



Identity and Access Solutions for BlackBerry Enterprise Server

Enhance BlackBerry Enterprise Server. Reduce Costs. Increase Security. Improve Service.

■ The Challenge

Mobile devices and smartphone technology are essential for enterprises looking to improve employee productivity, accessibility and responsiveness in today's economic environment. However, this increased flexibility and access can present problems for security and administration. As smartphones have taken on greater relevance, so too has the need to manage identity and security for mobile devices.

Given enterprise data is such a valuable corporate asset, ensuring its integrity is essential to any organization. Mobile devices that let users tap into corporate e-mail, instant messaging, voicemail, wireless networks and enterprise applications not only pose a risk to security, but can substantially increase the workload of IT administrators.

■ The Solution

Oxford Computer Group (OCG) provide solutions that use Microsoft Forefront Identity Manager (FIM) to manage BlackBerry® identity and security by integrating with BlackBerry® Enterprise Server (BES), the management solution for BlackBerry®. This allows secure access for Blackberrys to be managed through an integrated solution in the same way as other enterprise systems.

To complement FIM, OCG has developed a .NET-based Management Agent for BES (BES XMA). This provides added functionality and tighter integration between FIM and BES. The integration of BES XMA helps increase IT productivity and reduce administrative overheads by enabling centralized control and management of user accounts and mobile devices.

With this solution you can:

- Provide a central point of administration for BlackBerry® that's integrated with your existing enterprise systems and directories
- Enforce your company's BlackBerry® security policies with workflow and approval
- Automate the creation and removal of BES user accounts for Microsoft Exchange, IBM Lotus Domino, Novell GroupWise, or MDS Applications depending on an approval workflow
- Automatically send notification emails to BES administrators depending on an approval workflow
- Reset passwords for BES user accounts and BlackBerry® devices
- Reset BlackBerry® devices to their factory settings depending on an approval workflow

■ Identity Management with BlackBerry® in the Enterprise

When managing user accounts, it is vital to provide the right access to the right systems at the right time, while maintaining appropriate security and auditing activities. For organizations with BlackBerry® devices, the BlackBerry® Enterprise Server (BES) software provides a secure, centrally-managed link between their users' BlackBerry devices and the organization's enterprise systems, applications and wireless networks. But if an organization does not have a structured approach to the creation, management and synchronization of its identity and access data, then managing its mobile devices will pose a significant administrative burden.

OCG provides Identity and Access (IDA) solutions based on Microsoft Forefront Identity Manager (FIM). These solutions deliver a system of procedures, policies and technologies designed to manage the lifecycle and entitlements of your organization's digital identities. By combining the power and flexibility of FIM with OCG's FIM connector for BES, OCG can extend an IDA solution to BES in order to simplify and secure the administration of mobile devices across your organization.





The Benefits of Integrated IDA

Solutions for identity and access can:

- Simplify administration by creating a single point of access for the management of identity data
- Ensure all systems are provided with accurate and up-to-date identity data that consistently conforms to your organization's data conventions
- Reduce licensing and administration costs and improve productivity through the implementation of automated, workflow-enabled processes for account creation, deletion and management
- Provide self-service password management to increase staff productivity and reduce security threats
- Improve security and reduce ownership costs by synchronizing users' sign-on credentials across systems and provide facilities for Reduced Sign-on or Enterprise Single Sign-on
- Further improve security by automatically removing those rights when they leave, or their role changes



- Enhance compliance with regulatory standards through improved traceability, audit and reporting of identity data and user management activity

These benefits can now be extended to BES as well.

Why FIM and Why OCG?

FIM will define and automate the process used to manage the entire lifecycle of your digital identities and their associated entitlements. It uses a meta-directory approach to provide identity synchronization, provisioning and credential management. At the same time it supports and maintains multiple identity stores to provide, clean, consistent identity data in each of the connected systems.

FIM's powerful end user self-service capabilities significantly improve an organization's ability to manage its Blackberry® accounts and devices. With FIM, end-users can easily perform self-service tasks such as requesting an Active Directory user account, an Exchange mailbox and a Blackberry®, as well as performing group and distribution list management with self-help tools integrated into a SharePoint-based console or directly in Microsoft Office Outlook. Once requests to authoritative sources are approved, FIM's synchronization engine can action them.

OCG combines the collective knowledge of internationally regarded IDA specialists with results driven solutions. Our unique approach has made us the chosen partner of some of the world's leading technology providers. It is also why we are the chosen implementer of FIM solutions for some of the world's best known brands.

Licensing and Delivery

The OCG BES XMA is licensed on the basis of a one-off payment, for which you receive the XMA and associated documentation and a number of days consultancy from OCG to help you with implementation of the XMA. An annual support agreement can also be purchased to provide you with updates and helpdesk support, should you need it.

Contact us today to discuss your requirements. OCG can help you realize the full potential of your BES investment.



Microsoft
GOLD CERTIFIED
Partner

2009 SECURITY SOLUTIONS
Identity and Secure Access
PARTNER OF THE YEAR
FINALIST

Microsoft
GOLD CERTIFIED
Partner

2008 ADVANCED INFRASTRUCTURE SOLUTIONS
PARTNER OF THE YEAR-WINNER
Active Directory

Oxford Computer Group UK
Bignell Park Barns
Chesterton, Oxfordshire OX26 1TD UK
Tel: +44 (0)8456 584425
Fax: +44 (0)8456 584426
Email: info@oxfordcomputergroup.com
www.oxfordcomputergroup.com

Oxford Computer Group North America
One Microsoft Way
Building 25, Room 1482
Redmond, WA 98052
Tel: +1 877 862 1617
Email: info@oxfordcomputergroup.com
www.oxfordcomputergroup.com

Oxford Computer Group Deutschland
Winterlestr. 10b
D-85435 Erding, Deutschland
Tel: +49 8122 892089-0
Fax: +49 8122 892089-99
Email: info@oxfordcomputergroup.com
www.oxfordcomputergroup.de

Oxford Computer Group BeNeLux
Sweelinkplein 9 (Unit 11)
2517 GK Den Haag, The Netherlands
Tel: +31 (0)70 36 21 627
Fax: +31 (0)70 36 21 677
Email: BeNeLux@oxfordcomputergroup.com
www.oxfordcomputergroup.com

About Oxford Computer Group

Oxford Computer Group (OCG) is an IT service company that specializes in identity and access management. With worldwide operations OCG has an enviable repository of expertise, solution components and training courses. OCG has deployed 400+ enterprise-wide identity and access solutions and our instructors have trained over 4000 people on Microsoft IDA technologies. We understand identity and access management – benefit from our experience and capability. Worldwide operations in North America, United Kingdom, Germany and BeNeLux