Cloud Access Manager 8.1.4

How to Configure Advanced Form Fill Authentication

Cloud Access Manager How to Configure Advanced Form Fill Authentication
Updated - November 2018
Version - 8.1.4

Contents

Introduction

Many applications, especially those that are internet facing, choose to use form fill authentication. This means they display username and password fields on the web page for the user to manually enter their sign-in credentials. Each application is different and while the majority of applications can be configured automatically, some applications require manual configuration. This guide describes how Cloud Access Manager implements its form fill functionality so that you can configure applications manually.

For complete examples of how to configure form fill authentication applications in Cloud Access Manager, please refer to the section entitled Form Fill Authentication in the *One Identity Cloud Access Manager Configuration Guide*.

Background

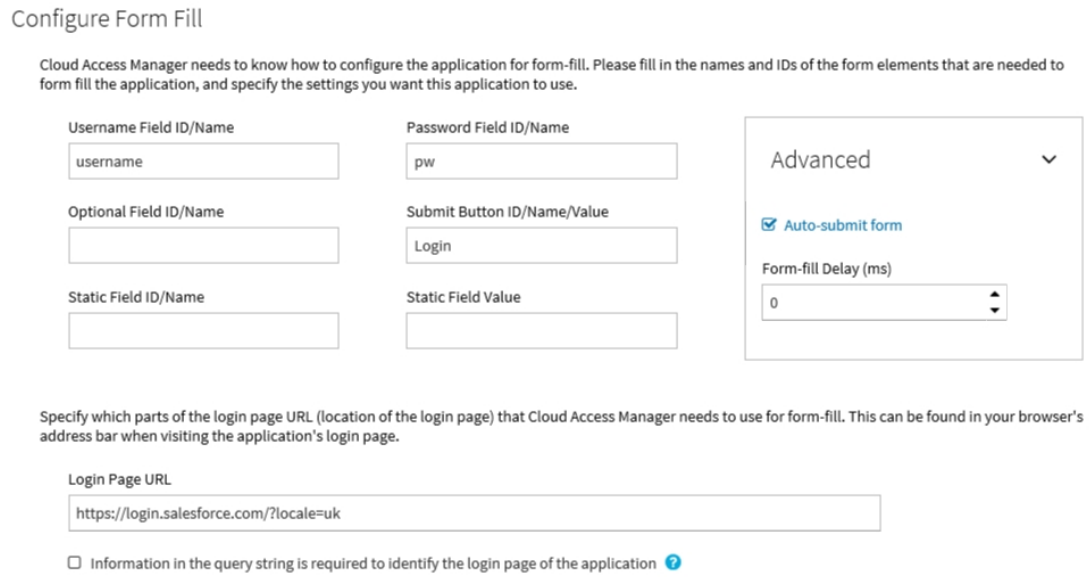
To successfully Single Sign-on (SSO) a user into a web site using Cloud Access Manager form fill functionality, some details about the site's login page must be collected and added to the application's configuration in Cloud Access Manager. This guide describes the elements that are required to log in to a site and what Cloud Access Manager needs to know about the application to successfully automate the process for you.

Form fill field values

Cloud Access Manager asks the user to identify the fields on the login page, typically by their HTML ID or name. The **Username Field ID/Name** and **Password Field ID/Name** are required fields, the others are optional. However, many applications require the user to click a Sign In/Log In button, which means that the **Submit Button ID/Name/Value** is often required.

