MarketDirect StoreFront® User Authentication White Paper

EFI Productivity Suite | *MarketDirect StoreFront User Authentication White Paper*

February 2019 MarketDirect StoreFront

Document Version 1.1

Patents

Trademarks

Table of Contents

About This Document

MarketDirect StoreFront® is EFI's Web-to-Print solution. MarketDirect StoreFront lets print service providers offer their products and services via the Web. This paper is intended to educate current and prospective customers about user authentication in MarketDirect StoreFront. The white paper assumes you have a technical background.

About User Authentication

User authentication is the process of restricting a system to authorized users. MarketDirect StoreFront offers the following methods for authenticating users:

- MarketDirect StoreFront internal authentication
- Active Directory Services authentication (available as a licensed option in two modes)
- Login bypass (available as a licensed option)

This white paper provides details of these user authentication options.

MarketDirect StoreFront Internal Authentication

What Is Internal Authentication?

Internal authentication is part of the core MarketDirect StoreFront product. A user enters a user name and password to log into MarketDirect StoreFront, and the system checks the login credentials against an internal list of user profiles on the MarketDirect StoreFront server. If the credentials are valid, the user is logged in and granted permissions based on the group to which he or she belongs, for example, administrators or operators. (This type of authentication is also known as "forms authentication.")

Passwords are SHA512 (Secure Hash Algorithm[1]) encrypted, and the use of a "strong" password can be enforced.

How Are Users Added?

Bulk import

Users can be added via a bulk import of a flat file. This import can take place periodically to add new users to the system. (An import adds new users without overwriting existing users.) A bulk import of users can include all their profile data including user passwords. User passwords are stored on the MarketDirect StoreFront server using SHA512 (Secure Hash Algorithm) encryption.

Self registration

If self registration is enabled in MarketDirect StoreFront, site visitors (print buyers) can create a user profile themselves.

Manual registration

Administrators can add new users to the system manually (on the Users page in MarketDirect StoreFront).

[1] Secure Hash Algorithm (SHA) is a algorithm developed by the National Security Agency (NSA) for use in the digital signature standard for encrypting information. To learn more about this standard, use the following link: http://en.wikipedia.org/wiki/Secure_Hash_Algorithm.

Who Should Use?

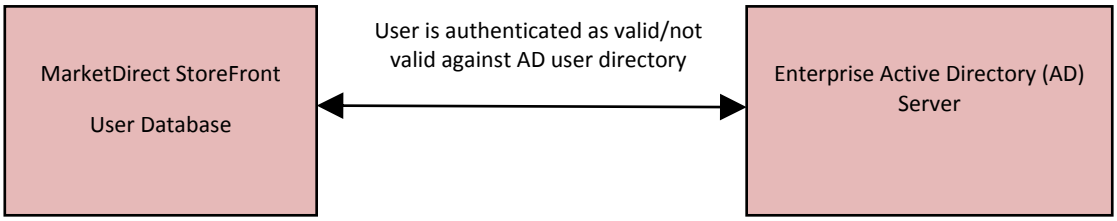
MarketDirect StoreFront internal authentication is ideal for sites that do not need to share information about MarketDirect StoreFront users with another system or to provide users with the ability to use single sign-on (SSO). No site setup is required.

Active Directory Authentication

What Is Active Directory Authentication?

MarketDirect StoreFront supports Active Directory (AD) authentication. When AD authentication is used with MarketDirect StoreFront, as users attempt to log into MarketDirect StoreFront, their credentials (user name and password) are verified against an authoritative directory on a trusted AD server. If the users are valid, they are logged into MarketDirect StoreFront with appropriate access and permissions.

Note MarketDirect StoreFront validates only that the user has access to his or her account in the AD database (by checking the user name and password).



Active Directory authentication supports single sign-on (SSO) which means that a user logs into one system and then has access to other systems without having to log into each system separately. With MarketDirect StoreFront SSO, when a user is logged in on a Windows system via Windows authentication, as soon as the user browses to the MarketDirect StoreFront site or clicks an SSO button, he or she is automatically logged into MarketDirect StoreFront.

