

Infrastructure Planning and Design (IPD)

Windows Optimized Desktop Scenarios Assessment

Version 1.1

Published: June, 2009

For the latest information, please see
microsoft.com/technet/**SolutionAccelerators**

Copyright © 2009 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, AppLocker, BitLocker, BitLocker To Go, BranchCache, Excel, Hyper-V, Outlook, RemoteApp, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[The Infrastructure Planning and Design Series Approach 1](#_Toc232483022)

[Executive Overview of the Windows Optimized Desktop Scenarios 1](#_Toc232483023)

[Current IT Challenges 1](#_Toc232483024)

[New Desktop Technologies Available to Address the Challenges 2](#_Toc232483025)

[The Need for User Segmentation 2](#_Toc232483026)

[About This Solution Accelerator 2](#_Toc232483027)

[The Guide 2](#_Toc232483028)

[The Tool 3](#_Toc232483029)

[What’s New in Version 1.1 3](#_Toc232483030)

[Feedback 3](#_Toc232483031)

[The Decision Process 4](#_Toc232483032)

[Step 1: Understand the Windows Optimized Desktop Scenarios 5](#_Toc232483033)

[Office Worker Scenario 5](#_Toc232483034)

[Mobile Worker Scenario 6](#_Toc232483035)

[Task Worker Scenario 8](#_Toc232483036)

[Contract Worker Scenario 9](#_Toc232483037)

[Access from Home Scenario 10](#_Toc232483038)

[ScenarioVariations 11](#_Toc232483039)

[Summary of All Scenarios 11](#_Toc232483040)

[Step 2: Identify the Target User Population 12](#_Toc232483041)

[Task 1: Determine Location Scope 12](#_Toc232483042)

[Task 2: Identify User Segments 12](#_Toc232483043)

[Step 3: Match User Groups with Scenarios 13](#_Toc232483044)

[Task 1: Review the Windows Optimized Desktop Scenario Selection Tool Questions 13](#_Toc232483045)

[Task 2: Run the Windows Optimized Desktop Scenario Selection Tool 15](#_Toc232483046)

[Task 3: Record the Results 16](#_Toc232483047)

[Step 4: Preview the Scenario Solutions 17](#_Toc232483048)

[Scenarios Mapped to Products and Technologies 17](#_Toc232483049)

[Challenges Mapped to Solutions 17](#_Toc232483050)

[Step 5: Evaluate Relevant Windows Optimized Desktop Scenarios 23](#_Toc232483051)

[Conclusion 23](#_Toc232483052)

[Key Takeaways 23](#_Toc232483053)

[Appendix A: Products and Technologies 24](#_Toc232483054)

[Appendix B: Virtualization Technologies 31](#_Toc232483055)

[User State Virtualization 31](#_Toc232483056)

[Presentation Virtualization 32](#_Toc232483057)

[Application Virtualization 33](#_Toc232483058)

[Client-Hosted Desktop Virtualization 34](#_Toc232483059)

[Server-Based Desktop Virtualization (VDI) 35](#_Toc232483060)

[Acknowledgments 37](#_Toc232483061)

# The Infrastructure Planning and Design Series Approach

This guide is one in a series of planning and design guides that aim to clarify and streamline the infrastructure planning and design process for Microsoft® infrastructure technologies.

Each guide in the series addresses a unique infrastructure technology or scenario. These guides include the following topics:

* Defining the technical decision flow (flow chart) through the planning process.
* Describing the decisions to be made and the commonly available options to consider in making the decisions.
* Relating the decisions and options to the business in terms of cost, complexity, and other characteristics.
* Framing the decision in terms of additional questions to the business to ensure a comprehensive understanding of the appropriate business landscape.

The guides in this series are intended to complement and augment the product documentation. The guides are available at [go.microsoft.com/fwlink/?LinkId=100915](http://go.microsoft.com/fwlink/?LinkId=100915).

# Executive Overview of the Windows Optimized Desktop Scenarios

Organizations today face the challenge of maintaining rigorous controls over their computing environments while providing the power and flexibility users need to be productive. User and IT goals can sometimes appear to be in conflict. Optimizing the corporate desktop environment resolves this conflict by providing IT the manageability it requires while giving users the varying levels of power and flexibility they need.

The Windows Optimized Desktop scenarios relate the business requirements (IT and user) for a flexible, efficient, and managed desktop environment to sets of complimentary Microsoft technologies by defining and using five standard user scenarios that map business requirements to technology solutions.

## Current IT Challenges

The challenges for IT encompassed in the need for management controls and users’ needs for computing power and flexibility are many, especially when the need for efficiency in resource use is added. Goals include:

* Increase compliance with security, privacy, and auditing requirements by centralizing data and securing the desktop.
* Meet user expectations for a flexible workplace that travels with them from office to office and terminal to terminal.
* Rapidly deploy (and remove) desktop environments for contingent staff on and off premise in a secure manner.
* Extend the life of older hardware, thus avoiding the dumping of electronics into landfills and further harming the environment.