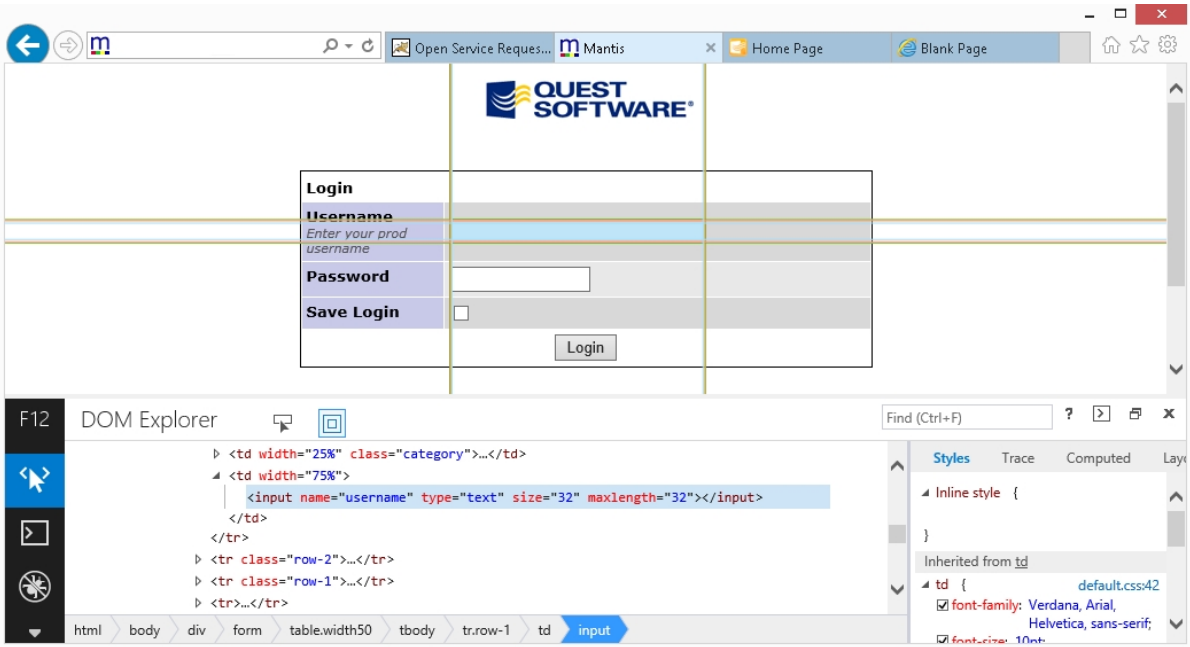
- The **Optional Field ID/Name** is used to capture and fill an additional field on the login page, such as the user's domain.
- The **Static Field ID/Name** and **Static Field Value** boxes are used when all users are required to enter the same value into an additional field on the login page. For

example, the instance name of the application.



NOTE: If the application displays the password field on a separate page to the username field, check the **The password field is located on a separate page** box. You can then manually enter the field identifiers for the password field and submit button.

The easiest way to obtain the correct Field ID and Name from a web page is to use the browser's built-in developer tools — Internet Explorer, Google Chrome browser and Mozilla Firefox all have this feature. This allows you to click each field in turn and locate its ID and/or name:



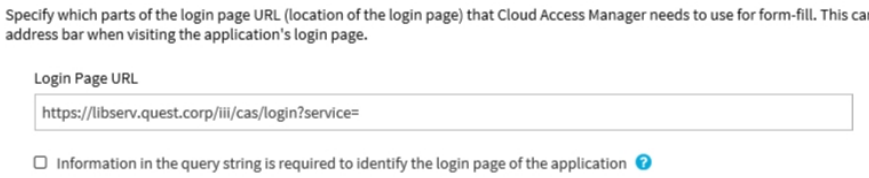
Form fill URLs

This section describes how to define the URLs used by the application's login page.

Most applications have a login page that can be easily identified within the path portion of the URL, for example:

http://192.168.121.18/mantis/login_page.php?return=my_view_page.php&error=1

In this situation, Cloud Access Manager can locate the login page without taking into account the parameters within the query string, which are likely to differ from user to user and so the query string information selection box can be clear:



Some applications use URLs where only the query string portion of the URL changes when navigating between pages. For example, pages in an Oracle application may only differ by a function ID in the query string. The home page might have the ID of 150, for example https://server/OA_HTML/RF.jsp?functionId=150 and the login page an ID of 200, for example https://server/OA_HTML/RF.jsp?functionId=200

To configure this type of application, select the box labelled **Information in the query string is required to identify the login page of the application**. Cloud Access Manager will then allow you to select the query string parameter that identifies the login page, such as the functionId=200 parameter used in the previous Oracle example.

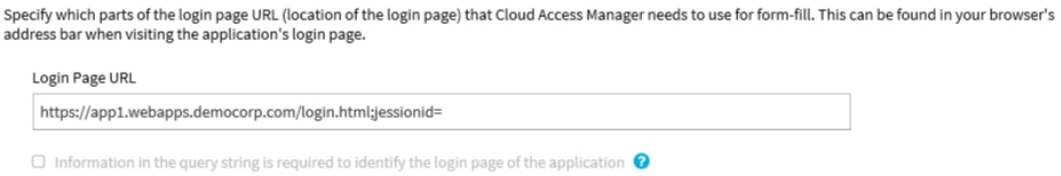
If an application uses multiple query string parameters, select only the parameters that identify the login page. For example, some applications use additional parameters to store information unique to a particular user or access attempt, such as a session identifier. You should not select these parameters as they would prevent the login page from being detected for all users/requests.