In MarketDirect StoreFront, Active Directory authentication is a licensable option (**Authentication Pkg: LDAP and Login Bypass** must be selected on the License page).

Active Directory authentication is available in two modes:

- Site-level Active Directory authentication.
- Active Directory Services with Federated Identity Services for site or company-level authentication.

Site-level Active Directory Services authentication

This mode of authentication can be used only on customer-hosted (standalone) MarketDirect StoreFront installations. Cloud-hosted installations must use Active Directory Services with Federated Identity Services authentication as described on page 7.

When site-level Active Directory authentication is used, MarketDirect StoreFront communicates with an enterprise-wide Active Directory (AD) server in the same domain/network as the MarketDirect StoreFront server. The AD server contains a directory of user information and associated privileges. When users attempt to log into MarketDirect StoreFront, their credentials (user name and password) are verified by the AD server, which in turn communicates the information on the users to MarketDirect StoreFront.

Who should use?

Site-level Active Directory authentication is ideal for customer-hosted (standalone) sites that want to provide users with the ability to use single sign-on (SSO) and are authenticating users against a single AD server *in the same network* as the MarketDirect StoreFront server. For example, a university print shop wants students, staff, and faculty to access the print shop site with their university login credentials (SSO).

How is it set up?

Site-level Active Directory authentication is configured in the Site Settings in MarketDirect StoreFront: **Site Settings > Authentication > Directory Services Authentication**. After you click **Directory Services Authentication**, you can configure the authentication and perform the profile field mapping between Active Directory and MarketDirect StoreFront. (For examples of profile field mapping, see page 10.)

For SSO, you must also configure the LDAP AUTH application in IIS.

For information about implementing site-level Active Directory authentication in MarketDirect StoreFront, refer to online Help while on the administration side of MarketDirect StoreFront.

In addition, note the following:

- You must be licensed for authentication. (The integration option **Authentication Pkg: LDAP and Login Bypass** must be selected on the License page in MarketDirect StoreFront.)
- You must be using an Active Directory compliant server for managing user information.
- MarketDirect StoreFront must be customer-hosted (not in the cloud, hosted by EFI).
- MarketDirect StoreFront must be configured for Directory Services Authentication (as described in online Help).
- MarketDirect StoreFront supports the following service types (protocols): LDAP, LDAPS, ADSI, NDS, and NWCOMPAT. When you configure site-level Active Directory authentication, you select one of these types.

  Notes When LDAP or ADSI service is configured, MarketDirect StoreFront uses the Microsoft-provided .NET Active Directory service provider found in the System.DirectoryServices namespace to communicate with the directory service provider. These services authenticate both user name and password against an AD; require the domain name or IP address of the AD server; require a valid base DN (distinguished name) – the directory within the directory server where a user search starts; and require the MarketDirect StoreFront server to be in the domain.

  When NDS or NWCOMPAT service is configured, the AD is pre-appended to a directory bind, and the AD user name is used along with the password to do the bind.
- The AD server must give access rights to the server on which MarketDirect StoreFront is located.
- The MarketDirect StoreFront server must be part of the customer's domain.
- Multiple domains are supported – when logging in, users just select their domain from a dropdown list.
- Port 389 is required when communicating with an AD server.
- When site-level Active Directory authentication is enabled, the authentication can be done using either or both of these methods:
  - Users are logged into Windows and use the SSO MarketDirect StoreFront URL (or click an SSO button). This automatically logs them into MarketDirect StoreFront.
  - Users provide their user credentials when logging into MarketDirect StoreFront, and AD authenticates the credentials.

  Note If a user self-registered, AD authentication will not occur.

Active Directory Services with Federated Identity Services Authentication

This mode of authentication can be used on both customer-hosted and cloud-based (EFI-hosted) installations of MarketDirect StoreFront.

Important This authentication mode is supported only on SmartStores, not classic storefronts. It is also not supported with PrintMessenger.

When Active Directory Services with Federated Identity Services authentication is being used, MarketDirect StoreFront communicates with one or more Active Directory Federation Servers (ADFS) that contain a directory of user information and associated privileges. When users log into MarketDirect StoreFront through, for example,

a company-branded URL, their credentials are authenticated against the appropriate ADFS, which in turn communicates information on the user to MarketDirect StoreFront.

