Test 1: Table width 80%, Column Width 33%, Cell Width 33%

## Self Assessment

Microsoft has developed a self-assessment tool that you can use to determine your current optimization level. We recommend that you use this tool before proceeding with this guide. The tool is based on the material presented in this guide. To access the self-assessment tool, visit: <http://www.microsoft.com/business/peopleready/coreinfra/ac/default.mspx>.

The following section presents questions for each of the core capabilities that direct you to relevant sections of this planning guide. Your answers to the questions will dictate which sections contain guidance applicable to your organization. Many requirements in the following section have minimum attributes associated with them. If your organization meets every requirement and requirement attribute outlined in this section, you have already achieved the Rationalized level and can proceed to the Dynamic level in Core Infrastructure Optimization. You can print this section as a scorecard for determining which requirements and attributes you need to implement in your organization.

### Capability: Identity and Access Management

The Rationalized level of optimization requires a directory-based tool to centrally administer configurations and security on 80 percent or more desktops in your organization.

|  |  |  |
| --- | --- | --- |
| Requirement: Identity and Access Management | Yes | No |
| Implemented a directory-based tool to centrally administer configurations and security on 80 percent or more of your desktops |  |  |
| Attributes:   * Identified which configurations should be monitored or enforced. * Selected tools for monitoring and enforcing configuration compliance. * Defined Group Policy objects for settings managed through Group Policy. * Implemented Group Policy Management Console to manage Group Policy objects. * Applied Group Policy to at least 80 percent of your desktops. | | |

For more details, see [Centralized Directory-based Configuration and Security](#_Centralized_Directory_Based) in this document, or visit the following Web sites:

* [Windows Server 2003 Active Directory Technology Center](http://www.microsoft.com/windowsserver2003/technologies/activedirectory/default.mspx)
* [Windows® XP Security Guide](http://go.microsoft.com/fwlink/?linkid=14839)
* [Windows Vista Security Guide](http://go.microsoft.com/fwlink/?linkid=74027)
* [Windows Server 2003 Technical Library](http://technet2.microsoft.com/WindowsServer/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx?mfr=true)
* [Microsoft Operations Framework Configuration Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcfgmg.mspx)
* [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx)
* [Medium Business Solution for Management and Security using Active Directory Group Policy](http://www.microsoft.com/downloads/details.aspx?FamilyId=BB534B41-B413-4483-9097-879F5CAFE2DC&displaylang=en)

Additional information is available at [Medium Business Solution for Client Configuration](http://www.microsoft.com/technet/solutionaccelerators/smbiz/mits/cc/mit_cc.mspx).

Capability: Identity and Access Management

# Introduction

Identity and Access Management is a Core Infrastructure Optimization capability and the foundation for implementing many capabilities in the Infrastructure Optimization Model.

The following table lists the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in Identity and Access Management.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Difficult to enforce IT policies required by the organization or regulations  No way to enable a known, stable, and secure state for client PCs  **IT Challenges**  No centralized policy control for identity and access management—implementing broad policy changes requires modification of each identity  Identities are centrally administered, but difficult to manage users and resource settings, configurations | **Projects**  Identify and define configuration standards requiring enforcement  Implement a centralized, directory-based policy solution for administration of desktops, servers, configuration, and security | **Business Benefits**  Enforced, known state of environment  Consistent user experience across PCs based on business role  Easier to modify system and add functionality  Reduced operations and desktop support costs  Reduced user downtime and disruption  **IT Benefits**  Reduced workload due to introduction of role-based administration/group policy  Improved security by implementing policy-based patch management and security lockdown  Profile management allows user system and data recovery |

Ongoing Identity and Access Management focuses on the following capabilities as outlined in the Microsoft Identity and Access Management Series:

* The Foundation for Identity and Access Management
* [Fundamental Concepts](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Fund.mspx)
* [Platform and Infrastructure](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Plat.mspx)
* Identity Life-Cycle Management
* [Identity Aggregation and Synchronization](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P2Ident.mspx)
* [Password Management for Intranet and Extranet](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2pass.mspx)
* [Provisioning and Workflow](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* Access Management and Single Sign-On
* [Intranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* [Extranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)

Note that the capabilities outlined above are all key parts of the Identity and Access Management service in any organization. For more information, please see the [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx).

The Rationalized level of Identity and Access Management in the Infrastructure Optimization Model addresses the need for centralized control of configurations and security.

