WHITE PAPER

Distributed Document Imaging: Maximizing Your Investment in Microsoft® Technology

Integration with Active Directory®

NUANCE®

Contents

Introduction

Given the fundamental role of Active Directory (AD) in the IT infrastructure, any distributed document imaging solution must integrate with AD for purposes of security, administration, and ease-of-use:

- The authentication process at the device must mirror the authentication process at the Windows desktop, using the same AD logon credentials and secure protocols.
- Having logged on, users must be able to access the applications they are authorized to use without logging on again. To do this, the solution must leverage AD's single sign-on feature, which automatically unlocks applications, including 3rd-party applications, which use Windows integrated authentication.
- The user's existing AD profile must determine the level of access to various network resources from the scanning device. Users must be able to scan documents to the same libraries, databases, folders, etc. they use from their desktop, but must be prohibited from accessing those for which they do not have access rights.

This eCopy technology brief is one in a series of four briefs that examine the requirements for successfully integrating a distributed document imaging application into your existing Microsoft-focused IT environment. Other technology briefs in this series include:

- Exchange
- SharePoint
- SQL Server / Access

The other three technology briefs in this series can be downloaded from our Web site.

Distributed Document Imaging in Microsoft IT Infrastructures

Distributed document imaging solutions enable knowledge workers to convert paper documents into electronic files.

As a result, these solutions offer significant benefits, including:

- Making paper-based information available throughout the organization
- Speeding up the processing of paper documents while simultaneously reducing the associated costs
- Enabling administrators to apply policies for compliance with records management and security regulations
- Safeguarding paper documents through electronic backup to offsite facilities

To achieve these benefits, the imaging application must be easy to use and must integrate with the applications people already use on a daily basis for communication, collaboration, and document storage. Users must be able to walk up to any scanning device and store, distribute, and share paper documents the same way they handle electronic files at their desktop – by browsing the network, storing files to pre-configured locations, selecting recipients from address lists, and indexing documents for quick retrieval.

For organizations with Microsoft-focused IT infrastructures, this means integrating with the Microsoft technologies and applications already in place, such as Active Directory®, Exchange, SharePoint®, and SQL Server®-based business management applications.

Dynamic integration with back-end servers (domain controllers, Exchange servers, SharePoint servers, etc.) through programmed interfaces ensures that the user interface reflects the latest changes to the underlying applications, directories, and site structures. It also eliminates the need for preconfigured scanning cover sheets that some imaging solutions require. The application interfaces must be sophisticated enough to handle the infinite variety of complex network environments involving multiple domains, multiple forests, outsourced IT management, and internet-hosted services.

Authentication and security

An ideal distributed imaging application uses the Security Support Provider Interface (SSPI) to negotiate the best protocol (frequently Kerberos or NTLM) based on the security policies in place.

If capturing user credentials on a non-Windows platform (for example, an imaging client running on the MFP's embedded computing engine), the client must use a secure protocol, like Triple DES or SSL, to ensure the credentials cannot be intercepted during transfer over the network.

Lowering total cost of ownership

Some distributed imaging solutions require manual account setup for each user. This adds significantly to the administrative workload, since IT staff must continually add, modify, and delete accounts as employees transition throughout the organization.

It also compromises security, since manual processes are error-prone and subject to delayed implementation.

Integration with AD eliminates the need to manage separate user lists and passwords, dramatically reducing the need for IT intervention and thereby lowering the total cost of ownership. When an IT administrator creates a new user account, that user is automatically configured to use the scanning device, subject to any restrictions associated with existing group policies.

AD maintains links between user accounts, mailbox accounts, and applications, so a single change updates the user information for all applications and services. If the imaging application is tied into the same account management database, the rights and restrictions associated with that user propagate immediately to each scanning device. Similarly, password changes are applied automatically to all AD-integrated applications.

Implementing access controls

An ideal distributed imaging solution integrates with the existing AD organizational structure.

The Organizational Unit (OU) is the level at which administrative controls are typically delegated, and administrators may need to limit access to devices to those within a specific OU. By enabling administrators to restrict access to certain branches of the organizational hierarchy, administrators can effectively control access to devices with minimal effort.