Note Two federation protocols are supported: WS-Federation and SAML 2.0. The SAML 2.0 protocol supports Shibboleth, an open source federated identity solution.

Cloud-based sites have the option of providing single sign-on (SSO) capability and authentication at the *company* level with each company pointed to its own ADFS.

Important To use Active Directory Services with Federated Identity Services authentication, *you must set up and configure your own Active Directory Federation Server (ADFS)*. EFI will not assist with the setup of ADFS nor provide support for it. If you are using a Microsoft solution (WS-Federation protocol), contact Microsoft. For SAML 2.0 and Shibboleth, go to http://www.shibboleth.net.

Who should use?

Active Directory Services with Federated Identity Services authentication is ideal for cloud-based sites that want to provide users with the ability to use single sign-on (SSO) at the company level, with each company pointed to its own ADFS. For example, a commercial printer has two or more company-branded sites and wants users associated with those companies to be able to log into the company-branded storefront with SSO. In this model, each company can have its own ADFS against which company users are authenticated.

For customer-hosted sites, ADFS authentication allows *cross-network* authentication.

How is it set up?

Before you can configure Active Directory Services with Federated Identity Services authentication in MarketDirect StoreFront, you *must set up and configure your own Active Directory Federation Server (ADFS)*. EFI will not assist with the setup of ADFS nor provide support for it. If you are using a Microsoft solution (WS-Federation protocol), contact Microsoft. For SAML 2.0 and Shibboleth, go to http://www.shibboleth.net.

You can then configure the authentication in the Site Settings in MarketDirect StoreFront: **Site Settings > Authentication > Federated SSO**. After you click **Federated SSO** and select your Federation protocol, you can then configure the authentication on a site or company-level and perform the profile field mapping between ADFS and MarketDirect StoreFront. (For examples of profile field mapping, see page 10.)

What Are the Advantages of Active Directory Authentication?

Regardless of the mode you are using (site-level Active Directory or Active Directory Services with Federated Identity Services), Active Directory authentication offers the following advantages:

- Makes it easier for users to access MarketDirect StoreFront since they can log in with their domain credentials or via Single Sign On (SSO). Different login credentials are not required.
- With MarketDirect StoreFront SSO, when a user is logged in on a Windows system via Windows authentication, as soon as the user browses to the MarketDirect StoreFront site or clicks an SSO button, he or she is automatically logged into MarketDirect StoreFront.
- Users are automatically associated with the correct company and department in MarketDirect StoreFront if this information is in AD.
- No separate registration process is necessary in MarketDirect StoreFront.
- User information is managed in a single place (AD) so maintenance is simpler.

What MarketDirect StoreFront Active Directory Authentication Does

- When a user logs into MarketDirect StoreFront via Active Directory (AD) for the first time, a MarketDirect StoreFront user profile (account) is automatically created. This involves copying information from the AD user fields to the MarketDirect StoreFront user profile fields. (For this to work the MarketDirect StoreFront user profile fields must be mapped to the AD user fields. For some examples of mapping, see below.)

  Note Users can still register themselves manually in MarketDirect StoreFront when AD authentication is enabled, but the manually-created profile will not be authenticated against AD.

- When a user logs into MarketDirect StoreFront, LDAP authentication verifies his or her user name against the AD server to make sure that the user is valid.
- AD authentication prevents someone from logging into MarketDirect StoreFront if he/she was deleted or made inactive in the AD user database.

- AD authentication prevents someone from creating a new user profile if he/she was deleted or made inactive in the AD user database.
- If a user's AD profile changes, the MarketDirect StoreFront user profile fields are automatically updated when the user next logs into MarketDirect StoreFront. For example, if a user's address changes, it will be automatically updated in MarketDirect StoreFront.