Test 2: Table width 9 inches, Column Width 3 Inches, Cell width 3 Inches

## Self Assessment

Microsoft has developed a self-assessment tool that you can use to determine your current optimization level. We recommend that you use this tool before proceeding with this guide. The tool is based on the material presented in this guide. To access the self-assessment tool, visit: <http://www.microsoft.com/business/peopleready/coreinfra/ac/default.mspx>.

The following section presents questions for each of the core capabilities that direct you to relevant sections of this planning guide. Your answers to the questions will dictate which sections contain guidance applicable to your organization. Many requirements in the following section have minimum attributes associated with them. If your organization meets every requirement and requirement attribute outlined in this section, you have already achieved the Rationalized level and can proceed to the Dynamic level in Core Infrastructure Optimization. You can print this section as a scorecard for determining which requirements and attributes you need to implement in your organization.

### Capability: Identity and Access Management

The Rationalized level of optimization requires a directory-based tool to centrally administer configurations and security on 80 percent or more desktops in your organization.

|  |  |  |
| --- | --- | --- |
| Requirement: Identity and Access Management | Yes | No |
| Implemented a directory-based tool to centrally administer configurations and security on 80 percent or more of your desktops |  |  |
| Attributes:   * Identified which configurations should be monitored or enforced. * Selected tools for monitoring and enforcing configuration compliance. * Defined Group Policy objects for settings managed through Group Policy. * Implemented Group Policy Management Console to manage Group Policy objects. * Applied Group Policy to at least 80 percent of your desktops. | | |

For more details, see [Centralized Directory-based Configuration and Security](#_Centralized_Directory_Based) in this document, or visit the following Web sites:

* [Windows Server 2003 Active Directory Technology Center](http://www.microsoft.com/windowsserver2003/technologies/activedirectory/default.mspx)
* [Windows® XP Security Guide](http://go.microsoft.com/fwlink/?linkid=14839)
* [Windows Vista Security Guide](http://go.microsoft.com/fwlink/?linkid=74027)
* [Windows Server 2003 Technical Library](http://technet2.microsoft.com/WindowsServer/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx?mfr=true)
* [Microsoft Operations Framework Configuration Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcfgmg.mspx)
* [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx)
* [Medium Business Solution for Management and Security using Active Directory Group Policy](http://www.microsoft.com/downloads/details.aspx?FamilyId=BB534B41-B413-4483-9097-879F5CAFE2DC&displaylang=en)

Additional information is available at [Medium Business Solution for Client Configuration](http://www.microsoft.com/technet/solutionaccelerators/smbiz/mits/cc/mit_cc.mspx).

Capability: Identity and Access Management

# Introduction

Identity and Access Management is a Core Infrastructure Optimization capability and the foundation for implementing many capabilities in the Infrastructure Optimization Model.

The following table lists the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in Identity and Access Management.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Difficult to enforce IT policies required by the organization or regulations  No way to enable a known, stable, and secure state for client PCs  **IT Challenges**  No centralized policy control for identity and access management—implementing broad policy changes requires modification of each identity  Identities are centrally administered, but difficult to manage users and resource settings, configurations | **Projects**  Identify and define configuration standards requiring enforcement  Implement a centralized, directory-based policy solution for administration of desktops, servers, configuration, and security | **Business Benefits**  Enforced, known state of environment  Consistent user experience across PCs based on business role  Easier to modify system and add functionality  Reduced operations and desktop support costs  Reduced user downtime and disruption  **IT Benefits**  Reduced workload due to introduction of role-based administration/group policy  Improved security by implementing policy-based patch management and security lockdown  Profile management allows user system and data recovery |

Ongoing Identity and Access Management focuses on the following capabilities as outlined in the Microsoft Identity and Access Management Series:

* The Foundation for Identity and Access Management
* [Fundamental Concepts](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Fund.mspx)
* [Platform and Infrastructure](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Plat.mspx)
* Identity Life-Cycle Management
* [Identity Aggregation and Synchronization](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P2Ident.mspx)
* [Password Management for Intranet and Extranet](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2pass.mspx)
* [Provisioning and Workflow](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* Access Management and Single Sign-On
* [Intranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* [Extranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)

Note that the capabilities outlined above are all key parts of the Identity and Access Management service in any organization. For more information, please see the [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx).

The Rationalized level of Identity and Access Management in the Infrastructure Optimization Model addresses the need for centralized control of configurations and security.