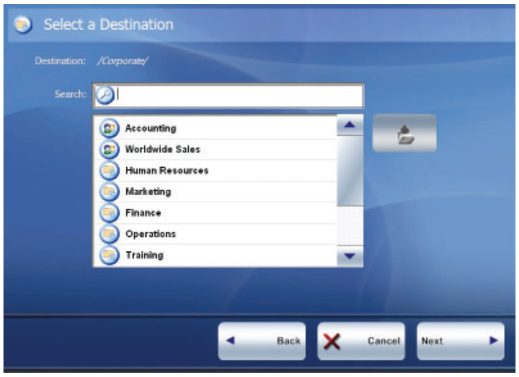
For example, a college has MFP devices located in common areas. The administrator needs to restrict access so that students and faculty can use “scan to email” but only faculty can use “scan to folder.” Although students and faculty have accounts on the same domain, students are in the “Students” OU, while faculty members are in the “Faculty” OU. In this case, the administrator can provide general access to both OUs but limit “scan to folder” access to OU=Faculty.

Personalization at the device

When a user logs on through an AD-integrated imaging application, the application can access the information in the user’s AD profile.

For example, the application can read the user’s “Home Directory” attribute and make that location immediately available for storing scanned documents without requiring any folder navigation or selection. When browsing the network, personalization ensures that users can see only folders they are allowed to access.

Imaging applications that support AD-integrated applications like Microsoft Exchange or SharePoint (both covered in other documents in this series) can make extensive use of personalization. Exchange integration can provide the user with access to personal contacts and distribution lists, while SharePoint integration can filter available destinations and pre-populate available content types and metadata based on the user’s profile.



Select a Destination

Destination: /Corporate/

Search:

Users logging on through an AD-integrated imaging application can only see the folders they are allowed to access.

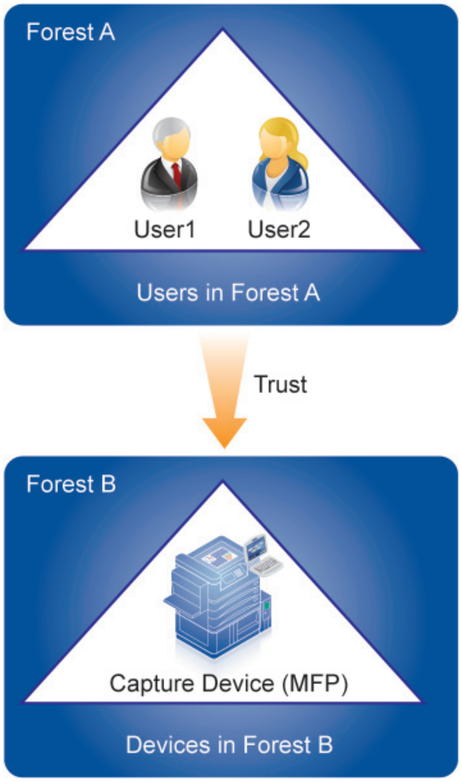
Handling complex environments

In a multi-domain forest, each domain stores information about objects in that domain only.

For example, a user in “Domain A” is stored only on Domain A’s domain controllers, while a device in “Domain B” is stored only on Domain B’s domain controllers. In this type of environment, a distributed imaging solution must enable users in Domain A to access devices in Domain B.

In a multi-forest environment, cross-forest authentication enables secure access to resources when the user account is in one forest and the capture device is in another forest. This enables users to work securely without sacrificing the single sign-on and administrative benefits of having only one user ID and password.

Access to resources in other domains or forests is supported through trust relationships and global catalog servers. In a multi-domain or multi-forest environment, therefore, it is important that the distributed imaging application can communicate with global catalog servers, and not just with servers within the local domain or forest.



A multi-forest environment with cross-forest authentication.

Summary

Ideally, a distributed imaging solution should bring the user’s existing Windows environment to the scanning device.

Integration with Active Directory makes that possible. Doing so virtually eliminates any administrative overhead, since the solution ties into the existing user management infrastructure.

Considerations when selecting a distributed imaging solution:

- Does the authentication process at the device mirror the authentication process at the Windows desktop, using the same user credentials and the same secure protocols?
- Does the solution integrate with AD to restrict access to applications and resources based on the user’s AD profile and the groups to which the user is assigned?
- Once logged on, can users access any of the applications they are authorized to use without having to log on again?
- Can the administrator restrict device access to those below a specified DN (Distinguished Name) in the organizational hierarchy?
- Can the solution filter available options and pre-configure certain fields based on the user’s identity?
- Does the solution work in complex multi-domain and multi-forest environments?

The experience speaks for itself™

NUANCE COMMUNICATIONS, INC.

ONE WAYSIDE ROAD
BURLINGTON, MA 01803

781 565 5000
NUANCE.COM

NUANCE®