How User Field Mapping Works

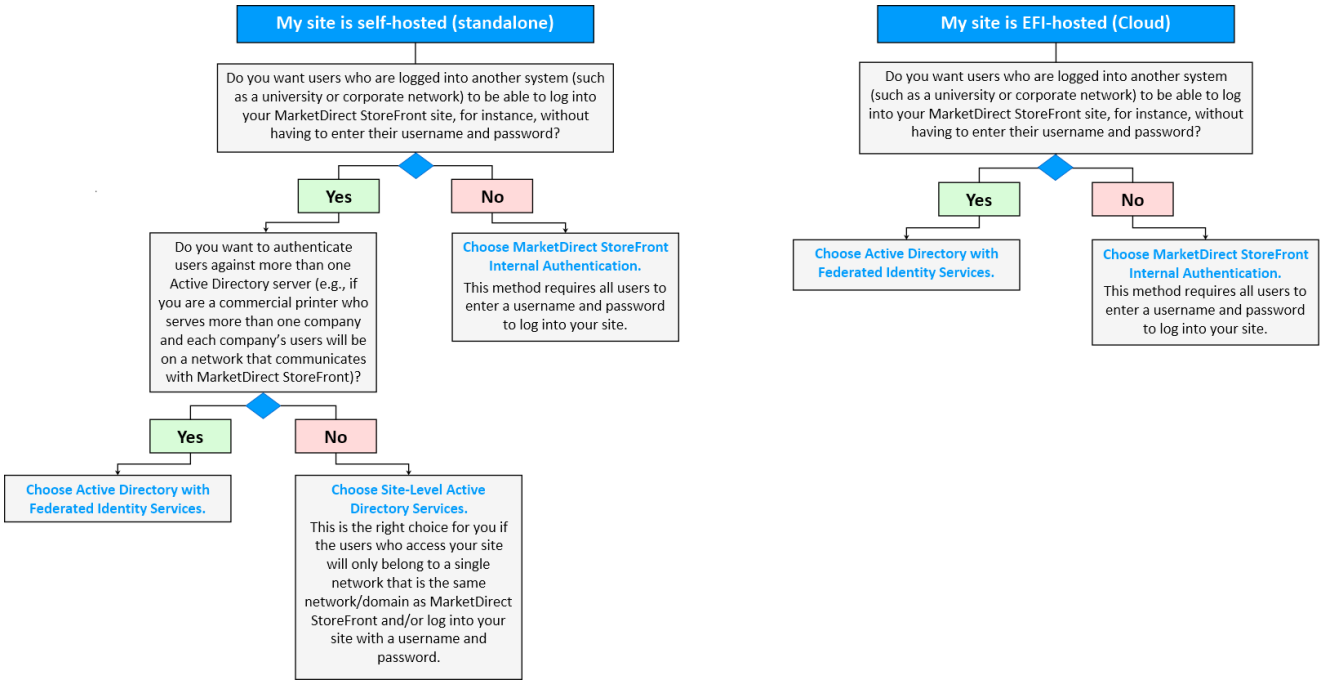
As part of configuring Active Directory authentication in MarketDirect StoreFront, you map fields in the user profile fields in MarketDirect StoreFront to AD user profile fields (attributes). This makes it possible for information to be copied from the AD fields to the user profile fields in MarketDirect StoreFront. Here are some examples of mapping:

MarketDirect StoreFront User Profile Field	AD User Profile Field
First Name	**givenName**
Last Name	**sn**
Email	**mail**
Company	**company**
Department	**department**
Country	**c**
Title	**title**
Address 1	**streetAddress**
State	**st**
Zip/Postal Code	**postalCode**
Phone Number 1	**telephoneNumber**

Note For information about mapping these fields, see online Help on user authentication while on the administration side of MarketDirect StoreFront.

Which Authentication Method Is Right for You?

The following diagram may help you decide which authentication method will best suit the needs of your organization.



Login Bypass

What Is Login Bypass?

Login bypass allows print buyers to avoid the MarketDirect StoreFront home/login page. Here the print buyer's login credentials are obtained from an external system and the buyer is logged into MarketDirect StoreFront automatically. This is accomplished by a token and password being sent via a POST request to the MarketDirect StoreFront server.

Note The user's (print buyer's) Windows/domain login does not interact in *any* way with the login bypass functionality. For login bypass to work, the user must arrive at MarketDirect StoreFront from another Web page that passes the login credentials.