Test 3: Distribute Columns Evenly

## Self Assessment

Microsoft has developed a self-assessment tool that you can use to determine your current optimization level. We recommend that you use this tool before proceeding with this guide. The tool is based on the material presented in this guide. To access the self-assessment tool, visit: <http://www.microsoft.com/business/peopleready/coreinfra/ac/default.mspx>.

The following section presents questions for each of the core capabilities that direct you to relevant sections of this planning guide. Your answers to the questions will dictate which sections contain guidance applicable to your organization. Many requirements in the following section have minimum attributes associated with them. If your organization meets every requirement and requirement attribute outlined in this section, you have already achieved the Rationalized level and can proceed to the Dynamic level in Core Infrastructure Optimization. You can print this section as a scorecard for determining which requirements and attributes you need to implement in your organization.

### Capability: Identity and Access Management

The Rationalized level of optimization requires a directory-based tool to centrally administer configurations and security on 80 percent or more desktops in your organization.

|  |  |  |
| --- | --- | --- |
| Requirement: Identity and Access Management | Yes | No |
| Implemented a directory-based tool to centrally administer configurations and security on 80 percent or more of your desktops |  |  |
| Attributes:   * Identified which configurations should be monitored or enforced. * Selected tools for monitoring and enforcing configuration compliance. * Defined Group Policy objects for settings managed through Group Policy. * Implemented Group Policy Management Console to manage Group Policy objects. * Applied Group Policy to at least 80 percent of your desktops. | | |

For more details, see [Centralized Directory-based Configuration and Security](#_Centralized_Directory_Based) in this document, or visit the following Web sites:

* [Windows Server 2003 Active Directory Technology Center](http://www.microsoft.com/windowsserver2003/technologies/activedirectory/default.mspx)
* [Windows® XP Security Guide](http://go.microsoft.com/fwlink/?linkid=14839)
* [Windows Vista Security Guide](http://go.microsoft.com/fwlink/?linkid=74027)
* [Windows Server 2003 Technical Library](http://technet2.microsoft.com/WindowsServer/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx?mfr=true)
* [Microsoft Operations Framework Configuration Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcfgmg.mspx)
* [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx)
* [Medium Business Solution for Management and Security using Active Directory Group Policy](http://www.microsoft.com/downloads/details.aspx?FamilyId=BB534B41-B413-4483-9097-879F5CAFE2DC&displaylang=en)

Additional information is available at [Medium Business Solution for Client Configuration](http://www.microsoft.com/technet/solutionaccelerators/smbiz/mits/cc/mit_cc.mspx).

Capability: Identity and Access Management

# Introduction

Identity and Access Management is a Core Infrastructure Optimization capability and the foundation for implementing many capabilities in the Infrastructure Optimization Model.

The following table lists the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in Identity and Access Management.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Difficult to enforce IT policies required by the organization or regulations  No way to enable a known, stable, and secure state for client PCs  **IT Challenges**  No centralized policy control for identity and access management—implementing broad policy changes requires modification of each identity  Identities are centrally administered, but difficult to manage users and resource settings, configurations | **Projects**  Identify and define configuration standards requiring enforcement  Implement a centralized, directory-based policy solution for administration of desktops, servers, configuration, and security | **Business Benefits**  Enforced, known state of environment  Consistent user experience across PCs based on business role  Easier to modify system and add functionality  Reduced operations and desktop support costs  Reduced user downtime and disruption  **IT Benefits**  Reduced workload due to introduction of role-based administration/group policy  Improved security by implementing policy-based patch management and security lockdown  Profile management allows user system and data recovery |

Ongoing Identity and Access Management focuses on the following capabilities as outlined in the Microsoft Identity and Access Management Series:

* The Foundation for Identity and Access Management
* [Fundamental Concepts](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Fund.mspx)
* [Platform and Infrastructure](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Plat.mspx)
* Identity Life-Cycle Management
* [Identity Aggregation and Synchronization](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P2Ident.mspx)
* [Password Management for Intranet and Extranet](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2pass.mspx)
* [Provisioning and Workflow](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* Access Management and Single Sign-On
* [Intranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* [Extranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)

Note that the capabilities outlined above are all key parts of the Identity and Access Management service in any organization. For more information, please see the [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx).

The Rationalized level of Identity and Access Management in the Infrastructure Optimization Model addresses the need for centralized control of configurations and security.

