DFS DX User Management White Paper

Ensuring Data Security in a Cloud-Enabled Solution

User Management Considerations for Establishing a Secure and Seamless Experience

Introduction

From a compliance and margin-generating perspective, enterprise-wide asset optimization will define a fueling operation's competitive edge. Digital transformation is necessary to drive this optimization.

Dover Fueling Solutions (DFS) is drawing on 130 years of expertise as a global technology leader in the fueling industry to guide fuel site operators and their IT stakeholders through this digital transformation.

To assist with this objective, Dover Fueling Solutions has developed the DFS DX connected solutions platform, the industry's first open, global and common cloud platform. It utilizes artificial intelligence to spur efficiencies and cost savings across the operation, while simultaneously creating value for customers and end-users through frictionless experiences. Advanced analytics and IoT deliver solutions spanning wetstock management, remote access monitoring, targeted advertising and dispenser media, fleet fueling site management, point of sale management and partner integrations.

With the capability to comprehensively collect and share asset data across the enterprise, end-to-end data security is a prerequisite for a cloud-enabled, connected solution. Solutions architects designed DFS DX, which is powered by Microsoft Azure, to maximize security by establishing detailed — and practical — user management protocols. This white paper aims to educate fuel site operators and IT admins about the measures integrated into DFS DX to ensure data security and privacy.

Topics Covered in This Report

- Authentication and Authorization: Supporting Federated Identity Solutions
- Defining Permissions in a Connected Solutions Platform
- Considerations for Meeting Data Privacy Compliance Standards

Authentication and Authorization: Supporting Federated Identity Solutions

Identity Provider Authentication

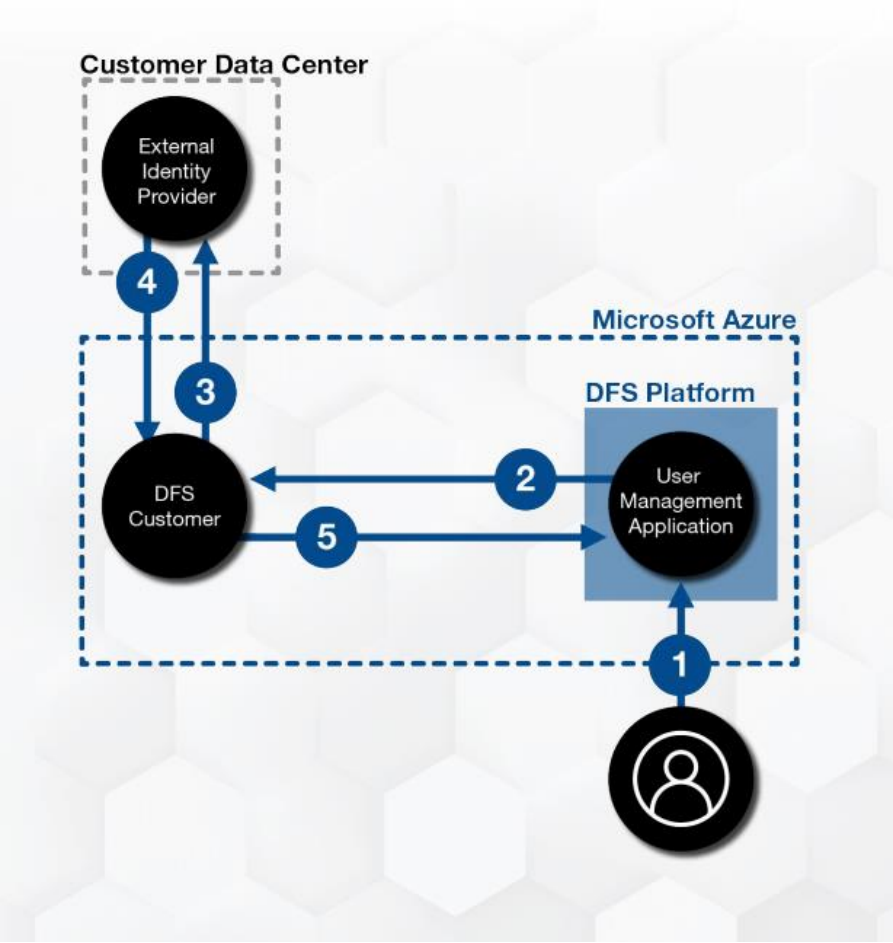
Authentication and authorization processes in a cloud-enabled solution must be both secure and user-friendly.

