Understanding Microsoft Forefront Identity Manager 2010

Planning Guide

Applies to: Microsoft® Forefront Identity Manager 2010 Release Candidate 1

Microsoft Corporation

Published: October 2009

Authors: Markus Vilcinskas, Lori Craw, Brjann Brekkan

Editor: Femila Anilkumar

Abstract

This paper provides an overview of the strategy for Microsoft® Forefront Identity Manager 2010, with a focus on the upcoming release of Microsoft® Forefront Identity Manager 2010 RC1, and the features and benefits delivered through Microsoft's approach.

Contents

Understanding Forefront Identity Manager 2010

Executive Summary

The Microsoft strategy for identity management delivers a comprehensive solution to manage identities, credentials, and identity-based access policies across Windows and heterogeneous environments.

Today, Microsoft® Identity Lifecycle Manager (ILM) 2007 provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. It provides identity synchronization, certificate and password management, and user provisioning in a single solution that works across heterogeneous systems. As a result, IT organizations can define and automate the processes used to manage identities from creation to retirement.

The next release of Microsoft Identity Lifecycle Manager, Microsoft® Forefront Identity Manager 2010 extends the functionality of ILM 2007. New features empower end users with self-service tools integrated in Office and Windows. Additional features allow IT organizations more control through a robust delegation model and business process framework. New capabilities improve operational efficiency by automating common identity lifecycle management tasks and empowering end-users with self-help solutions. For organizations that want or need a more customized approach, Microsoft is implementing FIM 2010 on common set of services that includes workflow, delegation, Web services APIs, and logging. These services can be utilized by customers and vendors to customize and extend the functionality of FIM 2010 to meet their specific needs.

This paper provides an overview of the strategy for Microsoft Identity Management, with a focus on the upcoming release of Microsoft® Forefront Identity Manager 2010, and the features and benefits delivered through Microsoft's approach.

Delivering on the Promise

Microsoft ILM 2007, the evolution of Microsoft Identity Integration Server (MIIS) 2003, for the first time brought together traditional identity management with certificate and smart card management into one offering. Prior to ILM 2007, customers had to purchase products from different vendors and manually integrate the two offerings.

Enabling comprehensive identity and access management in the enterprise, Microsoft® Forefront Identity Manager 2010 changes the current state of the art in identity management by delivering an integrated identity management solution across heterogeneous systems and serving audiences across IT professionals, end users, and developers. In response to customer feedback that current identity management tools place an undue burden on IT departments and help desks without meaningful tools for end users, FIM 2010 dramatically changes the identity

management landscape by delivering powerful self-service capabilities for Office end-users, rich administrative tools and enhanced automation for IT professionals and .NET and Windows SharePoint Services based extensibility for developers.

FIM 2010 provides organizations with unique solutions to manage user accounts and access-, password- and certificate-based credentials such as smart cards and identity-based policies across Windows and heterogeneous environments.

FIM 2010 delivers capabilities that focus on empowering end users, IT professionals, and developers; delivering agility and efficiency through integration, automation, and self-service; and increasing security and compliance through tools for policy management and easier deployment and management of strong credentials.

Realizing the Value of Identity Management

Today's IT enterprise must deliver identity and access management that is efficient, cost effective, and secure. The complexity of managing and securing users, devices, and services is increasing. Whether due to regulatory mandate or business growth, identity management becomes more complex, and does often not deliver as much business benefit as it could. To put Microsoft's strategy for overcoming these challenges in context, you should consider the following business issues and customer pain-points relating to identity management.

Managing Identities Must be Cost-Effective and Efficient

Nearly all organizations must manage identities, credentials, and resources across multiple directory trees and application-specific identity sources. Inefficient Identity management proves to be costly and inefficient for organizations.

