users and groups as required.

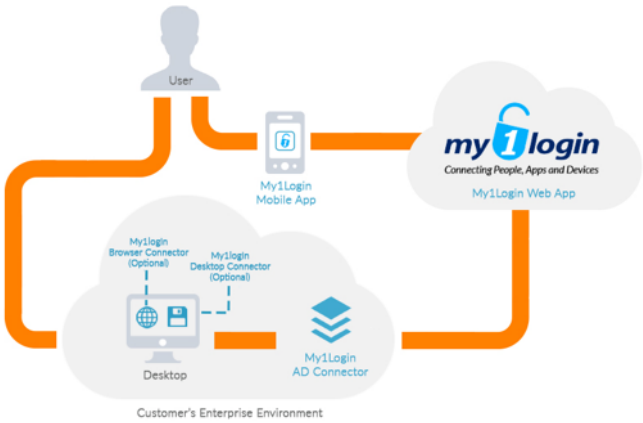


9.2 User Bulk Import of Login Credentials

Where permitted with the My1Login account settings, users can also be provided with access to the bulk import feature.

10 Solution Architecture

My1Login Web App provides the core administrative portal and user portal for the My1Login services. The portal also acts as an Identity Provider for SAML authentication.



My1Login's Active Directory Connector (Optional) provides two key functions:-

1/ Provisioning and de-provisioning of selected AD users and groups on the My1Login service.

2/ Seamless authentication of AD users with My1Login.

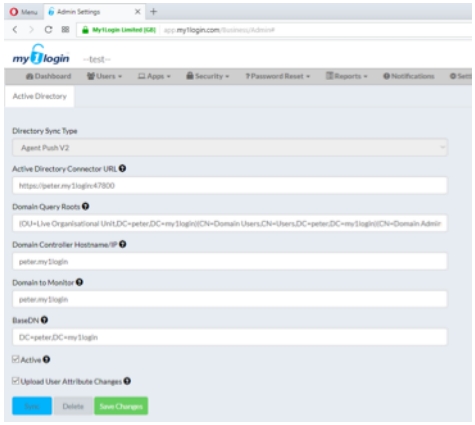
My1Login's Browser Connector (Optional) is installed as a browser extension available on Internet Explorer, Chrome, Firefox, Safari, Opera etc. and provides Single Sign-On for credential-based web applications. It also provides the functionality for web app auto-discovery and auto-integration. The plug-ins are also used to seamlessly authenticate AD users to the My1Login portal so they do not have to enter a username or password.

My1Login's Desktop Connector (Optional) is installed on end-user PC's to enable Single Sign-On for apps that run as desktop executables i.e. fat-clients, virtualised apps, emulator-based apps/mainframes and Flash-based web applications.

My1Login's Mobile Connector (Optional) is installed as an application on users' mobile devices and provides SAML and credential-based Single Sign-On to web apps via a contained browser within the My1Login mobile app.

11 Directory Integration

My1Login integrates with Active Directory and LDAP compliant directories.



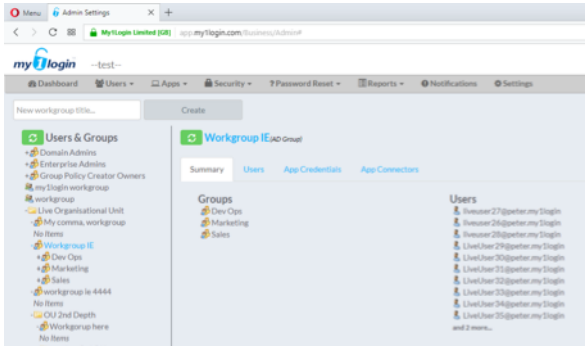
'Push' integration can be achieved with Active Directory using My1Login's AD connector. With 'push' integration information is sent from the customer's network to My1Login.

'Pull' integration can be achieved with any LDAP compliant directory by configuring the LDAP settings within the My1Login administrator interface. With 'pull' integration information is pulled from the customer's network by My1Login, this can require LDAP ports to be opened and firewall rules to be configured by the customer.

11.1 Directory Integration: User Synchronisation with My1Login

Directory integration enables users to be automatically provisioned or de-provisioned in My1Login based on their directory status (i.e. active, disabled, deleted).