Who Should Use?

Login bypass is ideal for customers who have multiple sites but no central authentication server such as Active Directory.

Important Login bypass is designed for advanced users who are proficient in working with Web applications or for site that have an IT staff capable of configuring and managing login bypass.

How Is It Set Up?

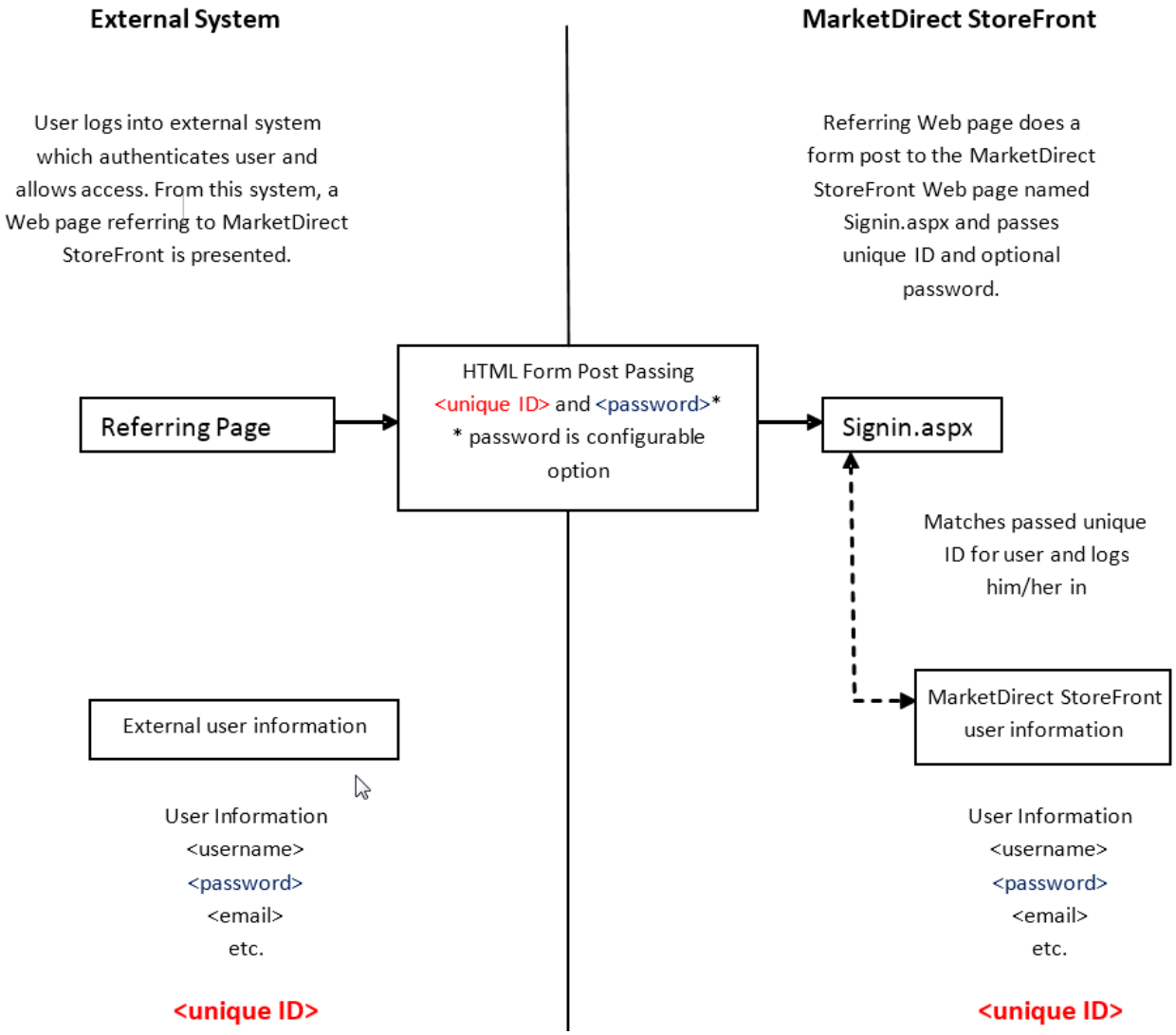
You must be licensed for login bypass. (The integration option **Authentication Pkg: LDAP and Login Bypass** must be selected on the License page in MarketDirect StoreFront.)

