WatchDox by BlackBerry

Authentication and Identity Connectors

Flexible options give enterprises the luxury of choice

No enterprise security strategy or solution is complete without authentication. Managing and authorizing hundreds of user identities across disparate systems presents a formidable challenge for any IT organization. WatchDox® by BlackBerry® recognizes that authentication and identity management should not be a deterrent to adopt new technology. Thus, we make it easy for enterprises to adopt WatchDox by providing self-provisioning methods out-of-the-box or by integrating with existing systems to align with current policies.

Start Collaborating Now

WatchDox provides two default self-provisioning authentication methods to allow users to immediately start securely sharing files with WatchDox:

1. Username-Password

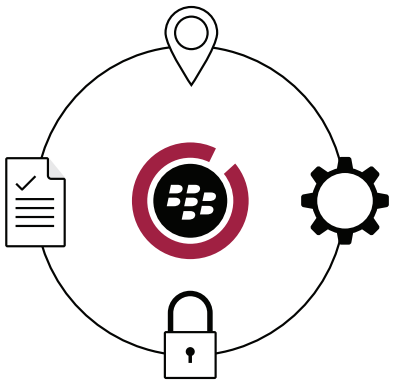
The user can create his account through the main login screen. An email link is sent for validation. A security certificate is exchanged on the backend to prevent the user from having to re-authenticate every time he enters the system. The user must authenticate with every new device he is using to access WatchDox.

Password complexity and lockout policies can be set by the system administrator. Parameter settings include:

- Minimum and maximum length
- Minimum and maximum lowercase characters
- Numbers
- Special symbols
- Wrong entry attempts
- Days before re-authentication
- Secret questions for password recovery
- Blacklist: Words that cannot be used

2. Email Authentication

The user is prompted to enter an email address. Like username and password, an email with a validation link is sent to the user.



Connectors for Your Existing Authentication Systems

Integrating with existing identity management systems makes it easy for enterprise IT to provision users in WatchDox and for users to utilize existing corporate credentials to access the system and quickly start sharing files.

The WatchDox Enterprise Edition allows enterprise organizations integration with Identity Connectors using SAML (Security Assertion Markup Language) and OAuth.

Supported enterprise authentication solutions for a Single-Sign-On experience include:

1. Active Directory (Kerberos)
2. Active Directory Federated Services (ADFS) via SAML 2.0
3. Third party authentication solutions that integrate via SAML 2.0
4. Third party authentication solutions that integrate via OAuth 2.0

CONNECTORS FOR YOUR EXISTING AUTHENTICATION SYSTEMS

WatchDox is the only enterprise file sharing solution that presents the option for mixed-mode authentication. Mixed-mode authentication allows companies to share files with different groups of users by defining different ways to enroll and authenticate them.

In the course of conducting business, corporate relations are constantly in flux – alliances develop, partnerships grow, projects end and companies divest. As such, the only way to address the complex relationships enterprises have with end users is to control how to authenticate them.

With mixed-mode authentication, for example, a company can implement the following authentication scheme:

USER GROUP	AUTHENTICATION METHOD
Employees (internal) Defined full-time workspace owners	Active Directory
Supplier A (external) Defined part-time collaborators	SAML-based single sign-on
Supplier B (external) Undefined project-based team visitors	Default email authentication

This feature eliminates the need for companies to go through the hassle of temporarily adding part-time contractors to Active Directory. Likewise, business transactions need not be delayed as a result of an undefined supplier being unable to access product designs from the internal system. Only authorized individuals should have access to your company's corporate data. With mixed-mode authentication, that can easily be enforced without burdening IT.

Technology Partnerships

WatchDox has successfully implemented integrations with the following providers (more to come):

Learn more at **www.blackberry.com/watchdox**