Users, groups and Organisational Units (OUs) can be synchronised with My1Login.



11.2 Directory Integration: User Authentication with My1Login

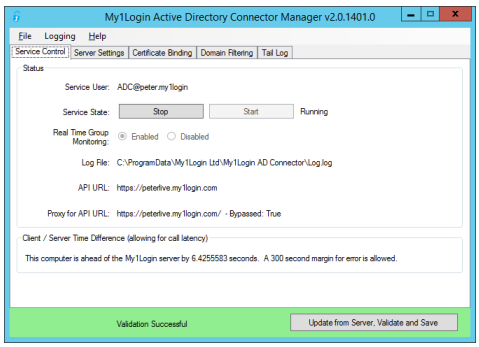
Where My1Login's Active Directory connector has been installed, AD users are 'seamlessly' authenticated with My1Login without having to enter a username and password and without having to open their 'portal'.

11.3 Directory Integration: AD Connector

My1Login's AD Connector allows selection of specific OUs or Groups to be monitored. It also recognises real-time changes to groups and users and synchronises these changes with My1Login.

This enables suspended (disabled) and deleted users to have their access to My1Login immediately revoked.

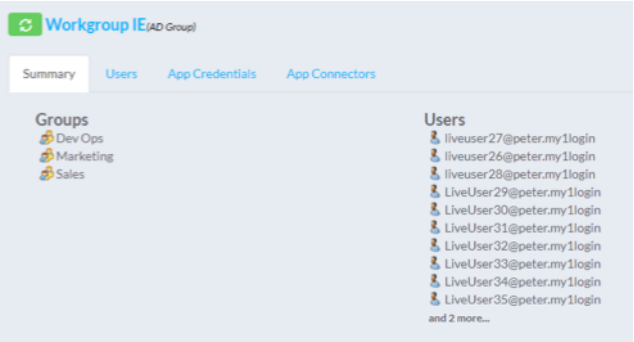
My1Login's AD connector also acts as a permanent administrator, enabling re-generation of RSA security keys should these be required where a user has changed their AD password. It can also be load-balanced for resilience.



11.4 AD Groups

AD Groups can be used within the My1Login system to: -

1/ Enable privileged passwords to be shared with group members
2/ Enable policies to be set to allow SAML applications to be automatically provisioned to members of specific groups.



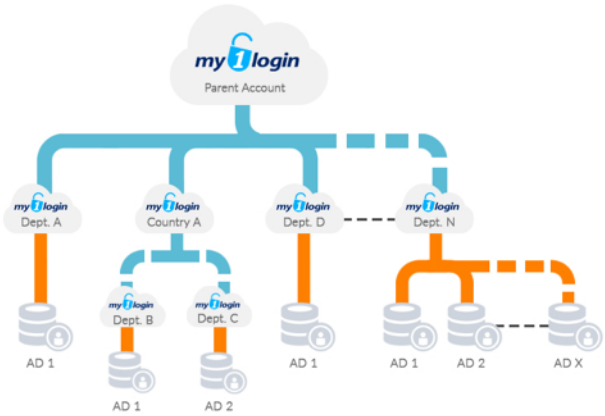
11.5 Local Groups in My1Login

Local groups can also be configured within My1Login to: -

1/ Enable privileged passwords to be shared with group members
2/ Enable policies to be set to allow SAML applications to be automatically provisioned to members of specific groups.

11.6 Multiple AD Domains / Large Scale AD Structures

My1Login can integrate with multiple Active Directory domains, allowing an organisation to provide Single Sign-On access to all users, regardless of the Active Directory they are a member of. Parent accounts only have reporting and audit visibility over any "child" accounts in their branch of the tree.



12 Custom Branding / Managed Service Providers

12.1 Custom Branding

My1Login customer accounts are, by default, assigned a sub-domain of my1login.com. This sub-domain is referred to as the customer's white label URL.

It is also possible to map a customer's white label URL to their own custom domain, e.g. sso.customer.com.

The My1Login landing page of a customer's white label URL may be customised to match the customer's branding style.

12.2 Managed Service Providers

A managed service provider is defined, within My1Login, as a customer that manages sub-accounts on behalf of its customers.

