

## Protecting Microsoft Outlook Web Access with Ubilogin Application Integration Solution for Outlook Web Access

### CHALLENGE

**Microsoft Exchange and Outlook Web Access** provide employees web-based access to e-mail, calendar, task and other information stored in the Microsoft Exchange servers. Outlook Web Access is used to grant access to e-mail for the traveling users, outside the company intranet, or sometimes even from the intranet.

In small companies the Microsoft Exchange servers are usually standalone servers, where as in larger companies they are configured as front-end and back-end servers. This improves security as the front-end servers act as a first point of authentication for the Exchange. Back-end servers' databases include the e-mails, contact information and so on.

As Outlook Web Access provides a convenient way to access e-mails and other personal information, it also leaves the door open to uninvited guests, if not properly

protected. E-mail is the number one tool to exchange information, even classified, in companies. The Inboxes of employees include highly confidential data, and in most cases even company confidential data. This means that the access to this information should be granted to only those who are authorized to view it.

Microsoft Exchange provides some authentication mechanisms for the users, but unfortunately lacks strong authentication and mobile authentication. Due to the nature of Outlook Web Access, it is broadly deployed for users that are traveling and accessing the information outside the company intranet from locations and possibly computers which security settings cannot be confirmed. Because of this, it is utmost important that proper security measures are implemented to protect the confidential information of the employees and the company.

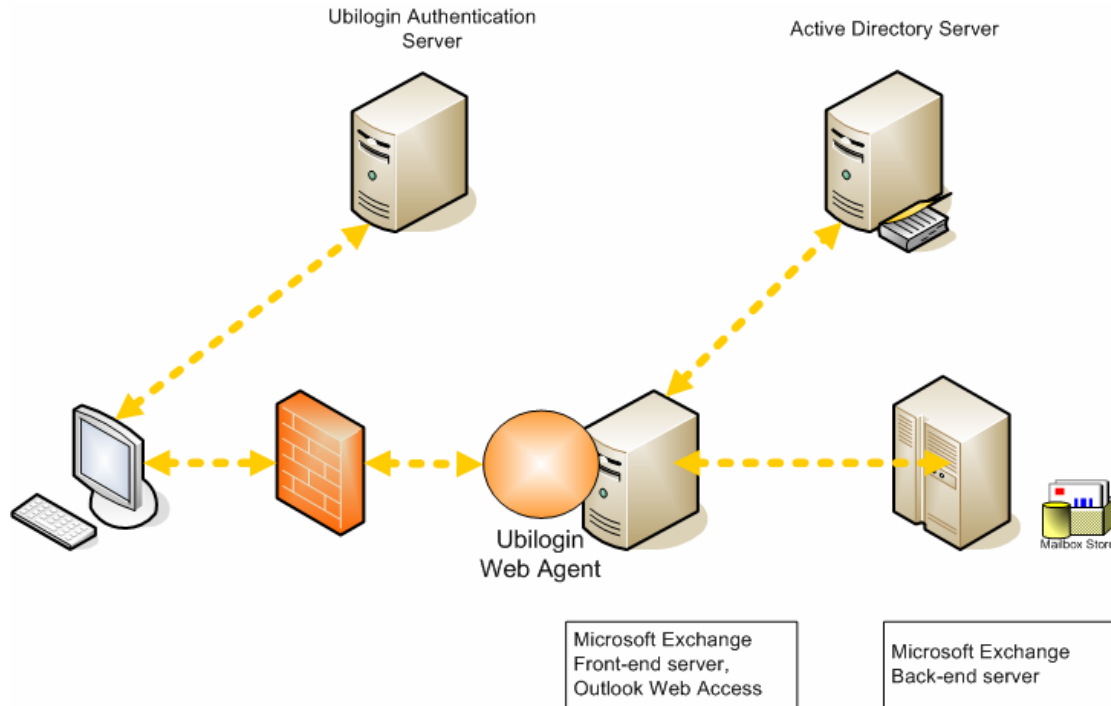
### SOLUTION

**Ubilogin** can provide over 20 different authentication methods to protect Outlook Web Access. 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. Normal password is an insecure authentication method, which should not be used to protect confidential information of the company. Passwords also require additional administration efforts as the users will forget them and administrators are required to reset them on regular basis

Installing Ubilogin Web Agents in the Microsoft Exchange server that the users first connect to improves the security and provide companies with ways to offer proper

authentication, corresponding to the confidentiality level of the information. Ubilogin components are easy to deploy and they do not introduce any additional performance requirements to the servers. Ubilogin Application Integration Solution for Outlook Web Access provides also Single Sign-On and the possibility to relay authorization data to the applications.

Mobile authentication is one of the methods Ubilogin provides and 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.



## BENEFITS

- Secure Web access to e-mail and other personal information
- Proper authentication to protect the information
- Mobile authentication that prevents phishing attempts
- Cost savings through reduced password resets
- Enhanced productivity through better information availability
- Single Sign-On to all Web services protected by Ubilogin Web Agents
- Easy and cost efficient deployment

**Ubilogin enhances Microsoft Exchange and Outlook Web Access security cost effectively and provides employees with secure access to their personal and company confidential information. Ubilogin's advanced authentication methods can be used to fight current Internet threats. Reduced password resets and Single Sign-On lower operating costs and provide quick ROI.**