NOTE: Elements within the login path of an application are case sensitive and must be entered into Cloud Access Manager exactly as they appear in the URL bar in your web browser.

Some applications place a session ID on the end of the PATH to track a user's session called a JSESSIONID. For example:

http://host/page.htm;**jsessionid=<value>**?query

When this happens, it can prevent Cloud Access Manager from matching the URL of the form as the value is different for every session. For these applications make sure that the JSESSIONID value is not appended to the URL. If you want Cloud Access Manager to verify that a JSESSIONID value is present, but not what the value is, you can just strip the value as shown below.



NOTE: If the password field is located on a separate page, you will need to manually specify the URL of the password page. Cloud Access Manager requires the application to use a different URL for the password page to that of the login page containing the username field.

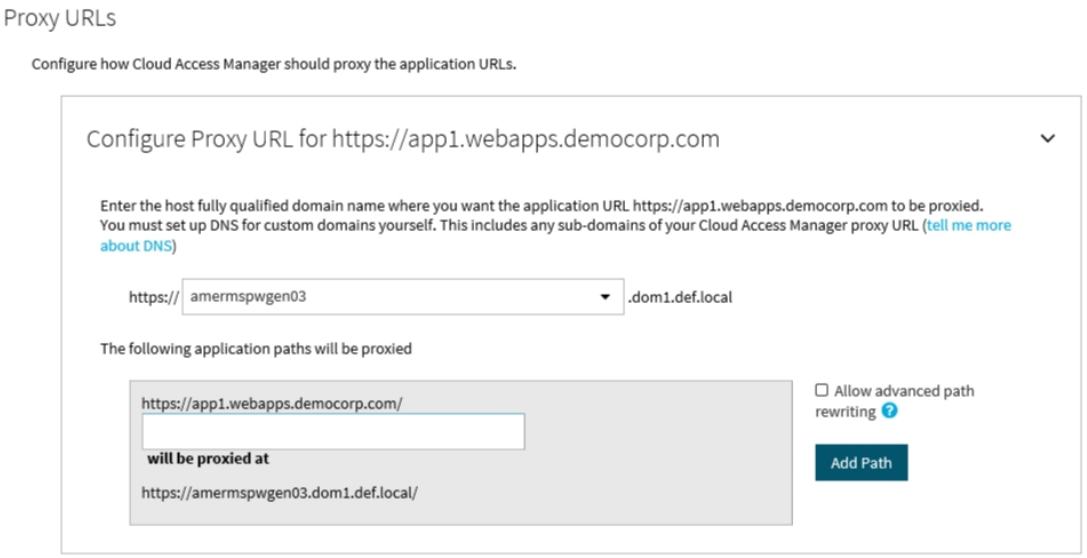
NOTE: If you are configuring an application that contains more than one </head> tag in its form fill URL (for example, because it launches a pop-up via JavaScript), it is possible that Cloud Access Manager could inject the form fill JavaScript at the wrong point in the page. This may prevent form fill authentication and rendering of the application from functioning as expected. To avoid this issue, ensure that any extra </head> tags in the page are positioned after the closing tag for the page's actual head.

Understanding proxy URL mappings

The proxy URL mapping defines how Cloud Access Manager will proxy the web application. Typically the entire web server serving the application will be included by the proxy using a dedicated Domain Name System (DNS) alias assigned to the proxy. This is the preferred mapping method and is compatible with the most applications. Internally we refer to this type of mapping as a root-to-root mapping.