## New Desktop Technologies Available to Address the Challenges

New desktop technologies from Microsoft offer a variety of options to help address these challenges. They can improve desktop flexibility, increase availability, and boost the productivity of end users. They can also help reduce cost, address compliance requirements, accommodate contingent staff, and support green initiatives.

**Note** This guide refers to the specific products and technologies that support the Windows Optimized Desktop scenarios. For a list of these technologies and brief descriptions of how each one contributes to the overall solution, see Appendix A, “Products and Technologies.”

## The Need for User Segmentation

Organizations that wish to make use of the new technologies need to account in their planning for the different business requirements that apply to individual users’ computing environments. Any particular environment can vary in both the types and degree of management controls that IT needs, and the types and degree of flexibility and access to resources that the user needs. Yet, customizing the desktop experience for each user is usually not feasible.

Microsoft has therefore identified five core scenarios: Office Worker, Mobile Worker, Task Worker, Contract Worker, and workers who need to Access from Home that segment users according to their work situations. These scenarios cover most desktop user situations, and describe the business requirements that apply to that situation, including both the individual user’s needs and the IT management needs. Each scenario puts a different emphasis on computer equipment, applications, security, and networking. These scenarios give IT a workable approach to optimizing the organization’s desktops without needing to customize desktops on an individual user basis.

**Note**    It is important to remember that “one size does not fit all.” The scenarios described will not necessarily meet all the needs of any given organization; some customization might be required. Also, the expectation is that some users will transition across more than one scenario as part of their daily activities. In such cases the organization may decide to provision all of the Windows Optimized Desktop scenarios that apply.

# About This Solution Accelerator

This Solution Accelerator helps organizations identify the Windows Optimized Desktop scenarios that are relevant for them, so they can match the scenario solutions (the technologies) to their needs.

Version 1.1 of this Solution Accelerator, Windows Optimized Desktop Scenarios, includes two components:

* *Windows Optimized Desktop Scenario Assessment* (this guide)
* Windows Optimized Desktop Scenario Selection Tool

## The Guide

The assessment guide helps IT pros optimize desktops within their organization by providing a systematic process for understanding the scenarios, identifying target user populations, and matching these populations to user scenarios. The guide describes a few recommended variations for some specific scenarios and provides a preview of the integrated technology solutions associated with each scenario. After the scenarios have been identified, organizations can proceed to plan for deploying the indicated technology solutions

The intended audience for this guide is IT infrastructure specialists who are responsible for planning and designing the client platform infrastructure for their organization. The guide assumes that the reader’s organization is considering a Windows Desktop Optimization project. IT pros who will implement the selected scenario solutions will also find the guide helpful to understand the planning and designing context for the project.

## The Tool

The Scenario Selection Tool is an Excel tool that helps IT pros take a systematic approach to identifying the most appropriate scenario for a given organizational segment by considering user and business requirements.
**Note**   Because most organizations have a varied environment, more than one Windows Optimized Desktop scenario will likely apply. From an IT planning perspective, the organization should prepare to support more than one scenario.

## What’s New in Version 1.1

The Version 1.1 release of this Solution Accelerator reflects the additional functionalities provided by Windows 7 and Windows Server 2008 R2. A detailed listing of Windows 7 and Windows Server 2008 R2 functionality is included in the Appendix.

## Feedback

Please direct questions and comments about this guide to satfdbk@microsoft.com.

# The Decision Process

This guide addresses the following decisions and activities that need to occur to prepare for a Windows Desktop Optimization project.

* Step 1: Understand the Windows Optimized Desktop scenarios
* Step 2: Identify the target user populations for which you want to optimize desktops
* Step 3: Match user groups with scenarios
* Step 4: Preview the scenario solutions
* Step 5: Evaluate relevant Windows Optimized Desktop scenarios

The following figure provides a graphical overview of the steps to select the Windows Optimized Desktop scenarios that best fit the user groups in an organization.



Figure 1. The Windows Desktop Optimization assessment decision flow

# Step 1: Understand the Windows Optimized Desktop Scenarios

The Windows Optimized Desktop uses five scenarios that are characterized by one or more of the following attributes:

* Roles that the user has within the organization, the location or locations in which they work, and the type of computer and applications they use.
* Complexity of the user’s workflow.
* Organizational challenges that IT faces.

This section describes each of the scenarios from a user and IT perspective to provide context for use of the Windows Optimized Desktop Scenario Selection Tool. The “Preview the Scenario Solutions” section later in this guide describes the underlying technologies that address the challenges for each of these scenarios.

## Office Worker Scenario

The Office Worker scenario includes roles such as physician, architect, and research analyst. These users typically perform work that requires a stationary desktop computer within an office, or designated workspace, although they might also access multiple computers during the day if they roam from one floor or office to another within a workplace.