DFS DX facilitates authentication two ways. The first option is via the convenience operation's own SAML or OpenID Connect-supported identity provider (IdP). The IdP establishes a single, consistent, federated identity, which enables the identity to be used across multiple platforms, applications and networks. DFS DX utilizes SAML and OpenID Connect standards to create a Single Sign-On (SSO).

The second option is local authentication, which is utilized by fueling operations that either do not have an IdP or do not want to deploy one. This option also utilizes the customer identity access management capabilities of Microsoft Azure Active Directory B2C and establishes a Single Sign-On (SSO) experience.

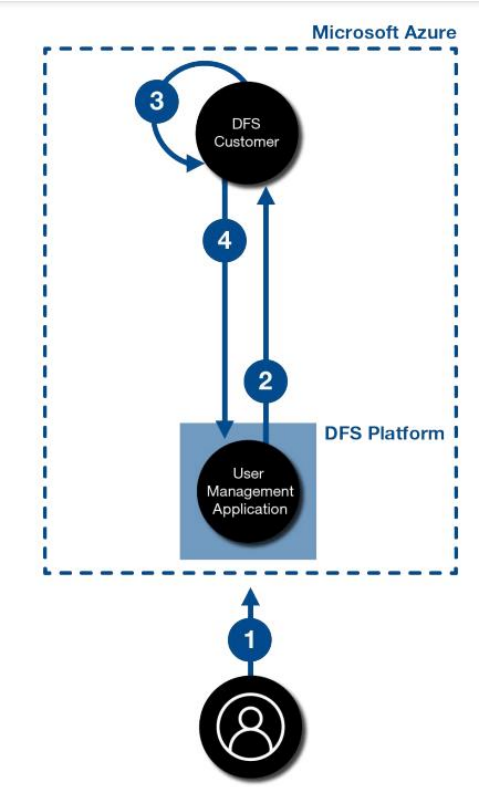
Because DFS DX is web-based, the sign-in experience is the same for on-site logins and remote logins. Other Microsoft Azure capabilities, such as multi-factor authentication, can provide additional measures of controlling access to the platform.

With the identity provider authentication option, the web addresses are reserved by the fueling enterprise and become exclusive to the operation.



