Forefront Identity Manager 2010 R2

NERCOMP

Alex Voysest
Solution Specialist – Identity Management
alex.voysest@microsoft.com

Christopher Irwin
Technology Solutions Professional – Identity & Security
cirwin@microsoft.com
Agenda

• Identity Management in Education
• Forefront Identity Manager 2010 Introduction
• FIM Demo
• FIM Solutions
• FIM Architecture and Topologies
• FIM Licensing Basics
• Resources
• Q&A
Identity Management Benefits

Scale: 1=very low, 2=low, 3=medium, 4=high, 5=very high

- Immediate deprovisioning on... 3.6 4.4
- Appropriate ID proofing... 3.7 4.2
- Track unauthorized activity 3.4 4.1
- Self-service 3.4 4.1
- Single affiliations source 3.4 4.1
- Immediate new-user enablement 3.2 4.1
- Reduced or single sign-on 3.3 4.0
- Immediate role change 3.0 3.9
- User access to off-campus... 3.3 3.9
- Scalable authorization and... 3.6 3.8
- Strong authentication 3.2 3.8
- Appropriate guest access 3.0 3.7
- Non-institutional user access to... 2.6 3.0
- Decentralize account management 2.3 2.6

Capability  Importance increment

© 2011 EDUCAUSE
## Microsoft’s Identity Offerings

<table>
<thead>
<tr>
<th>Microsoft Product</th>
<th>Functionality / Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Authentication, Authorization and more Standards Implemented: Kerberos, LDAP, X509</td>
</tr>
<tr>
<td>Active Directory Lightweight Directory Services</td>
<td>Authentication Standards Implemented: LDAP</td>
</tr>
<tr>
<td>Active Directory Certificate Services</td>
<td>Strong Authentication Standards Implemented: X509</td>
</tr>
<tr>
<td>Active Directory Federation Services</td>
<td>Web Single Sign-On; Claims-based Authentication Standards Implemented: WS-Federation; SAML</td>
</tr>
<tr>
<td>Forefront Identity Manager</td>
<td>Identity Provisioning</td>
</tr>
<tr>
<td>Windows Identity Foundation</td>
<td>Identity Processing APIs</td>
</tr>
<tr>
<td>Forefront Unified Access Gateway</td>
<td>Perimeter Authentication &amp; Authorization</td>
</tr>
<tr>
<td>Rights Management Services</td>
<td>Identity-based document protection</td>
</tr>
</tbody>
</table>
Forefront Identity Manager 2010

Credential Management
- Self-Service Password Reset
- Managing User Certificate and Smart cards
- Send notifications when certificates near expiration date

User Management
- Self-service, users manage their own personal data
- Provisioning of AD accounts from SIS, and sync attributes
- De-provisioning when users leave

Group Management
- Self-service group management tools
- Offline approvals for restricted or secure groups
- Automated group and distribution list updates

Role Management
- Generate Audit Reports
- Attestation
- Enforce Segregation of Duties
Evolution of Forefront Identity Manager

1997
- Acquired LinkAge Directory Exchange
- Active Directory

1999
- Acquired Zoomit Via
- Metadirectory Services

1999
- Identity Integration Server 2003

2003
- Identity Lifecycle Manager 2007

2005
- Acquired Alacris
- Identity Integration Server 2003

2007
- Identity Lifecycle Manager FP1

2007
- Identity Lifecycle Manager 2007

2008
- Identity Lifecycle Integration Server 2008

2008
- Identity Lifecycle Manager 2008

2010
- FIM 2010 AD FS 2.0

2010
- FIM 2010

2011
- FIM 2011
- Acquired Bhold technologies

Microsoft Forefront Identity Manager 2010 R2

Common Platform
- Workflow
- Connectors
- Logging
- Web Service API
- Synchronization

Group Management

Policy Management

Credential Management
- Web based password reset
- Reporting
- Enhanced performance
- Enhanced MA connectivity
- Role Management

User Management

Group & DL Management
- Office Integration for Self-Service
- Declarative Provisioning
- Workflow and Policy
- Support for 3rd Party CAs

Credential Management

Common Platform
- Workflow Connectors
- Logging
- Web Service API Synchronization

Workflow and Policy Support for 3rd Party CAs

User Management

Group Management

Policy Management

Web Service API Synchronization
Forefront Identity Manager 2010 R2

DEMO

Christopher Irwin
Technology Solutions Professional – Identity & Security
cirwin@microsoft.com
Provisioning, reconciliation and the common identity

Active Directory

Microsoft Forefront Identity Manager 2010

LDAP

Email

Integrated and federated common identity

Student Information System

Private Cloud
Private Cloud
- Exchange
- SharePoint
- Web Sites
- Line of Business Apps
- File / Print