### Typical Work Patterns

Office workers perform complex workflows that require multiple computer applications and tools, most of which must run locally on the desktop computer. These programs provide rich user experiences and might impose a high demand on computing resources for best performance. The desktop computer must have sufficient resources such as CPU, memory, and disk space to run these complex applications.

Examples of office workers include:

* A physician performs the majority of diagnostics, filings, and documentation within an office in a hospital, or even within the patient examination room. The physician may run concurrent applications such as the hospital’s electronic medical record system, pharmaceutical system, Microsoft Office Outlook® 2007 for e-mail and scheduling, and Microsoft Office Word 2007 for documentation. Physicians might need to access these programs from several different locations, including their office, a nursing station, or the patient examination room.
* An architect works primarily at a design studio using CAD, ray tracing software, and a building code database simultaneously.
* A research analyst conducts engineering analysis in a lab or in an office cubicle in a building at a corporate campus. The research analyst may actively and simultaneously use sequence analysis and visualization software, a trials database application, Microsoft Office Excel® 2007, and Office Outlook 2007 for e-mail and scheduling.

### Challenges for IT

Organizations that have users who fit the Office Worker scenario face the following challenges:

* **Support application-specific security and regulatory compliance efforts**. Office workers typically have differing levels of access to confidential information within their organization. This confidential information can include both sensitive data and the applications that access sensitive data. IT needs to ensure that office workers can access the information they need to do their job, while restricting access to confidential information. IT might also need to enforce policies around the local storage and processing of sensitive applications or information, so that office workers can access confidential information without it being stored on the local computer.
* **Ensure PC integrity by allowing installation of only approved applications and devices**. Users who run unauthorized software can experience a higher incidence of malware infections, generate more help desk calls, and undermine efforts to standardize corporate desktops. With the vast number of applications available on the Web, IT professionals need sophisticated tools to ensure that office workers run only approved, licensed software.
* **Secure confidential local data**. At each work location, stationary desktop computers and their hard drives are at risk for loss, which increases the vulnerability of the company’s confidential data. Physical security is typically in place to protect these locations from theft; however, threats exist from internal sources including people who have access to the facilities. Confidential data can be exposed at a variety of times, including during a significant business event such as a merger and acquisition, during a routine event such as an equipment refresh, or residual data on the drives could be exposed when the computer is discarded at the end of its life.
* **Maintain high levels of continuity**. Office workers expect highly available systems. When problems arise, they require immediate response for triage and repair, and demand rapid restoration of services. This applies to deployment of applications to address application fixes, and restoration of local files and preferences.
* **Provide flexibility to access multiple desktop computers**. Office workers occasionally need to access different desktop computers as they work or as part of an exception process. To maintain productivity, users are best served if their preferences, desktop icons, files, and even key applications, are available on different computers. This provides them with a familiar and seamless desktop experience without requiring them to access their principal desktop computer.
* **Address compatibility issues between applications or between an application and the operating system**.Officeworkers need to use specific applications to solve critical issues, but such applications may not be supported on the latest operating system, or may have interoperability issues with existing applications. By resolving application compatibility issues, organizations can benefit from deploying the latest operating system and still provide the applications that users need to be productive.
* **Improve data access responsiveness for workers in low-bandwidth locations**.The number of branch offices—as well as the number of employees who visit those branch offices—is also increasing rapidly. However, the productivity of branch office users can be negatively affected by network bandwidth limitations and latency in response times. Providing faster access to remote files for office workers in low-bandwidth locations will increase user productivity and reduce strain on corporate networks.

## Mobile Worker Scenario

The Mobile Worker scenario focuses on users who require a mobile computer and whose work requires them to travel between offices, often outside the corporate network. They have similar needs and challenges to office workers. However, unlike office workers, mobile workers do not have a consistent high-speed connection to the corporate network.

Mobile worker roles include outside sales, professional services consultants, and field engineers. These users typically perform work that requires mobile computers, which they connect to the corporate network when they return to their office, or occasionally connect to the company network remotely via VPN.

### Typical Work Patterns

Like many office workers, mobile workers perform complex workflows that require multiple computer applications and tools that run locally on the computer. These programs often provide rich user experiences and might impose a higher demand on computing resources for best performance. These applications must be able to perform their specific functionality without needing to be connected to the company’s network.