Test 4: Autofit (aka no widths specified)

## Self Assessment

Microsoft has developed a self-assessment tool that you can use to determine your current optimization level. We recommend that you use this tool before proceeding with this guide. The tool is based on the material presented in this guide. To access the self-assessment tool, visit: <http://www.microsoft.com/business/peopleready/coreinfra/ac/default.mspx>.

The following section presents questions for each of the core capabilities that direct you to relevant sections of this planning guide. Your answers to the questions will dictate which sections contain guidance applicable to your organization. Many requirements in the following section have minimum attributes associated with them. If your organization meets every requirement and requirement attribute outlined in this section, you have already achieved the Rationalized level and can proceed to the Dynamic level in Core Infrastructure Optimization. You can print this section as a scorecard for determining which requirements and attributes you need to implement in your organization.

### Capability: Identity and Access Management

The Rationalized level of optimization requires a directory-based tool to centrally administer configurations and security on 80 percent or more desktops in your organization.

|  |  |  |
| --- | --- | --- |
| Requirement: Identity and Access Management | Yes | No |
| Implemented a directory-based tool to centrally administer configurations and security on 80 percent or more of your desktops |  |  |
| Attributes:   * Identified which configurations should be monitored or enforced. * Selected tools for monitoring and enforcing configuration compliance. * Defined Group Policy objects for settings managed through Group Policy. * Implemented Group Policy Management Console to manage Group Policy objects. * Applied Group Policy to at least 80 percent of your desktops. | | |

For more details, see [Centralized Directory-based Configuration and Security](#_Centralized_Directory_Based) in this document, or visit the following Web sites:

* [Windows Server 2003 Active Directory Technology Center](http://www.microsoft.com/windowsserver2003/technologies/activedirectory/default.mspx)
* [Windows® XP Security Guide](http://go.microsoft.com/fwlink/?linkid=14839)
* [Windows Vista Security Guide](http://go.microsoft.com/fwlink/?linkid=74027)
* [Windows Server 2003 Technical Library](http://technet2.microsoft.com/WindowsServer/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx?mfr=true)
* [Microsoft Operations Framework Configuration Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcfgmg.mspx)
* [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx)
* [Medium Business Solution for Management and Security using Active Directory Group Policy](http://www.microsoft.com/downloads/details.aspx?FamilyId=BB534B41-B413-4483-9097-879F5CAFE2DC&displaylang=en)

Additional information is available at [Medium Business Solution for Client Configuration](http://www.microsoft.com/technet/solutionaccelerators/smbiz/mits/cc/mit_cc.mspx).

Capability: Identity and Access Management

# Introduction

Identity and Access Management is a Core Infrastructure Optimization capability and the foundation for implementing many capabilities in the Infrastructure Optimization Model.

The following table lists the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in Identity and Access Management.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Difficult to enforce IT policies required by the organization or regulations  No way to enable a known, stable, and secure state for client PCs  **IT Challenges**  No centralized policy control for identity and access management—implementing broad policy changes requires modification of each identity  Identities are centrally administered, but difficult to manage users and resource settings, configurations | **Projects**  Identify and define configuration standards requiring enforcement  Implement a centralized, directory-based policy solution for administration of desktops, servers, configuration, and security | **Business Benefits**  Enforced, known state of environment  Consistent user experience across PCs based on business role  Easier to modify system and add functionality  Reduced operations and desktop support costs  Reduced user downtime and disruption  **IT Benefits**  Reduced workload due to introduction of role-based administration/group policy  Improved security by implementing policy-based patch management and security lockdown  Profile management allows user system and data recovery |

Ongoing Identity and Access Management focuses on the following capabilities as outlined in the Microsoft Identity and Access Management Series:

* The Foundation for Identity and Access Management
* [Fundamental Concepts](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Fund.mspx)
* [Platform and Infrastructure](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Plat.mspx)
* Identity Life-Cycle Management
* [Identity Aggregation and Synchronization](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P2Ident.mspx)
* [Password Management for Intranet and Extranet](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2pass.mspx)
* [Provisioning and Workflow](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* Access Management and Single Sign-On
* [Intranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* [Extranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)

Note that the capabilities outlined above are all key parts of the Identity and Access Management service in any organization. For more information, please see the [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx).

The Rationalized level of Identity and Access Management in the Infrastructure Optimization Model addresses the need for centralized control of configurations and security.