Public Cloud
- PaaS
- SaaS
- Windows Azure
- Office 365

Public Cloud

Private Cloud

Public Cloud

LDAP

Active Directory

Active Directory

Active Directory
User Profile Management

• Allow users to manage identity
  – Create contractor
  – Update phone number
  – Change home address
  – Add missing information

• Workflow and policy driven
Group Management

- Group and distribution list management, including dynamic membership calculation in these groups and distribution lists based on user's attributes
- Self-service group and distribution list management
- Office integration allows users to manage group membership from within Microsoft Office Outlook® for maximum productivity
Improved Self-Service Password Reset

• Adds web-based password reset
• Supports password reset and registration from intranet or extranet via a web browser
• Support for non-domain-joined machines
• No ActiveX control required for browser-based reset
• Internet Explorer 9 support
• Firefox 4 support for password reset and registration portals *only*
• Simplify deployment and management experiences for password reset*

* Not included in beta
Self service password reset user experience

• Registration for self service password reset

![Password Reset Form](image-url)
Reporting

FIM 2010
- Current state of resources
  - People, Groups, Policy Rules, etc.
- Limited log of system state changes
  - Requests and Request History view

FIM 2010 R2
- Adds historical reporting for tracking changes to FIM-managed resources
  - Includes frequently-requested out of the box reports
  - Enables long term data retention
- Built on proven technology
  - Partnership with System Center Service Manager
- Extensible framework
<table>
<thead>
<tr>
<th>User Name</th>
<th>User ID</th>
<th>Operation</th>
<th>Attribute</th>
<th>Value</th>
<th>Requestor</th>
<th>Committed Time</th>
<th>Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colin Wilcox</td>
<td>{732d2…}</td>
<td>Remove</td>
<td>User</td>
<td></td>
<td>FIM Service</td>
<td>2/13/2011 01:22:00</td>
<td>{532aa…}</td>
</tr>
<tr>
<td>Colin Wilcox</td>
<td>{732d2…}</td>
<td>Remove</td>
<td>Display Name</td>
<td>Colin Wilcox</td>
<td>FIM Service</td>
<td>2/13/2011 01:22:00</td>
<td>{532aa…}</td>
</tr>
<tr>
<td>Colin Wilcox</td>
<td>{732d2…}</td>
<td>Remove</td>
<td>First Name</td>
<td>Colin</td>
<td>FIM Service</td>
<td>2/13/2011 01:22:00</td>
<td>{532aa…}</td>
</tr>
<tr>
<td>Colin Wilcox</td>
<td>{732d2…}</td>
<td>Remove</td>
<td>Last Name</td>
<td>Wilcox</td>
<td>FIM Service</td>
<td>2/13/2011 01:22:00</td>
<td>{532aa…}</td>
</tr>
<tr>
<td>Colin Wilcox</td>
<td>{732d2…}</td>
<td>Add</td>
<td>Manager</td>
<td>gfort</td>
<td>FIM Service</td>
<td>9/22/2006 08:55:28</td>
<td>{8457b…}</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Manager</td>
<td>samanthas</td>
<td>FIM Service</td>
<td>9/22/2006 08:55:28</td>
<td>{8457b…}</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Employee Type</td>
<td>FTE</td>
<td>FIM Service</td>
<td>9/22/2006 08:55:28</td>
<td>{8457b…}</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Employee Type</td>
<td>Contractor</td>
<td>FIM Service</td>
<td>9/22/2006 08:55:28</td>
<td>{8457b…}</td>
</tr>
<tr>
<td>Colin Wilcox</td>
<td>{732d2…}</td>
<td>Add</td>
<td>Manager</td>
<td>samanthas</td>
<td>FIM Service</td>
<td>5/2/2002 08:32:11</td>
<td>{126da…}</td>
</tr>
<tr>
<td>Colin Wilcox</td>
<td>{732d2…}</td>
<td>Add</td>
<td>Employee Type</td>
<td>Contractor</td>
<td>FIM Service</td>
<td>5/2/2002 08:32:11</td>
<td>{126da…}</td>
</tr>
<tr>
<td>Colin Wilcox</td>
<td>{732d2…}</td>
<td>Add</td>
<td>Display Name</td>
<td>Colin</td>
<td>FIM Service</td>
<td>5/2/2002 08:32:11</td>
<td>{126da…}</td>
</tr>
<tr>
<td>Colin Wilcox</td>
<td>{732d2…}</td>
<td>Add</td>
<td>User</td>
<td></td>
<td>FIM Service</td>
<td>5/2/2002 08:32:11</td>
<td>{126da…}</td>
</tr>
</tbody>
</table>

Colin is created in FIM in 2002 via a sync through HR. Samantha Smith is his first manager.

In 2006, Colin becomes a full-time employee and, as a result, gets a new manager, Garth.