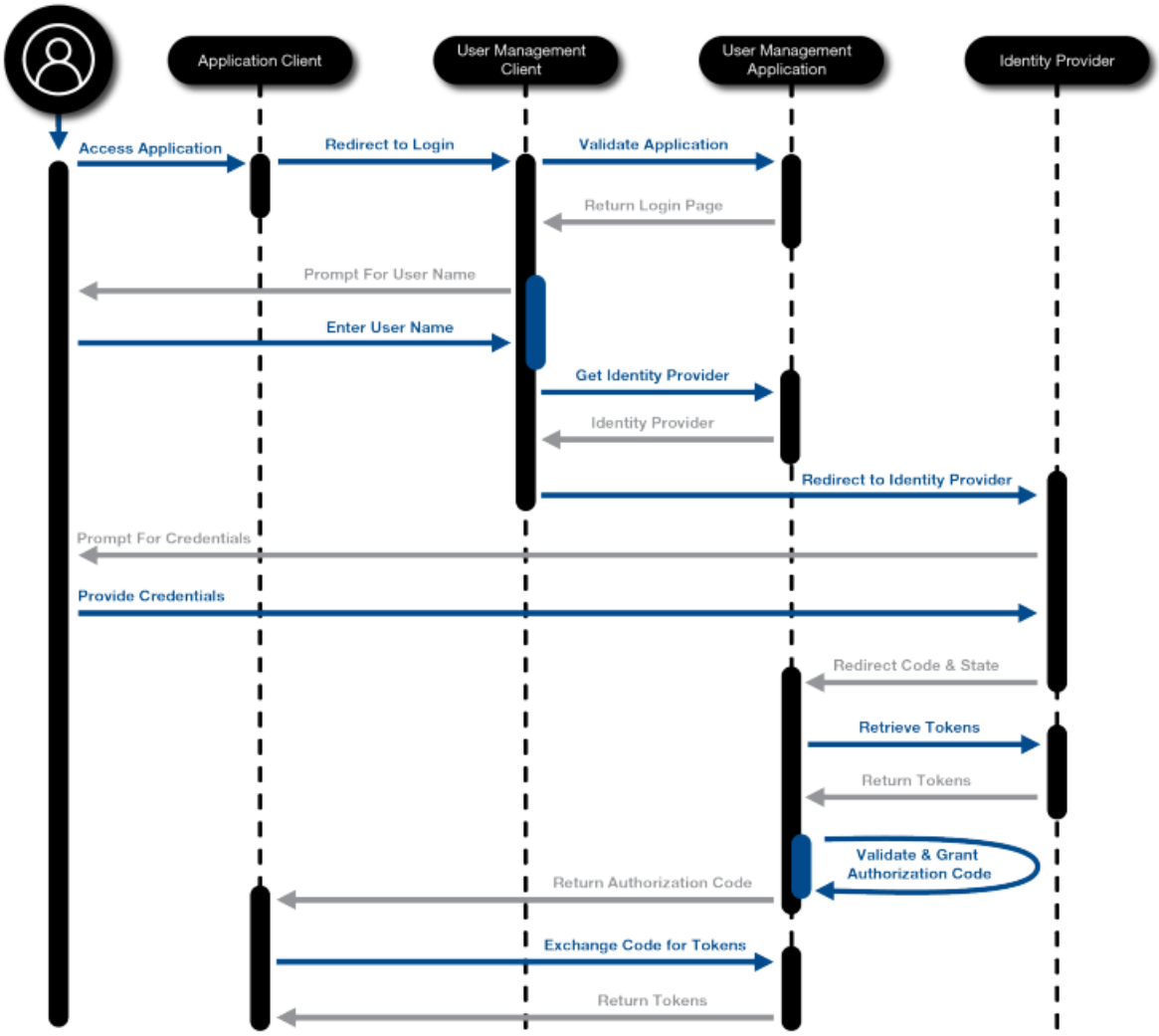
1. Unauthorized user signs in to an application and is redirected to the DFS User Management Application (UMA) sign-in page.
2. The UMA redirects the user to a Customer Identity Access Management (CIAM) solution.
3. The CIAM recognizes the user's domain and takes the user to the fueling operation's registered identity provider.
4. The external identity provider returns a SAML response to the CIAM.
5. The CIAM returns the authentication result to the UMA.

Local Authentication
With local authentication, the fueling operation creates an account. Operations that utilize their own IdP reserve a web address that becomes exclusive to them. New users can be invited to join an organization through the DFS User Management Application. As a member, users can create an account, reset a password and review and edit their profile.



1. A user who is not authorized to access DFS DX applications will be redirected to a UMA sign-in page.
2. The UMA redirects user to a CIAM solution.
3. The CIAM redirects authentication to an IdP that issues a response using the IdP's supported protocols or SAML.
4. The CIAM solution returns the authentication result to the UMA.

DFS DX Authentication and Authorization Sequence
During the DFS DX login process, several steps validate the authenticity of the user. During the authorization process, users are approved to access DFS DX applications that the fueling operation's IT admin has assigned the user to access.


Application Client
User Management Client
User Management Application
Identity Provider
Access Application
Redirect to Login
Validate Application
Return Login Page
Prompt For User Name
Enter User Name
Get Identity Provider
Identity Provider
Redirect to Identity Provider
Prompt For Credentials
Provide Credentials
Redirect Code & State
Retrieve Tokens
Return Tokens
Validate & Grant Authorization Code
Return Authorization Code
Exchange Code for Tokens
Return Tokens

