

Identity & Access Management

Microsoft
GOLD CERTIFIED
Partner

Microsoft Solutions

The cost and effort required to effectively and securely implement and manage user communities in a corporate network made up of diverse systems can be overwhelming. However, the failure to do so risks security breaches, regulatory compliance breakdowns and an inability to effectively deploy new business initiatives.

Key Solution Elements:

- Identity Lifecycle Management
- Information Protection
- Federated Identity
- Strong Authentication
- Directory Services

Identity Lifecycle Management

Microsoft Identity Lifecycle Manager 2007 provides an integrated product that builds on Microsoft Identity Integration Server 2003 and offers identity synchronization, certificate management and user provisioning in one solution that works across the OS and other organizational systems.

Benefits:

- Keeps information synchronized and constant across a wide range of directories, databases and proprietary identity systems.
- Provides a single place for IT and users to manage the entire lifecycle of user credentials.
- Provides best-in-class directory synchronization, giving IT control and visibility over identity cleanup and reconciliation processes.
- Provides IT a robust, policy-based management solution for controlling and helping secure resources.
- Provides 25 connectors to external identity stores out of the box and offers extensibility to develop additional connectors.
- Delivers a platform that can be customized as needed by IT, independent software vendor (ISV) partners or

software integrator (SI) partners with a vast set of third-party solutions available.

Information Protection

Microsoft Windows Rights Management Services (RMS) provides a comprehensive solution to protect and control access to sensitive information, both during and after its delivery into authorized hands.

Benefits:

- Reduces risk of leaks of confidential information through persistent protection of data.
- Eases adoption by users through smooth integration with Microsoft Office programs.
- Eases deployment through integration with Windows Server Active Directory.
- Supports third-party applications and document formats through a powerful software development kit (SDK).

Federated Identity

Active Directory Federation Services (ADFS) provides a standards-based mechanism for establishing trust between different entities, enabling organizations to collaborate more securely and efficiently. This gives users a smooth, cross-company single sign-on (SSO) experience.

Benefits:

- Increases efficiency and helps reduce cost through proficient management of IDs, passwords and your investment in Active Directory.
- Enhances collaboration and efficiency between companies by adding a level of transparency to the accessing of information that is securely located at the other company.



- Improves security by integrating with your current security infrastructure and business policies, using the ADFS claim-mapping capability along with its extensibility through support of Security Assertion Markup Language (SAML) token type and Kerberos authentication.

Strong Authentication

Microsoft Windows Certificate Services provides a comprehensive solution for issuing and administering certificates used in software security systems employing public key technologies. It also includes an integrated user experience in Windows. Certificate Services enables the secure exchange of information with strong security and easy administration across the Internet, extranets, intranets and applications.

Benefits:

- Increases access security with improved security over username and password, with the ability to verify validity of certificates using online certificate status protocol (OCSP).
- Lowers cost of ownership by leveraging full integration with Active Directory for enrollment, store and revocation process.
- Simplifies management of certificates from a single certificate store by using integration with Microsoft

Management Console.

- Simplifies deployment by enrolling user and computer certificates without user intervention.

Directory Services

Active Directory Domain Services (ADDS), the world's most widely deployed directory service, provides a single place in the network to store and manage user privileges and devices. For organizations requiring flexible support for directory-enabled applications, Microsoft has Active Directory Lightweight Directory Services (ADLDS): a Lightweight Directory Access Protocol (LDAP) directory service. With direct integration with Federated Identity, Strong Authentication, Information Protection and Identity Lifecycle Management solutions, Active Directory is an ideal foundation for building a comprehensive identity and access solution.

Benefits:

- Lowers costs associated with managing Windows networks.
- Simplifies identity management by providing a single view of all user information.
- Provides a key data source for important compliance and audit information.
- Enables multiple security types within your network.
- Provides the ideal platform for building a comprehensive identity and access solution.

Phased Approach

We take a phased approach to your Identity and Access Management projects, with set milestones based on best practices. These phases are based on Microsoft's proven approach to technology projects, the Microsoft Solutions Framework (MSF). This is how it works:

Assess: Help identify your business drivers, review your current environment and develop an initial logical design for the new environment. The phase concludes with a milestone where you approve the vision and scope, based on the business case.

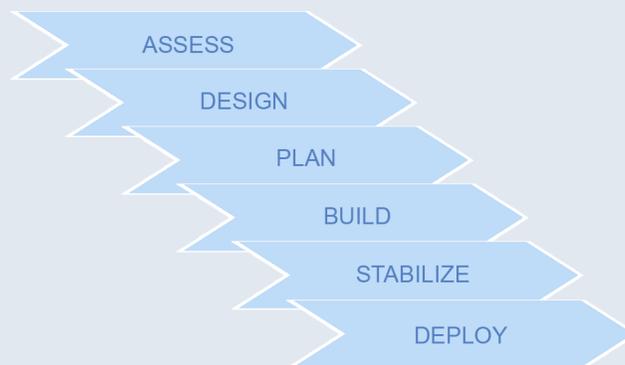
Design: Our experts work closely with your staff to refine the design for the new environment. At the end of this phase we re-examine the business case to ensure the design aligns with the desired goals.

Plan: Once the infrastructure design is complete, our team guides your staff through the implementation options and documents the detailed plans.

Build: With the plans completed, we help test the infrastructure design, implementation strategy, systems management design and operations plan in a test lab.

Stabilize: Our team helps define a detailed release-management plan and sets up a pilot environment to further stabilize the final solution.

Phased Project Approach



Deploy: The core technology and site components are deployed and the project is transitioned to operations and support. After the deployment, the team conducts a project review and a customer satisfaction survey.

Not Sure Where to Begin?

Let us help. We can assess your current environment, help map strategic business goals to the capabilities offered in our Microsoft Solutions for Identity and Access Management and help establish your end-state vision for implementation. For more information contact us at mssolutions@prosysis.com or contact your local ProSys representative.