In 2011, Colin leaves the company, and he is removed from FIM.
FIM Topology Choices

All Components
- Together
- All apart
- Combinations in between

SQL Clustering is supported

The FIM Portal may scale out

The FIM Service may scale out

FIM Synchronization Service may be separated from FIM Service

FIM Service may be separated from FIM Portal

Dedicated instance of the FIM Service may be used
FIM Service and Sync Separated

Client PC → Portal WebService (FIMService DB) → Sync FIM Synchronization DB
3 Tier – Load Balanced

Diagram showing a 3-tier architecture with load balancing.
# Forefront Identity Manager Licensing

<table>
<thead>
<tr>
<th>FIM SKU</th>
<th>Purpose</th>
<th>ERP-SELECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIM Server License</td>
<td>Required to run any of the FIM Server software (Sync, Service, Portal) on a Windows Server 2008 machine.</td>
<td>$3400</td>
</tr>
<tr>
<td>FIM Client Access License</td>
<td>Needed for each administrator, and for each user whose IDENTITY DATA will be managed by FIM. Required for FIM Solutions: Cert. Mgt; Role Mgt; Pwd Mgt; Portal</td>
<td>$4</td>
</tr>
<tr>
<td>FIM External Connector License</td>
<td>Can be used instead of CALs only for non-employees (students, alumni, parents). Need to assign an EC License to each FIM Server in your infrastructure.</td>
<td>$4200</td>
</tr>
<tr>
<td>FIM Server LIVE License</td>
<td>For your Live@edu or Office 365 (DirSync only)</td>
<td>$455</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>Required for each FIM Server or Database Server</td>
<td></td>
</tr>
<tr>
<td>SQL Server 2008</td>
<td>Database software</td>
<td></td>
</tr>
</tbody>
</table>

**Exercise:**

- **10,000 Students+Alumni**
- **1,000 Faculty+Staff**

- FIM Portal
- FIM Service
- FIM Sync
Reporting Architecture Overview

- Reporting in System Center Service Manager based on SQL Server Reporting Services
FIM 2010 Customers

Contra Costa Community College District

GRAND CANYON UNIVERSITY

Florence
Public School District One

CC

SABIS

Tulane University

TCG

PBCC

Pittsford Schools

HOOVER CITY SCHOOLS

NKU

Marion County Public Schools
Where Every Child Can Learn

Valdosta
Technical College
A College of Applied Science

Yesha Community College District
<table>
<thead>
<tr>
<th>Microsoft Product</th>
<th>Functionality / Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Authentication, Authorization and more Standards Implemented: Kerberos, LDAP, X509</td>
</tr>
<tr>
<td>Active Directory Lightweight Directory Services</td>
<td>Authentication Standards Implemented: LDAP</td>
</tr>
<tr>
<td>Active Directory Certificate Services</td>
<td>Strong Authentication Standards Implemented: X509</td>
</tr>
<tr>
<td>Active Directory Federation Services</td>
<td>Web Single Sign-On; Claims-based Authentication Standards Implemented: WS-Federation; SAML</td>
</tr>
<tr>
<td>Forefront Identity Manager</td>
<td>Identity Provisioning</td>
</tr>
<tr>
<td>Windows Identity Foundation</td>
<td>Identity Processing APIs</td>
</tr>
<tr>
<td>Forefront Unified Access Gateway</td>
<td>Perimeter Authentication &amp; Authorization</td>
</tr>
<tr>
<td>Rights Management Services</td>
<td>Identity-based document protection</td>
</tr>
<tr>
<td>Identity Need</td>
<td>FIM Capability</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Immediate deprovisioning on user</td>
<td></td>
</tr>
<tr>
<td>departure</td>
<td></td>
</tr>
<tr>
<td>Appropriate ID proofing confidence</td>
<td></td>
</tr>
<tr>
<td>Track unauthorized activity</td>
<td></td>
</tr>
<tr>
<td>Self-service</td>
<td></td>
</tr>
<tr>
<td>Single affiliations source</td>
<td></td>
</tr>
<tr>
<td>Immediate new-user enablement</td>
<td></td>
</tr>
<tr>
<td>Reduced or single sign-on</td>
<td></td>
</tr>
<tr>
<td>Immediate role change</td>
<td></td>
</tr>
<tr>
<td>User access to off-campus resources</td>
<td></td>
</tr>
<tr>
<td>Scalable authorization and authentication</td>
<td></td>
</tr>
<tr>
<td>Strong authentication</td>
<td></td>
</tr>
<tr>
<td>Appropriate guest access</td>
<td></td>
</tr>
<tr>
<td>Non-institutional user access to our resources</td>
<td></td>
</tr>
<tr>
<td>Decentralize account management</td>
<td></td>
</tr>
</tbody>
</table>
Resources

• Current FIM 2010 Resources

• FIM 2010 R2 Beta Documentation

• FIM 2010 Customer Evaluation Program registration

Alex Voysest: alex.voysest@microsoft.com
Christopher Irwin: cirwin@microsoft.com