Defining Permissions in a Connected Solutions Platform

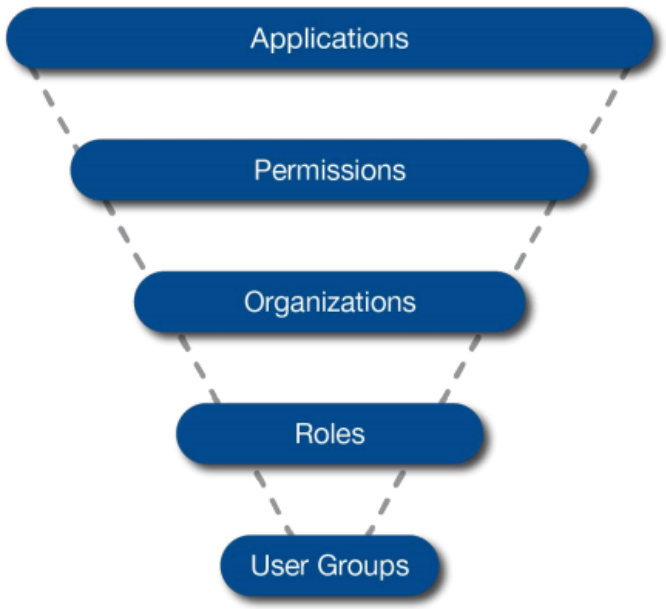
User management applications provide IT administrators of a cloud platform the tools they need to securely control their users' access and manage contact information. In some instances, though, parties outside your organization may need access to applications in order to perform managed services, such as wetstock monitoring. With that in mind, DFS DX is engineered to accommodate three primary models of user access:

- DFS DX manages all administrative actions and data analysis services on behalf of the fueling operation
- The fueling operation self-serves administrative actions and data analysis
- Managed services are delegated to a third party

A blend of these models is also possible. While DFS DX system administrators can facilitate access for delegated parties, DFS DX also enables an organization's IT administrator to provide controlled access to third parties through a series of key and token exchanges.

Controlling User Privileges

The DFS DX User Management Application controls user privileges at multiple levels:



Considerations for Meeting Data Privacy Compliance Standards

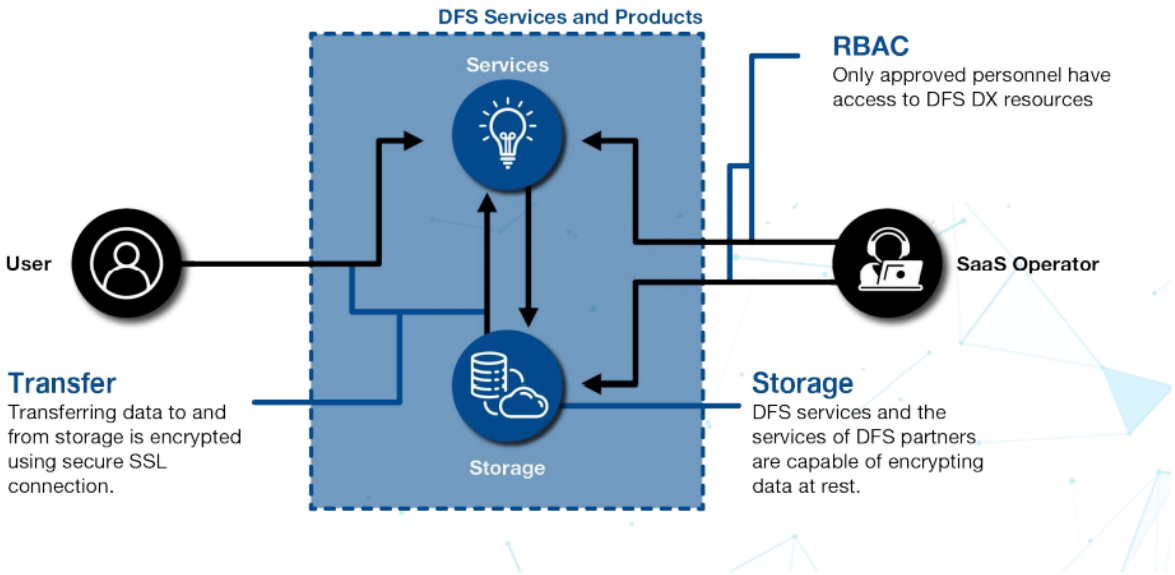
Data protection and privacy is foundational for a cloud-based platform to deliver on its value proposition to all fueling operation users — internal stakeholders, partners and consumers. Assurances need to be built into the system that it meets existing regulations such as the *California Consumer Privacy Act*, *New York SHIELD (Stop Hacks and Improve Electronic Data Security) Act* and the EU's General Data Protection Regulation. The platform must also be agile enough to seamlessly adapt to future requirements.