Impact of inefficient identity management:

- **High cost.** Manual or semi-automated identity management is costly and error-prone, especially when custom homegrown solutions and scripts are included. When users cannot manage their own identity and access needs, they push those operations back to the help desk, application owners and other IT departments.
- **Custom-coded solutions can be costly and inflexible.** Custom-coded solutions can be brittle and will not easily adapt to new business demands without additional engineering effort. Their management becomes more inefficient because of the new expert systems, consoles, dashboards, and applications that IT administrators must learn.
- **Decreased IT Agility.** When administrative and compliance activities demand regular manual intervention, IT cannot focus on strategic initiatives like delivering better IT governance or optimizing business processes.

Identity Management Must Enhance Security

Ensuring that only authorized users can access business resources in a timely manner is difficult to accomplish and expensive, if users are confronted with an overwhelming number of different passwords, common tasks such as resetting a password, and interactions with helpdesk. In

general, identity management helps improving the level of protection of corporate assets if it provides a comprehensive and integrated solution that includes all aspects of security such as identity, credential, policy and access management.

Impact of overly complex data protection:

- **Data loss.** Data loss has the greatest impact on your business since it affects every aspect of it.
- **Productivity loss.** If employees are locked out of a system or need to be granted access and don't have an easy way to reset their credentials or request access they cannot do their job.
- **Credibility loss.** In today's business climate of integrated systems, effective data protection is crucial to avoid losing credibility with partners.

Identity Management Must Drive Business Value

IT projects are assessed on their ability to enable more business to be done. Identity management should be leveraged to automate and integrate business processes. Whether it is order fulfillment, customer service or product development, business processes benefit from end-to-end workflow control and automation delivered through identity management. For instance, when new systems or employees can be seamlessly integrated into an enterprise with minimal additional effort and productivity impact as a result of an Identity Management investment, the investment enhances the business profitability. In this case, even mergers and acquisitions can be completed more efficiently and with greater speed.

Impact of solutions that do not deliver business agility:

- **Budgetary pressure.** Identity management projects are viewed as a cost creator and not as business enabler.
- **Strategic impact.** Identity management projects are viewed as a tactical necessity instead of a strategic imperative thus reducing the solution's efficiency.
- **Process alignment.** Identity management cannot maximize their contribution to the business if their systems hamper the business process.

Compliance is Critical

Regulatory compliance is a key driver of identity management among enterprises. Companies must be in a position to know who is accessing what data throughout the organization. Without an integrated identity management solution, organizations expose themselves to additional risk of noncompliance.

Impact of inefficient compliance:

- **Increased costs.** Manual auditing and monitoring across multiple systems is a costly endeavor for the enterprises.
- **Increased risk of non-compliance.** Manual auditing also introduces the potential for error and inadvertent non-compliance, which can result in legal and or financial issues.

Microsoft's Identity Management Approach

With ILM 2007 and its successor FIM 2010, Microsoft is taking a fundamentally different approach to identity management. In ILM 2007, Microsoft integrated certificate and smart card management functionality with traditional identity management lifecycle, enabling customers to achieve new levels of efficiency through common management of identities and credentials, as well as improve security and compliance by making it easier to implement and manage strong credentials.

Delivering on comprehensive identity and access management in the enterprise, FIM 2010 advances the current state of the art of identity management. FIM 2010 brings powerful self-service capabilities for the end-user through integration in Office in addition to administrative tools and enhanced automation for IT professionals in addition to .NET and Windows SharePoint Services based extensibility for developers. Microsoft's approach is focused on:

- Empowering people. FIM 2010 empowers end users, IT professionals, and developers by putting the right tools in the right hands. With FIM 2010, end users can easily perform self-service tasks with Microsoft Office Outlook. Likewise, FIM 2010 provides IT with the tools they need to manage identities through a SharePoint-based policy management console, and developers have access to extensibility features through .NET and Windows SharePoint Services.
- Delivering agility and efficiency. By delivering automation and self-service, FIM 2010 dramatically reduces the high costs and risk currently associated with identity management deployments. FIM 2010 integrates enterprises' heterogeneous identity infrastructure, including directories, database and line of business applications, and heterogeneous strong authentication systems such as third-party Certificate Authorities and One-Time Password devices. This heterogeneous approach helps organizations leverage existing identity infrastructure investments. By providing management of identities that can be utilized across the identity infrastructure and integrating with familiar developer tools and technologies, FIM 2010 makes it easier to enable new business scenarios.
- Increasing security and compliance. FIM 2010 provides policy management features that simplify identity management auditing and compliance. By integrating the tools IT uses to manage identities, credentials, and resources, FIM 2010 helps organizations integrate policies across the organization and secure the enterprise. Furthermore, with strong authentication management tools integrated with FIM 2010, organizations can more easily enjoy the security benefits of strong authentication.