Examples of mobile workers include:

* A sales account executive who connects to the company network to synchronize the daily reference data such as tax rates and price sheet information then logs off from the corporate network for the remainder of the day to meet with clients and prospective customers at their offices. This account executive might run the company’s customer relationship management (CRM) software, electronic product catalog, Office Outlook 2007 for e-mail and scheduling, and Office Word 2007 for contracts and documentation. The executive might also need to travel to and conduct business in foreign countries.
* A professional services consultant who is engaged in a project might principally work at a customer’s site and visit the main office infrequently. The consultant will generally connect to the company’s offices via VPN but will connect directly to the company’s network when in the main office, which may be infrequently. The consultant could have a process modeler tool, analytics software, and Microsoft Office for documentation, e-mail and presentations.
* Field engineers can be deployed to many locations during the day; however, they start and end their work day at the company offices. The field engineer actively uses a field-replaceable unit parts database, diagnostics and trace tools, and a forms application to track the work and components he had to deploy.

### Challenges for IT

Organizations that have users who fit the Mobile Worker scenario face the following challenges:

* **Provide offline access to files and data**. At a customer site, or just working away from the company’s office, mobile workers need to be able to quickly access their key files and directories. These critical assets should be up to date, and have high integrity without having to burden mobile workers with manual copying and manual synchronization.
* **Ensure PC integrity by allowing installation of only approved applications and devices**. Users who run unauthorized software can experience a higher incidence of malware infections, generate more help desk calls, and undermine efforts to standardize corporate desktops. With the vast number of applications available on the Web, IT professionals need sophisticated tools to ensure that office workers run only approved, licensed software.
* **Secure confidential local and portable data**. The mobile computer, its hard drives, and portable drives such as USB flash disks, are at risk for loss, which can expose the company’s confidential data. Mobile workers are more prone to having a mobile computer lost or stolen given the amount of transport and physical handling. Analysts believe hundreds of thousands of mobile computers are lost or stolen each year. Likewise, confidential data can be exposed at a variety of times, including during a significant business event such as a merger and acquisition, during a routine event such as an equipment refresh, or residual data on the drives could be exposed when the computer is discarded at the end of its life.
* **Support application-specific security and regulatory compliance efforts**. IT needs to ensure that mobile workers have access to the information they need to do their job, while restricting access to confidential information. This constraint might require that sensitive applications be run from an internal server, and confidential information be stored there too so that data is not sent across the Internet or stored on the user’s computer. Another challenge with respect to mobile workers is that they might need to access confidential corporate data even when they travel to other regions of the world. Corporate policies could prevent mobile workers from carrying confidential data on mobile computers when they travel to regions where they cannot control who can inspect their computer. In such cases, mobile workers need to be able to access confidential information without it being stored on the local computer.
* **Maintain high levels of continuity**. Mobile workers expect highly available systems. When problems arise, they require immediate response for triage and repair, and demand rapid restoration of services. Given the increased rate of loss and theft of mobile computers, this also applies to deployment of a new mobile computer. In order to have high levels of continuity and restore productivity to the user, the new mobile computer should have the same applications, local files and preferences as the one being replaced.
* **Address compatibility issues between applications or between an application and the operating system**. Mobileworkers need to use specific applications to solve critical issues, but such applicationsmay not be supported on the latest operating system, or may have interoperability issues with existing applications. By resolving application compatibility issues, organizations can deploy the latest operating system while still providing the applications that users need.
* **Manage mobile computers and provide access to corporate resources outside of the office**. Mobile Workers travel most of the time and are frequently outside the corporate network. While it is important for mobile workers to be able to connect to internal corporate applications and intranet sites quickly and easily, it’s also important for IT to be able to manage mobile computers and push updates to them, regardless of where they are physically.
* **Improve data access responsiveness for workers in low-bandwidth locations**.The number of branch offices—as well as the number of employees who visit those branch offices—is also increasing rapidly. However, the productivity of branch office users can be negatively affected by network bandwidth limitations and latency in response times. Providing faster access to remote files for office workers in low-bandwidth locations will increase user productivity and reduce strain on corporate networks.

## Task Worker Scenario

The Task Worker scenario focuses on employees who have task-specific roles, such as call center analyst, warehouse worker, or retail employee. These users typically perform work that requires a stationary computer. They perform repetitive tasks within a small set of applications, and work within a shared space with other people in similar roles.

### Typical Work Patterns

Task workers typically require no more than one or two applications throughout their work day. Unlike the programs that office workers and mobile workers use, these programs provide a simplified and streamlined user experience to help task workers complete their work rapidly. For example, during one shift, a call center analyst runs a single customer care application, a warehouse worker uses a logistics data entry application, and a retail employee uses a single application to provision and activate a new cell phone. The computers are typically well-managed so the user cannot install other applications or customize the environment.

Examples of task workers include:

* A call center analyst who works during the 5 PM to 3 AM shift shares the office space and terminal with other analysts. Such a task worker may log on to a different terminal each night. Regardless of the terminal the analyst logs on to, the task worker will need to access their specific desktop environment.
* A warehouse worker has a designated computer in the warehouse office that initiates the start and end of an inventory workflow. The worker uses only one module within the ERP suite, and that is the only application that runs on that computer.
* A retail employee has a workstation within the store to conduct point-of-sale transactions. The workstation runs only one application, but it is accessed by multiple retail employees.