Leveraging the security features that have been integrated into Microsoft Azure, which has been engineered to facilitate updates for future data protections requirements, enables a cloud platform to prevent, detect and respond to security threats. These capabilities support secure scalability enterprise-wide.

While requiring users to agree to the fueling operation's privacy statement and use conditions is fundamental, Dover Fueling Solutions has incorporated additional measures into DFS DX to keep personal data secure.

DFS DX Data Protection Measures

With DFS DX, consumer data such as customer preferences and promotional interests are never stored with personally identifiable information. The information is stored using an irreversible hash of consumer references. For example, John Smith becomes user one, Sally Jones becomes user two, and so on. This approach allows the consumer to be uniquely identified for the purposes of providing a customized experience without being able to tie it back to any information that could compromise the consumer.



1. **Role-Based Access Control (RBAC):** Visibility of the data is only available to entitled operators
2. **Encrypting Data at Rest:** This approach ensures the data cannot be read by anyone who obtains a raw copy of the data or has a direct access to the data files
3. **Encrypting Data at Transit:** This measure protects the data being transferred between the data source and the party requesting the data
4. **Audit Logs:** Tracks who accesses the data and the purpose of accessing the data
5. **Security Incidents Management:** Meticulously defined processes, supported by SMS and email notifications that alert operators to security issues, empower quick intervention in the event of a personal data breach
6. **Privacy by Default:** Every new service and feature is reviewed in the context of being compliant with data privacy regulations

In Summary

Digital transformation is rapidly accelerating across all industries. Leveraging the capabilities of IoT and data-driven analytics to optimize an enterprise's assets will be a significant point of differentiation for fueling operations moving forward. An open, global and common cloud platform, such as DFS DX, makes this possible.

However, it is incumbent upon architects of a cloud-based interface to implement forward-looking security controls. These controls need to ensure the solution can meet both existing and future data privacy standards, while still delivering a frictionless user experience. By combining decades of fueling technology expertise with the cloud-computing services of Microsoft Azure, DFS established the industry's first pathway to intelligent fueling and retail operations. Through prescriptive authentication, authorization and compliance protocols, DFS DX provides the user management capabilities that fuel site operators and IT admins need to securely realize true digital innovation.

Begin Optimizing Your Assets Today

DFS DX has been engineered with ease of use and data security in mind. To learn more about DFS DX, including user interface considerations, upgrade procedures and after-sale support, submit an inquiry at https://www.doverfuelingsolutions.com/contact-us today.

About DFS DX

DFS DX is the industry's first open, global and common cloud platform that harnesses advanced analytics and IoT to deliver five core innovative solutions focused on customer experience and asset optimization. These five core solutions span wetstock management, remote asset monitoring, targeted advertising and media at the dispenser, fleet fueling site management, and point-of-sale management. These solutions empower fuel retailers to identify fuel loss in real-time, optimize dispenser uptime, increase sales through targeted advertising at the fuel dispenser, centrally manage point-of-sale solutions and control an entire fleet fueling enterprise from a single cloud-based interface.

About Dover Fueling Solutions

Dover Fueling Solutions ("DFS"), part of Dover Corporation, comprises the product brands of ClearView, Fairbanks, OPW Fuel Management Systems, ProGauge, Tokheim and Wayne Fueling Systems, and delivers advanced fuel dispensing equipment, electronic systems and payment, automatic tank gauging and wetstock management solutions to customers worldwide. Headquartered in Austin, Texas, DFS has a significant manufacturing and technology development presence around the world, including facilities in Brazil, China, India, Italy, Poland, the United Kingdom and the United States.