Identity Lifecycle Manager 2007

ILM 2007 is designed to simplify and automate some of the most costly aspects of identity management, and provide a foundation for future identity integration and automation.

Features and Benefits of Identity Lifecycle Manager 2007

ILM 2007 delivers integrated identity synchronization, comprehensive certificate and smart card management and automated user provisioning in one secure solution.

Identity Synchronization

Combining identity data across multiple directories and systems yields automated account reconciliation, and consistency management for user accounts, credentials, and attributes. This means organizations with many different directories and other data repositories, such as a Human Resources application, can use ILM 2007 to synchronize user accounts across systems.

Organizations can also use ILM 2007 to synchronize e-mail address lists that are maintained by heterogeneous e-mail systems, such as Microsoft Exchange Server 2000, Exchange Server 2007, and Lotus Notes. Organizations that have multiple Active Directory® domain service and Exchange forests can use ILM 2007 to build a single address book. This increases the value of identity integration by simplifying collaboration as well as increasing IT control.

Certificate and Smart Card Management

While strong authentication is becoming both desirable and in many cases a mandated technology used to verify and secure user identity, the cost and complexity of managing digital certificates and smart cards has slowed adoption or forced customers to trade security for business agility.

ILM 2007 is the only Microsoft Windows-based certificate management solution that provides turnkey deployment and is designed to require no custom development work to fully deploy. ILM 2007 also simplifies digital certificate and smart card deployment in an enterprise with services such as Microsoft Active Directory and Windows Server™ Certificate Services to lower the cost to deploy, manage, and maintain a certificate-based infrastructure.

User Provisioning

Organizations using ILM 2007 can define policies that automatically create user accounts, mail boxes, and group memberships in real-time so that new employees are productive immediately.

When a user changes roles within an organization, ILM 2007 automatically makes the necessary changes in heterogeneous target systems to add and remove access rights. For example, if a user moves from a role in sales to a role in marketing, ILM 2007 can remove them from sales-specific groups and add them to marketing-specific groups to deliver appropriate access permissions to perform their job function.

Forefront Identity Manager 2010

The next release of ILM, FIM 2010, will extend the functionality of ILM 2007 to further reduce the cost and inefficiency associated with the management of the entire identity life cycle.

Building on the certificate management process, user account provisioning and identity integration available in ILM 2007, FIM 2010 aligns the management environment to the systems and processes most appropriate to the IT professional’s or business user’s role within an organization.

For example, an end user can most easily manage their group memberships from within Microsoft Outlook®, and the IT administrator is most productive when they can set policy and monitor security and workflow from a centralized system.

FIM 2010 Highlights:
Policy Management • SharePoint-based console for policy authoring, enforcement & auditing • Extensible FIM Service APIs and Windows Workflow Foundation workflows • Heterogeneous identity synchronization & consistency
Credential Management • Heterogeneous certificate management with third-party CA support • Self-service password reset integrated with Windows logon
User Management • Integrated provisioning of identities, credentials, and resources • Automated, declarative user provisioning and deprovisioning • Self-service user profile management and whitepages.
Group Management • Rich Office-based self-service group management tools • Offline approvals in Office Outlook • Automated group and distribution list updates

Expanded Features and Benefits Delivered in Forefront Identity Manager 2010

FIM 2010 builds on the metadirectory, certificate life cycle management and user provisioning available in ILM 2007, and adds a rich management environment including integrated user management, self-service for comprehensive credential management, group management, basic policy management, and expanded connectivity.

