

Protecting Microsoft SharePoint Services with Ubiligin SSO

CHALLENGE

Microsoft SharePoint Services provides an invaluable tool to share information across the enterprise. Extending the SharePoint Services to include partners provides an excellent method of collaborating on-line 24/7.

The current generation of SharePoint Services can utilize either token based (IIS) or claims based (.NET) authentication. With claims based authentication there's no need to save the user information to the local Active Directory. With token based authentication you must have the same user documented perhaps in several places.

The content that is available through SharePoint Services may vary greatly.

SOLUTION

Ubiligin can provide over 20 different authentication methods to protect SharePoint Services. If highly confidential data is shared between partners, companies may benefit from the authentication mechanisms. Among the supported methods are strong authentication using a smart card, USB-token, soft certificate, one-time-passwords, mobile certificates and mobile one-time-passwords etc. Simple password is an insecure authentication method, which should not be used to protect very confidential information of the company. Passwords also require administration efforts as the users will forget them and administrators are required to reset them on regular basis

Deploying the Ubiligin Integration Solution for Microsoft SharePoint Services, can improve security and provide companies' ways to offer proper authentication that corresponds to the actual confidentiality

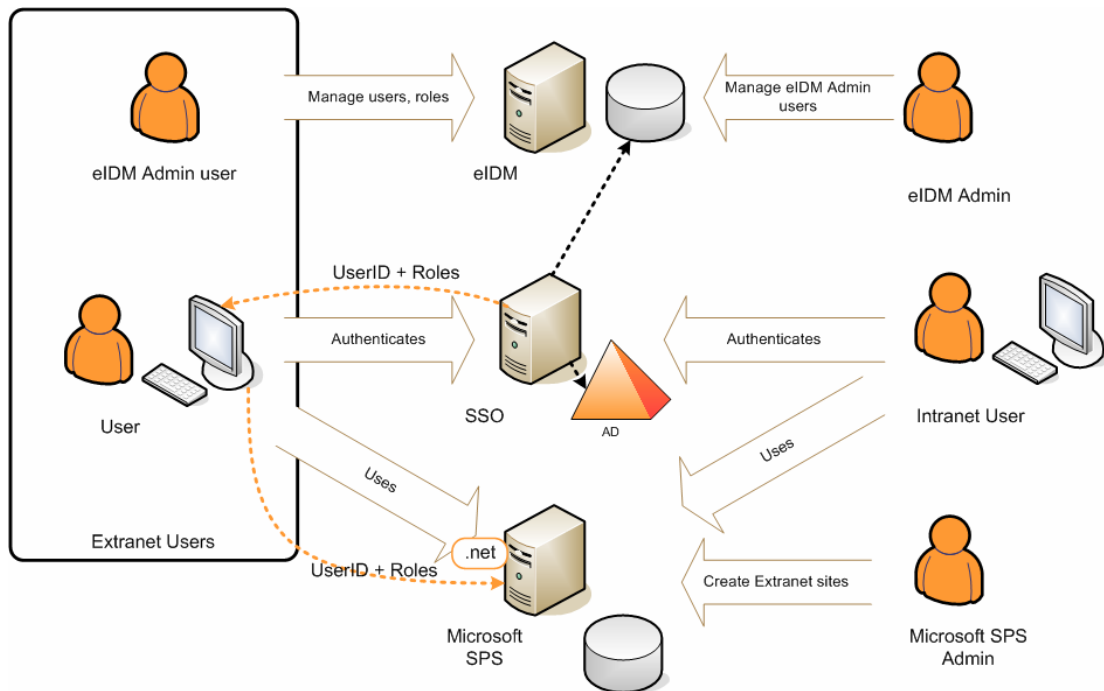
Sometimes it is necessary to use these services to share information between different units within an organization. More often the SharePoint Services is utilized to collaborate between two different companies. The confidentiality level of the information stored in SharePoint therefore varies and proper action should be taken to ensure that only those who have the right to use the information, can access it.

Microsoft SharePoint Services currently offer decent authentication options and even some workflow based identity management features. However, these features are not available for other applications in the organization.

level of the information. Ubiligin is easy to deploy and does not introduce any additional performance requirements to the servers. Ubiligin Web Agents also provide Single Sign-On and the possibility to relay authorization data to the applications. For flexible partner connections, Ubiligin provides out-of-the-box federated SSO to the partners' Windows domain.

Ubiligin mobile authentication can be used to effectively minimize the risk of phishing attempts. Mobile authentication separates the actual user authentication to another channel, mobile phone network and thus prevents any phishing or other identity theft attempts.

When combined with Ubiligin eIDM solution, the Ubiligin product family can deliver better identity management features and even enable completely outsourced extranet user management with extensive features in RBAC and intuitive workflows for the end users in the business ecosystem.



BENEFITS

- Secure access to SharePoint Services
- Proper authentication to protect the information
- Enhanced productivity through better information availability
- Audit trails for regulatory compliance
- Easy and cost efficient deployment
- Federated Single Sign-On to the partners' Windows domain
- Single Sign-On to all Web services protected by UbiLogin Web Agents
- Outsourced extranet identity and authorization management with UbiLogin eIDM
- Mobile authentication that can prevent phishing attempts

UbiLogin cost effectively enhances SharePoint Services security and enables employees' and external users' secure access to the confidential company information for which they are authorized. UbiLogin's advanced authentication methods can be used to obviate current Internet threats. Outsourced extranet identity management and Single Sign-On can lower operating costs and provide quick ROI