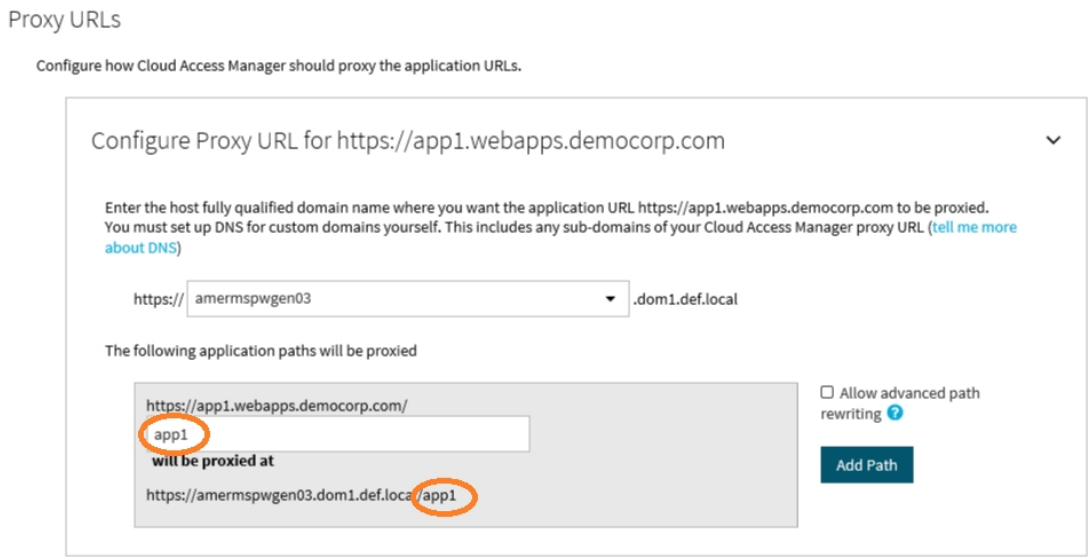
A root-to-root mapping requires a dedicated DNS alias for the application. The DNS alias typically contains the name of the application, for example **owa**.webapps.democorp.com. This new fully qualified domain name (FQDN) must be within the wildcard DNS subdomain created during the Cloud Access Manager installation and which will resolve to the public IP address used by the proxy. For example, if you created the wildcard DNS subdomain *.webapps.democorp.com during installation, you could now use an FQDN of owa.webapps.democorp.com to proxy an Outlook Web Access application or sp2010.webapps.democorp.com to proxy a Microsoft SharePoint Server 2010 application. For further information on creating a wildcard subdomain, please refer to the *One Identity Cloud Access Manager Installation Guide* and the *One Identity Cloud Access Manager Configuration Guide*.

If you did not create a wildcard DNS subdomain for Cloud Access Manager during installation, you will need to manually add the new FQDN into your public DNS. The new FQDN must be covered by the wildcard Secure Sockets Layer (SSL) certificate you are using to avoid certificate errors being reported by the client browsers.



When you configure this type of mapping, leave the path box empty. If you enter a path value, the mapping type will change from root-to-root to a symmetric mapping.

Alternatively, some applications are installed entirely within their own virtual directory on the web server where they reside. One example of such an application is One Identity Active Roles Server, which installs into the virtual directory/ARServerAdmin. Here it is possible to map the application path onto the same path on the proxy's public hostname allowing that hostname to be used instead of requiring a new public DNS Alias to be created, for example www.webapps.democorp.com/ARServerAdmin. Internally we refer to this type of mapping as a symmetric mapping.

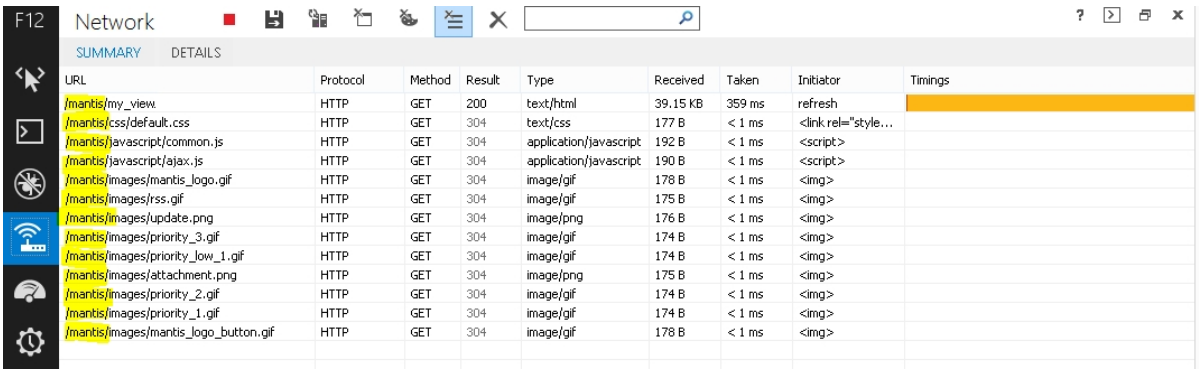


You can map multiple paths for an application, but you can only map paths that are unique to the application and not common path names, which could clash with other applications. For example, if you map the path /common for one application you cannot map the same

/common path to another unrelated application, as you cannot map them both onto the same path on the proxy's public hostname.

Often applications will not be installed within a self-contained virtual directory making symmetric mapping an unsuitable method for mapping them, for example OWA or SharePoint 2010. Attempting a symmetric mapping here can result in images not appearing on the application's pages, missing functionality, broken links and other unexpected behavior. Identifying whether an application is suitable for symmetric mapping can be difficult and so, if possible, it is more reliable to use a root-to-root mapping instead.