The hierarchical account feature of the My1Login system permits an MSP to create customer specific sub-accounts, which may themselves feature custom branding, and to view aggregate reports of their customers' activity.

13 Customer Implementation Overview

My1Login's implementation process is initiated by the Sales Team completing a Deployment Engagement Form which triggers the formation of project and allocation of resource. An Implementation Specialist is then appointed to lead a Project Initiation Meeting with the customer and progress through My1Login's Customer Deployment Procedure which incorporates User Acceptance Testing and handover sign-off.

14 Service Management

14.1 Information Assurance

My1Login's infrastructure is ISO27001 compliant. Customer data is stored in TIA-942 Tier 4 Data-centres. Backup, disaster recovery and resilience plans are in place. Data-centre is firewall protected and located within a 24/7 infrastructure and network monitoring, redundancy and backup is provided.

14.2 Data Back Up and Restoration

My1Login will ensure that regular backups of the system are made according to the following schedule:

- A full backup is taken once per day
- Incremental backups are taken every five minutes
- Backups are AES256 encrypted
- Backups are retained in a private Azure data store.

The individual infrastructure components, application servers, database servers, etc. are configured for high availability and are hosted on the Microsoft Azure services. Microsoft Azure is effectively a Tier 4 data centre.

14.3 Service Constraints

Maintenance windows: Maintenance for a maximum of 30 minutes per month shall be permitted subject to 48-hour notice being provided.

Depreciation of any functionality or services will be subject to a 12-month notice period.

14.4 On-boarding and Off-boarding

On-boarding into My1Login can be achieved by installing the My1Login Active Directory Connector which synchronises information with the My1Login service. Additionally, My1Login can provide on-site support in the on-boarding process for larger deployments. Full documentation and web conference/screensharing support is provided by My1Login to assist with onboarding. On-site training can also be arranged if required. To cease use of the My1Login service, contact My1Login support and request to terminate your licence. Access can be terminated immediately.

14.5 Financial Recompense

Subject to all reasonable endeavours used by both parties. For service failures attributable to My1Login:

- 1% of the annual licence fee for a full day of lost service
- maximum of 5% of the annual licence fee.

14.6 Pricing

Pricing details are contained within My1Login's "G-Cloud Pricing May 2018" document.

14.7 Service Levels

My1Login offers UK-Based high-availability infrastructure that operates at 99.9% availability.

14.8 Ordering and Invoicing

Standard customer purchase order issued to the supplier, no work will commence until a customer purchase order is received.

Invoicing within 30 days of purchase order receipt.

14.9 Scalability

My1Login is highly scalable and capable of operating globally on a multiple user, multiple location and multiple services capability.

14.10 Termination Process

- Customer minimum contract is 12 months, 30-day customer termination notice required.
- Supplier may terminate on non-payment

14.11 Technical Requirements

Operating Systems

- Windows
- Linux
- Mac OS X
- Terminal emulators on any of above platforms

Browsers

- Internet Explorer 9
- Internet Explorer 10+
- Microsoft Edge
- Firefox
- Chrome
- Safari
- Opera

Mobile Device:

- Windows Mobile
- Android Mobile
- iOS Mobile

15 Service Plans for Subscription

My1Login offers multiple service plans as follows:

	SSO	SSO Plus	My1Login Enterprise
Active Directory Integration	✓	✓	✓
Active Directory Self-Service Password Reset	✓	✓	✓
SSO for Web apps	✓	✓	✓
SSO for Mobile (Windows, Android, IOS)	✓	✓	✓
Integration of Target Apps with Connectors	✓	✓	✓
Reporting	✓	✓	✓
UK-Based High-availability and Security Infrastructure	✓	✓	✓
For Internal (i.e. AD) and External (i.e. non-AD) Users	✓	✓	✓
For Active Directory On-Premise and Off-Premise Users	✓	✓	✓
Integration of Target Apps Without Connectors i.e. Credentials Based		✓	✓
Automatic Password Generation for Web Apps		✓	✓
Password Policy Enforcement for Web Apps		✓	✓
Policy-based Enrolment		✓	✓
Security Policy		✓	✓
Multi-Factor Authentication		✓	✓
SSO Without Revealing Credentials		✓	✓
Audited Access to Privileged Accounts		✓	✓
IP Allow & Deny List		✓	✓
Domain Inclusion/Exclusion List for SSO		✓	✓
User Provisioning			✓
Custom Credential Fields for Authentication			✓
Hybrid Cloud / On-Prem Deployment Option			✓
White Label Branding			✓
Multiple AD Domains			✓
Custom Connectors			✓
Privileged Password Management			✓
Auto-Discovery of Web Apps being used by end-users			✓
Auto-Integrates Users' Apps			✓
Informs IT of Unknown Web Apps Being Used			✓
Automatic Password Updates on Target Apps			✓