### Challenges for IT

Organizations that have users who fit the Task Worker scenario face the following challenges:

* **Deliver a low-cost hardware solution that maintains high user productivity**. An organization that matches this scenario, such as a call center, usually has a large number of employees. The large number of users can make deploying and managing standard desktop computers a significant cost burden because the call center analysts will not use the full capabilities of the desktop computers. At the same time, the solution should provide a responsive and familiar experience that is similar to a standard desktop to maintain user productivity.
* **Support application-specific security and regulatory compliance efforts**. How task workers access and handle data must adhere to regulatory compliance policies. There are typically a large number of users within a task worker organization, and they usually handle a significant volume of customer data interactions. This volume of data access creates a challenge for IT to have technical and supervisory controls that don’t overburden the users. Fortunately, task workers typically operate together within centralized organizations.
* **Provide flexibility to access multiple computers**. Task workers occasionally need to access different computers when their shift changes, or as part of their regular daily workflow. To maintain productivity, users are best served if their preferences are available on that different computer. This provides them with a seamless and identical experience regardless of which computer they use.
* **Ensure PC integrity by allowing installation of only approved applications and devices**. The productivity of task workers can be negatively affected by extraneous applications or devices connected to their computers. IT must ensure that task workers are running only approved applications and devices on their work PCs.

## Contract Worker Scenario

The Contract Worker scenario focuses on organizations that have staff from vendors and outsource companies. These workers may connect to the corporate network from computers that are outside the control of the IT department yet still access sensitive applications or data.

### Typical Work Patterns

Contract workers typically have a temporary relationship with the organization. They may require a high end computer and local administrative access to develop applications. During their contract with the organization, these workers may also need to access and work with confidential and proprietary information while outside the immediate facility or beyond the control of the organization.

Examples of contract workers include:

* A group of software developers are employees of an outsource development company. They use computers owned by their company to access their client’s network and data. They need administrator access to their computers to complete unit testing. The client has no direct control over the computers to ensure they meet security requirements or that they have the right version of the development software and libraries.
* A contract accountant is hired by a client to work onsite at their headquarters offices. The accountant requires access to highly confidential company information to complete the work. The longer it takes to provision a client workstation for the contract accountant, the higher the cost the customer will incur.

### Challenges for IT

Organizations that have users who fit the Contract Worker scenario face the following challenges:

* **Deliver a low-cost hardware solution that maintains high user productivity**.An organization that fits this scenario might outsource software development to a team of contract developers. The hiring team might need to provide each developer with an IT-managed computer, but doesn’t want to incur the hardware cost associated with standard desktop computers. This also allows IT to provide low-cost desktop computing to workers in hostile physical environments -- such as dusty factory floors and medical emergency rooms -- where a typical PC would quickly sustain damage.
* **Maintain privacy and confidentiality**. Contract workers often perform activities that require administrative privileges on the local computer and access to company-sensitive information. How contract workers access and handle data must adhere to policies designed to protect company security interests. Contract workers might operate centrally as a group or distributed and work in diverse locations. They may be out of the direct control of the client, which is a challenge for IT to have technical and supervisory controls that don’t overburden the users.

## Access from Home Scenario

The Access from Home scenario extends the Office Worker scenario to provide these users the familiar experience of their office desktop computer from their home computer when they are unable to be in the office. The users who leverage the Access from Home scenario have identical needs and challenges to office workers; however, their home computer is not under the direct control of IT, might have different versions of Windows® or applications than the corporate standards, and they rely on a high-speed network connection from their personal home computer.

### Typical Work Patterns

The Access from Home scenario is designed to provide office workers access to applications and data; however, because they perform complex workflows that require extensive resources, some limitations may be imposed by remote access from home.

Examples of the Access from Home scenario include:

* A CEO has a sick child and can’t come to work for several days. The CEO needs to have immediate access to the company’s suite of applications from home, as well as access to sensitive data, while also having the familiar work environment to ensure instant productivity.
* A human resources administrator who is caught in a storm and can’t physically drive to the office needs to complete annual employee reviews. The administrator needs to use several applications to perform this work and also needs secure access to employee records, which might be saved on their desktop or their Documents folder.

### Challenges for IT

Organizations that have users who need the Access from Home scenario face the following challenges:

* **Support application-specific security and regulatory compliance efforts**. Users who access the corporate network from home likely do so from privately owned computers. These computers are typically unmanaged by the IT department. As a result these computers might not meet corporate policy requirements (for example they might not have the latest security updates and antivirus software).
* **Provide emergency access from home**. The principal driver of the Access from Home scenario is to provide secure remote access to a standard corporate environment and set of applications from the user’s home (non-managed) computer when the user is unable to work in the office due to illness or other emergencies.