Policy Management

FIM 2010 will deliver a framework for identity management automation and integration so all enterprise systems run using the same set of enterprise policies. This is accomplished by:

- **Centralized policy authoring, enforcement, & auditing.** As part of the FIM 2010 release, Microsoft will deliver an intuitive SharePoint-based user interface that enables system architects, IT administrators and end users to create rules governing users and groups using natural language descriptors and easy-to-use menu-driven controls. The policy management tools will also enable business owners and IT to report on the events and business rules processed by FIM 2010, and to act on that information in an automated manner. This provides a view into the state of compliance as well a mechanism to enforce business rules that support compliance.
- **Extensible Windows Workflow Foundation-based workflows.** FIM 2010 includes rich, visual workflow management based on the Windows Workflow Foundation, which enables IT to quickly define, automate and enforce identity management policies. IT can use the integrated workflow in the approval / rejection process for actions such as creating accounts, or delegating tasks. For further extensibility and customization, FIM 2010 will ship with web services APIs that enable customization at both the platform and solution level. FIM 2010 consumes Windows Workflow Foundation (WF) workflows, enabling organizations to import and reuse existing WF-based workflows in FIM 2010.
- **Heterogeneous identity synchronization & consistency.** FIM 2010 delivers integration with a broad range of network operating systems, e-mail, database, directory, application, and flat-file access. FIM 2010 supports connectors for Active Directory, Novell, Sun, IBM, Lotus Notes, Microsoft Exchange Server, Oracle databases, Microsoft SQL Server™ databases, SAP and others. This provides organizations with the power to connect and synchronize the plethora of disparate sources of identity information in their company—in most cases without the need to install software of any kind on the target systems. Since in some cases it might be necessary to connect to custom or legacy applications unique to a specific organization, FIM 2010 extensible agent capabilities enables companies to integrate and manage identities for these applications through developing custom agents in the Microsoft Visual Studio® development environments.

Credential Management

FIM 2010 provides the ability to manage multiple credentials in an integrated manner from the administrative and end user standpoint. IT professionals will have one place where they can look at user policies, define policies, and define smart card templates and processes for resetting PINs. With FIM 2010 the end user's experience will be very intuitive, Credential management activities for end users will be embedded in familiar applications and integrated with familiar tools, which reduces the cost of deploying identity management for the organization and enables easier and faster adoption. To implement these goals, FIM 2010 provides:

- **Credential lifecycle management integrated with provisioning.** With FIM 2010, IT will be able to define policies that manage the provisioning process across user accounts and credentials. This means that workflow in FIM 2010 can be configured to automatically

provision a user account, set their initial password, and kick off the process to issue the user smart cards and digital certificates. For instance, FIM 2010 can manage a user provisioning process that would not only issue a new user's Active Directory account and set up their mailbox, but also issue the new user a one-time use pin for them to activate their smart card.

- **Management of multiple credentials such as third-party Certificate Authorities (CAs) and One-Time Passwords (OTPs).** FIM 2010 can be extended to manage a wide range of credentials that your organization uses to secure resources. The certificate and smart card management capabilities introduced in ILM 2007 can now be extended to provide centralized management of additional strong authentication factors, including management of third-party CAs and OTP devices, which includes partner solutions.
- **Self-service password integrated with Windows logon.** FIM 2010 enables users to change and reset their own passwords and smart card PINs from the Windows desktop login.
- **Configurable authentication gates for self-service password reset**. FIM 2010 will ship with configurable question and answer authentication gates, and will include extensibility to build additional types of gates – for instance a smart card gate or a gate that requires a user to enter a code sent to a mobile phone. The enrollment process for authentication gates can be configured to ensure that all users in an organization enroll – for instance requiring registration at login.
- **Simplified sign-on by synchronizing passwords across systems.** Importantly, FIM 2010 provides a simplified sign-on experience through its identity synchronization capabilities, delivering the ability to synchronize passwords across heterogeneous systems.