SSO for Desktop*			
Single Sign-On for Legacy (Thick Client Apps)	✓	✓	✓
SSO Without Revealing Credentials	✓	✓	✓
Citrix, Mainframe, RDP and Terminal Compatibility	✓	✓	✓
Password Policy Enforcement for Legacy Apps	✓	✓	✓
Automatic Password Generation for Legacy (Thick Client) Apps	✓	✓	✓
Automatic Password Updates on Target Legacy (Thick Client) Apps	✓	✓	✓
Local Cache (offline mode)	✓	✓	✓

*note: must be purchased with SSO, SSO Plus or My1Login Enterprise. Cannot be purchased standalone.

16 Training and Deployment Services

My1Login offers packages for training and deployment services in addition to consulting engagements billed hourly and specified in advance via a statement of work contract.

16.1.1 Training and Deployment Packages

16.1.1.1 Silver

Silver		
Planning	Engagement Lead (Term)	4 weeks
	Directory Deployment	Single Domain Directory Integration
	System Documentation	Yes
	DR Planning	No
Deployment	User Management/Provisioning	Up to 1 App
	Configure MFA	Yes
	Sandbox Account for Testing	Yes
	App Configuration & Roll-out	Up to 5 Apps
	Custom App Connector	No
	Configure Desktop SSO (Legacy)	No
	Policy Configuration	No
	On-Site (UK) Deployment Support	No
Pricing		£5,000

16.1.1.2 Gold

Gold		
Planning	Engagement Lead (Term)	6 weeks
	Directory Deployment	Multiple Domain Directory Integration
	System Documentation	Yes
	DR Planning	Yes
Deployment	User Management/Provisioning	Up to 3 Apps
	Configure MFA	Yes
	Sandbox Account for Testing	Yes
	App Configuration & Roll-out	Up to 5 Apps
	Custom App Connector	Up to 2 Apps
	Configure Desktop SSO (Legacy)	Yes
	Policy Configuration	Yes
	On-Site (UK) Deployment Support	No
Pricing		£8,000

16.1.1.3 Platinum

Platinum		
Planning	Engagement Lead (Term)	10 weeks
	Directory Deployment	Multiple Domain Directory Integration
	System Documentation	Yes
	DR Planning	Yes
Deployment	User Management/Provisioning	Up to 5 Apps
	Configure MFA	Yes
	Sandbox Account for Testing	Yes
	App Configuration & Roll-out	Up to 8 Apps
	Custom App Connector	Up to 4 Apps
	Configure Desktop SSO (Legacy)	Yes
	Policy Configuration	Yes
	On-Site (UK) Deployment Support	Yes
Pricing		£10,000

17 Basic and Premium Support

Basic Support. Cost: included in any license

- Major Incident Reporting by telephone: 24 x 7
- Other Incidents: 0800hrs to 2300 hrs phone support (UK time)
- Unlimited Online Customer Support

Premium Support (Optional)

- 24 x 7 Priority Phone Support
- Unlimited Online Customer Support
- Proactive Notifications

Premium Plus Support (Optional)

- Dedicated Technical Account Manager
- Participation in Customer Product Steering Group
- Must purchase Premium Support

18 Managed Services

Managed Service	Description	Pricing
Application Integration	My1Login will provide ongoing support in the creation of up to 15 application templates per year. Templates created within 1 working day of request.	£6,000 per annum
Customised Reports	Monthly provision of up to four custom audit reports charting specifically agreed metrics. i.e. average utilisation per user, license pool utilisation etc.	£6,000 per annum

18.1.1 Professional Services

Pricing stated within My1Login's pricing schedule and SFIA rate card.