## ScenarioVariations

For some of these scenarios, there may be one or more variants that include centralized execution of the entire desktop environment, depending on the needs of the organization. There is no “one size fits all” solution; organizations can choose to implement more than one virtualization solution to best meet the needs of their users. The Windows Optimized Desktop Scenario Selection Tool will indicate which specific conditions lead to scenario variations, and will display multiple options in the results.

## Summary of All Scenarios

The following list briefly summarizes the scenarios.

* **Office Worker**. These users are always connected to the corporate network and expect a rich client experience that can handle the broad range of tasks for which they are responsible. They use applications such as Microsoft Office and various line-of-business (LOB) applications that run on the local computer. These users include analysts, architects, researchers, and doctors.
* **Mobile Worker**. These types of users are highly mobile due to travel requirements, and frequently work outside the corporate network. They use a variety of applications that usually run locally on their mobile computer and, therefore, require a rich computing experience. These users need to be able to access applications and data offline, but also carry a higher risk of loss of data if their computer is lost or stolen. These users include sales people and account executives.
* **Task Worker**. These users perform a narrow set of tasks and use systems that are connected to the corporate network. Task workers usually do not have a dedicated desktop computer; instead, they leverage a pool of designated computers to access one or a few applications. These users include call-center analysts, warehouse workers, and retail employees.
* **Contract Worker**. These users are vendor or contract staff, often software developers, who perform a broad set of activities that require significant access to the local operating system. They work on corporate-owned intellectual property, but might be physically outside the realm of IT control. They typically use applications such as software development suites, testing tools, and project management tools. These users include software developers (onshore or offshore) and contingent staff.
* **Access** **from** **Home**. This usage scenario is for non-mobile employees who are not able to get to the office and need access to their personalized computer work environment, including applications and data. The IT department needs to ensure that corporate data remains protected and that the computing environment remains well controlled.

# Step 2: Identify the Target User Population

In order to match your users to the scenario that best captures their requirements, you will need to determine which parts of the organization’s environment to include in the infrastructure design, and establish the objectives of the project. These decisions will drive your use of the Windows Optimized Desktop Scenario Selection Tool to determine best fit scenarios.

## Task 1: Determine Location Scope

Planning a Desktop Optimization project begins with establishing the boundaries for which you are building a solution. The starting point of this task is to choose the user population that you are responsible for, which could be the entire enterprise, a geographic area in which your organization operates, or a single department.

Depending on the objective of the project, your goal may be to optimize the desktops of every person within your sphere of influence. Sometimes, however, a business imperative calls for narrowing the scope to a specific user segment. For example, regulations in a country or region might require changing the desktop configurations of the employees in your organization who work within that geographical area to bring them into compliance.

## Task 2: Identify User Segments

Having bounded the total user population for your project, the next step is to divide this population into groups that are likely fits for the scenarios. If your project scope includes the entire enterprise, it is highly likely that a particular requirement that applies to one subgroup of employees does not apply to another. For example, if you have a sales force that consists of in-house telemarketers and sales people who make in-person sales, their requirements will be different so it might be necessary to subdivide them into two groups.

The goal will be to make each group as large as possible while accurately matching a scenario. Each identified group of users will require using the tool to complete an assessment.

Some possible approaches to segmenting users are to:

* Identify individuals with similar job roles.
* Choose a specific team within a division or sub-division.
* Identify users who follow similar workflows.
* Identify staff who have very similar connectivity, application needs, compliance requirements, and access preferences.

# Step 3: Match User Groups with Scenarios

The process of matching user groups with scenarios involves the following tasks.

* Task 1: Review the Windows Optimized Desktop Scenario Selection Tool questions
* Task 2: Run the Windows Optimized Desktop Scenario Selection Tool
* Task 3: Record the results

## Task 1: Review the Windows Optimized Desktop Scenario Selection Tool Questions

This section provides the questions from the Windows Optimized Desktop Scenario Selection Tool. Reviewing these questions will help you to understand the key differentiators that the tool uses to evaluate the applicability of a particular Windows Optimized Desktop scenario (the “Target”) to a user segment. The descriptions (labeled “Comment”) provide insight into the reasoning behind each question.

### User Requirements Questions

The following questions are from the **User Requirements** section on the **Scenario Selection** tab of the Windows Optimized Desktop Scenario Selection Tool. These questions apply to the users in the organization.

1. Do they need rich, locally executing applications that require significant performance and capacity from disk, memory, and graphics on the desktop client computer?