For login bypass to work, database synchronization between your system and the MarketDirect StoreFront user database is required.

Token Posting

The user profile in MarketDirect StoreFront includes a **SSOToken** field. This field can contain a unique ID value that matches a unique ID value in your user database(s). When this ID is passed (via form post) to a special MarketDirect StoreFront page (signin.aspx), MarketDirect StoreFront matches the ID to the field in the MarketDirect StoreFront user table and logs in the associated user.

A password can be required for an additional level of security. (PermitEmptyPasswordSSO in the MarketDirect StoreFrontConfiguration table can be set to True or False.)



Initial Setup

During initial setup, users (print buyers) must be bulk imported into MarketDirect StoreFront to synchronize the user information between MarketDirect StoreFront and your external user management database.

Connecting Your System to MarketDirect StoreFront

Your system (the external system) must include a Web page that passes the login credentials to MarketDirect StoreFront. The sample HTML pages that follow illustrate how you can modify your system/Web applications to bypass the login to MarketDirect StoreFront.

HTML File Samples

Below are two HTML examples.

Important The referring page must include the SITEGUID in the URL and this SITEGUID must match the SITEGUID on the **Administration > Site Settings > About** page.

Sample page with a submit button

```
<html>
<body>

<form id=Form1 action="http://brogers2k/dsf/signin.aspx" method="post">

    <input type="text" name="token" id="token" />
    <input type="text" name="pwd" id="pwd" />
    <input type="submit" />

</form>

</body>

</html>
```

Sample page with a link (using a hidden form to submit)

```
<html xmlns="http://www.w3.org/1999/xhtml">

<head>

    <title>MarketDirect StoreFront</title>

    <script language="javascript" type="text/javascript">

            function Login() { document.getElementById("Form1").submit(); }

    </script>

</head>

<body>

    <a href="javascript:Login()">LoginByPass</a>

    <form id="Form1" action="http://dsfserver/DSF/signin.aspx? SITEGUID=c9c70a5c-95ef-40c9-b5b5-

    5b2c891d3d84" method="post">

            <input type="hidden" name="token" id="token" value="LOGIN_BYPASS_USER_NAME" />

            <input type="hidden" name="pwd" id="pwd" value="LOGIN_BYPASS_PWD" />

            <!-- Example using blank password below (value="" when not sending

            password) -->

            <input type="hidden" name="pwd" id="pwd" value="" />

    </form>

</body>

</html>
```

How Are Users Added?

Bulk import

Users can be added via bulk import as well as during regular synchronization between your user database and the MarketDirect StoreFront one.

Self registration

Self registration can be enabled to allow site visitors (print buyers) to create a user profile themselves. Print buyers who register themselves, however, will not be able to use login bypass until the site administrator edits their user profile to include an **SSOToken**. In addition, the print buyer must be coming from a referring Web page that is passing login credentials (unique ID).

How Do You Maintain It?

User synchronization

When using login bypass, your user database and the MarketDirect StoreFront user database must be synchronized. Users (print buyers) should be updated regularly using the MarketDirect StoreFront bulk import.

In some cases, EFI Professional Services can perform additional fee-based services to extend synchronization.

E-mail notifications

Unless buyers are expected to know their user names and passwords, EFI recommends that e-mail notifications (including for approval workflows) are turned off when using login bypass.

Security Issues

Encryption

User passwords are one-way SHA512 (Secure Hash Algorithm) encrypted on the MarketDirect StoreFront server. You may, however, have encryption and security standards for all servers and applications within your environment. Be sure to identify such requirements to ensure that MarketDirect StoreFront can meet your implementation needs.

Site/page security

Because MarketDirect StoreFront uses a unique page that serves only to look up the customer ID and bypass the MarketDirect StoreFront home page, security and access to that page can be controlled via Internet Information Server (IIS) just like any other Web application. For example, IP filtering can be used to ensure that only users in a certain network can access MarketDirect StoreFront.