Using the network view on the browser's developer tools, or a tool such as Fiddler, will help determine if all of the requests to the application reside within a single virtual directory. For example, in the image below you can see that all requests reside within the /mantis virtual directory making this application suitable for a symmetric mapping:



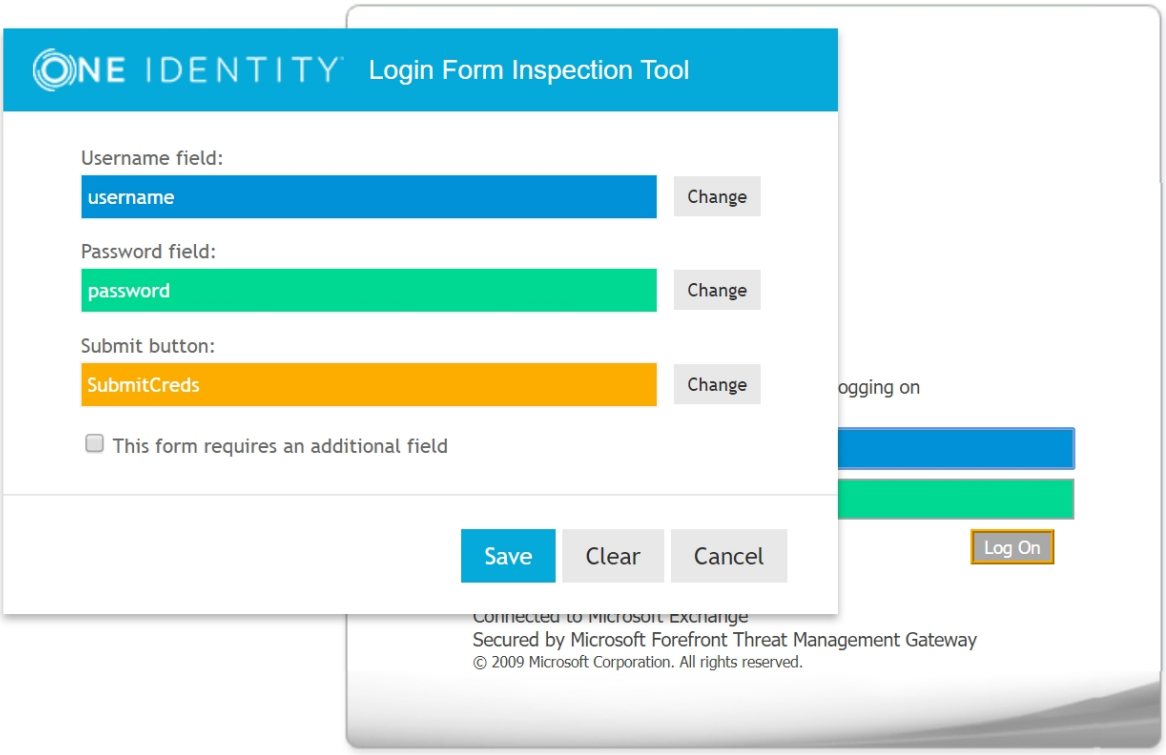
The symmetric mapping type is activated whenever you enter a path on the Proxy URL page.

When you configure a mapping, it is important to map to a directory or folder. It is not possible to map to an individual file.Cloud Access Manager must map to a whole web application, not a single page or file within an application. You cannot, for example, only proxy the login page by entering qpm/login.aspx into the path field.

LFIT-Login Form Inspection Tool

LFIT is a tool provided within Cloud Access Manager to enable fast identification of the values necessary to form fill against a supplied form. Generally LFIT collects the necessary data without issue, but occasionally it may fail to find certain fields or values. This is an indication that there is something non-standard about the login form or that JavaScript functions may be in place. Sometimes you can simply click in the fields manually to populate the values, at other times you may need to enter the values on the **Form Fill Details** page of the application wizard.

NOTE: If you are using LFIT in Internet Explorer, your Cloud Access Manager website will need to be in the Local intranet zone. For information on how to add the Cloud Access Manager proxy hostname to the intranet zone in Internet Explorer, please refer to the Form Fill Authentication section in the *One Identity Cloud Access Manager Configuration Guide*.


ONE IDENTITY Login Form Inspection Tool
Username field:
username
Change
Password field:
password
Change
Submit button:
SubmitCreds
Change
This form requires an additional field
Save
Clear
Cancel
ogging on
Log On
Secured by Microsoft Forefront Threat Management Gateway
© 2009 Microsoft Corporation. All rights reserved.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product