**Comment:** Users who have this need might run resource-intensive programs such as CAD or perhaps a relational database administration tool. The Office Worker scenario would be ideal to solve this challenge. The Mobile Worker scenario might also meet these criteria. **Targets: Office Worker and Mobile Worker**

2. Do they need to roam within the workplace from different computers to access their data and applications?

**Comment:** Users who follow a workflow that requires them to roam frequently within their office are likely to access the same applications on different computers. To preserve the user experience, the settings, files, and state are stored centrally. For example, a doctor might need to access patient information from the office and also the pre-surgery station. The Office Worker scenario would be ideal to solve this challenge. **Target: Office Worker**

3. Do they work in a branch office and need to access multiple corporate web-sites, web-portals, or corporate file shares?

**Comment:** Users who work in branch offices often experience latency in data response times due to distance from headquarters or limited bandwidth. This can adversely affect the productivity of Office Workers who are assigned to branch offices. This can also affect the productivity of Mobile Workers when they are in branch offices. For example, a bank loan officer who works at a remote branch must download a large file containing sales data daily. The Office Worker scenario could fulfill this need. **Target: Office Worker, Mobile Worker**

4. Do they work outside the office for a significant amount of time (for example, to visit customers or travel) and require access to their applications, data, and the corporate network?

**Comment:** Unlike an office worker, the mobile worker must perform specific work functions without a consistent connection to the Internet. For example, a field engineer works at numerous locations throughout the course of the day. The engineer needs to use diagnostic tools and database application without being connected to the Internet. **Target: Mobile Worker**

5. Do they perform a single job function that is highly repetitive, requires a single LOB application, and does not require personalized desktop settings?

**Comment:** Users who regularly access a specific set of applications and who do not require access to a rich desktop or additional network services can utilize a task-oriented environment. This allows the user to access only those specific applications needed to complete their tasks and share multiple client computers as needed. **Target: Task Worker**

6. Are they vendor staff who work either at your local job site or remotely?

**Comment:** Contract workers on temporary or offshore engagements who do not require dedicated computers will be provided with virtual desktop environments to complete their assignments. These virtual environments allow local administration (when needed) for the installation and customization of applications in a managed desktop environment that is provisioned only for the duration of the project. **Target: Contract Worker**

7. Does the organization require that no confidential information be stored on any contractor-owned computer?

**Comment:** Depending on the nature of the business, organizations must adhere to localized government regulations (for example, Sarbanes-Oxley, EUDPD, GLBA, PCI or HIPAA) and pass those same control requirements to their vendors and contractors for their systems and processes that manage confidential, financial or personal information. The solution can be to provision a Virtual Desktop Infrastructure (VDI) that allows contractors to work on confidential information without it being stored locally on their computers. **Target: Contract Worker**

8. If they are unable to get to their workplace, do they need to be able to use their home computer to access the important applications, data, and settings that their office or business computer provides?

**Comment:** In cases where an office worker is not able to access their workstation because they can’t get to their office, their lack of productivity can be costly to the organization. The Access from Home scenario provides the user a contingency means to access a remote computer with access to their applications and settings. **Target: Access from Home**

### Business Requirements Questions

The following questions are from the **Business Requirements** section on the **Scenario Selection** tab of the Windows Optimized Desktop Scenario Selection Tool. These questions apply to the business requirements of the users in your organization.

9. Do they need to travel abroad and use sensitive business data, but security policies prevent them from doing so?

**Comment:** A strict compliance requirement prescribes the use of a remote access capability such as Remote Desktop Services or VDI. This question addresses whether the application requires compatibility to a server-based or client-based operating system. If the application can successfully run on a multi-user server platform, Remote Desktop Services might be the solution. However, if the application needs a client operating system, VDI might be an appropriate choice. **Target: Solution Variation: Mobile Worker using Remote Desktop Services**

10. Does your organization have regulatory compliance requirements or policies that require applications to be run from a central server and data to be stored centrally?

**Comment:** When this is the case, business applications and data must only be accessed from a centrally managed desktop environment. To support this requirement, the Office Worker solution using RDS as needed or Mobile Worker using RDS to support compliance policies would apply. **Target: Mobile Worker using RDS**

11. Does your organization have regulatory compliance requirements or policies that require applications and data to remain on a server, but the applications require a client operating system?

**Comment:** Countries that have import restrictions on mobile computers could prevent users who are travelling from importing selected software. For example, an IT consultant travels to Asia where specialized software tools are prohibited. Because network connectivity is available at the job site, the consultant might consider using VDI. **Target: Solution Variation: Mobile Worker using VDI, Office Worker using VDI**

12. Does your organization have regulatory compliance requirements or policies that require applications to be run from a central server and data to be stored centrally, and the users require administrative permissions to perform their work?

**Comment**: If these constraints apply, business applications and data must only be accessed from a centrally managed desktop environment. In addition, users require local administrator privileges in the desktop environment to install new applications or to configure desktop environment settings. These requirements eliminate the option of presentation virtualization using Remote Desktop Services desktop virtualization. The choice that would best apply to this situation would be the Mobile Worker scenario using the VDI solution. **Target: Solution Variation: Mobile Worker using VDI, Office Worker using VDI**

## Task 2: Run the Windows Optimized Desktop Scenario Selection Tool

The Windows Optimized Desktop Scenario Selection Tool is designed to help you identify applicable scenarios, based on user and business requirements, for each user segment within your organization. The tool is included with this guide in the download package.