User Management

One of the most important things Microsoft is delivering from a developer standpoint and business standpoint is automated, codeless, user provisioning. FIM 2010 delivers tools for integrated user management and self-service across enterprise applications without the costly coding of business rules or recoding of the target systems. These automated and centralized user management tools include:

- **Declarative user provisioning.** FIM 2010 provides a user interface to configure provisioning rather than requiring customized code to be written as was the case in previous versions. Automated provisioning allows you to easily define the provisioning workflows associated with adding a new user to the enterprise and provisioning them with access to appropriate applications in an automated manner.
- **Integrated provisioning of identities, credentials, and resources.** Using management tools delivered in FIM 2010, IT can create a policy to provision the appropriate accounts, resources, and credentials, associate to users, ensure the appropriate workflows are integrated into the process, and do this in a very seamless manner. This means that an enterprise can provide automated and integrated processes for new users when they come to the enterprise, which makes them more productive from day one. De-provisioning for users leaving the enterprise also becomes centralized and less complicated, which makes it easier to ensure complete deprovisioning and to handle future compliance audits.

- **Self-service user profile management.** New features in FIM 2010 make it possible for users to manage their own identity information. IT can use FIM 2010 to set policies to require workflows such as approvals for or notifications of these user-generated changes. For example, IT may choose to delegate management of mobile phone numbers to end users. Users would be able to use the FIM 2010 portal to update this information. This helps keep identity data such as mobile phone number up to date so that users can be easily contacted in the process of doing business.

Group Management

FIM 2010 provides powerful capabilities out of the box that help increase the productivity of end users, frees up IT from repetitive tasks and provide better security and compliance outcomes. These features include:

- **Rich self-service group management tools.** FIM 2010 provides self-service group and distribution list management with the FIM 2010 Web portal. Integration with Outlook enables end users to manage their group membership requests using the collaboration tools they are familiar with for maximum productivity with minimal additional training. For example, with approve and reject buttons functionality provided in Outlook to approve or reject membership requests, FIM 2010 makes it possible for users to manage the membership of groups without requiring the assistance of the IT organization. FIM 2010 end users can create distribution lists for new virtual teams and manage requests made by others to join a distribution list.
- **Offline approvals through Outlook.** Capabilities to manage group membership are in FIM 2010 integrated into Outlook. This enables users to use Outlook to, for example, request membership in a group or manage approvals while they are offline.
- **Automated group and distribution list updates.** In addition to the self-service management of group membership, FIM 2010 also supports the dynamic calculation of group members based on the characteristics of an resources. With this feature, users are added and removed from groups automatically. For example, IT can configure a group that is used to control access to the resources of a team so that only the manager and the direct reports are members. In this case, FIM 2010 can calculate the group membership based on the manager attribute of the user resource. In case of structural changes to the team such as members joining or leaving the team, the group membership is automatically updated. Dynamic group membership helps reduce the manual interaction required to effectively protect resources.

Conclusion

The strategy and priorities outlined in this paper are intended to help customers get the most out of the Microsoft infrastructure while making their IT enterprise more efficient and easier to control. Because Microsoft delivers a rich management environment that uses tools most appropriate for each type of user, Microsoft lifts barriers and complexity while lowering the costs associated with identity management.

Imagine having an integrated view of all users and their permissions based on a sound business policy. Also imagine eliminating the manual provisioning processes that are only noticed if they

break down. Feel secure knowing that you can scale provisioning processes for sudden increases in hiring of new employees without negatively impacting other customer service level agreements.

Users will be productive on day one of their employment as their accounts, credentials, and resources will be automatically provisioned in heterogeneous directories and applications across the enterprise.

If users need additional access, the workflow that supports that decision can also be automated so the decision to grant access can remain with the appropriate approver. This is Microsoft's strategy for identity management, to make identity management much easier by putting the right tools in the right hands.