You may need to run this tool more than once. If your user population is very heterogeneous, you will likely end up with more than one equally applicable scenario. This may indicate that you need to target a narrower user population and rerun the tool on this population.

### About the Tool

The tool is built on Microsoft Office Excel 2003 and has four worksheets, identified by tabs:

* **Introduction**. Introduces the tool and provides general information about the five scenarios.
* **Instructions**. Provides quick instructions for using the tool.
* **Scenario Selection**. Uses your input to help you select the most appropriate Windows Optimized Desktop scenarios.
* **Calculation Model**. This tab, which is hidden by default, reveals the scoring system of the tool.

Only the **Scenario Selection** tab requires user input. Questions on this tab are organized around two sets of requirements:

* User Requirements
* Business Requirements

Your answers to these questions result in points added to or subtracted from one or more of the scenarios and variations, depending on how well they meet the requirement.

**Note**   To get the best results from the tool, you may need to consult different experts within your organization who are familiar with your business and technical requirements.

#### How Scoring Works

As you make selections, the tool calculates the points and indicates best fit scenarios by the tallest bars in a graph shown on the **Scenario Selection** tab.

* The tool calculates the total number of points for each scenario.
* It also calculates the percentage of points for each scenario, which reveals the relative distribution of scenarios within the user population considered (displayed on the graph).
* The formula used for calculating the percentage of points for each scenario is as follows:

Total points for the scenario \* 100
Total points for all scenarios

**Note**   The Windows Optimized Desktop Scenario Selection Tool helps you identify the most applicable scenarios based on a set of assumptions. If you have specific constraints, you will need to factor for them so that the scenarios you select meet the unique requirements for your organization.

## Task 3: Record the Results

Record the results of using the Windows Optimized Desktop Scenario Selection Tool for your target group of users and repeat the process until all users in scope have been classified into one or more of the Windows Optimized Desktop scenarios.

**Note**There can be exceptions based on specific user situations that necessitate the manual adjustment of an individual from one scenario to another.

You may want to use a table, such as the one illustrated below, to record the results of your assessment activities. This can serve as an inventory of the assessments you have done for future reference.

Table 1. Windows Optimized Desktop Assessment Inventory-example

| **User Name** | **Location** | **Segment** | **Scenario** |
| --- | --- | --- | --- |
| Walter Harp | Bldg A, Rm 100 | HR Department | Office Worker |
| Yolanda Sanchez | Southwest Region | Field Sales Force | Mobile Worker |

### Dealing with Multiple User Groups

In larger enterprises, it is highly likely that a particular requirement is true for one subgroup of employees and not true for another. In these cases, you may want to run the tool for each group, considering one group at a time. (For example, you may determine that the sales force conforms to the Mobile Worker scenario whereas the offshore engineering team conforms to the Contract Worker scenario.)

# Step 4: Preview the Scenario Solutions

This section illustrates the integrated technology solutions from two perspectives:

* How the scenarios map to individual products and technologies
* How the challenges described in the scenarios are addressed by each solution component

This section presents the information in tables for quick and easy reference.

## Scenarios Mapped to Products and Technologies

The following matrix maps the Windows Optimized Desktop scenarios to specific Microsoft products and technologies that address the stated challenges for that scenario.

Table 2. Scenarios Mapped to Products and Technologies



## Challenges Mapped to Solutions

The tables in this section map the specific “Challenges for IT" described for each worker scenario in the “Step 1: Understand the Desktop Optimization Scenarios” section to the Microsoft products and technologies that address those challenges.

Each table contains a horizontal header and two vertical columns. The horizontal header uses abbreviations to indicate to which scenarios the challenge applies. These abbreviations are:

* **O** for Office Worker
* **M** for Mobile Worker
* **C** for Contract Worker
* **T** for Task Worker
* **A** for Access from Home

The horizontal header also lists any assumptions made by the proposed solution. The

vertical columns indicate how specific Microsoft products and technologies address the challenge and list those specific products and technologies.

**Note**   For a brief introduction to these products and technologies, see Appendix A, “Products and Technologies.”

Table 3. Challenge: Support Application-Specific Security and Regulatory Compliance Efforts

| **Applicable Scenarios: O M T A**Application-specific security and compliance requirements can be met by running the sensitive application from a central server and using presentation virtualization to provide access from the local computer. |
| --- |
| **How specific solution components address the challenge** | **Solution Components** |
| Microsoft RemoteApp™ gives the **Office Worker** and **Task Worker** the ability to interact locally with remotely executing applications. Users perceive that their applications run locally when in reality their applications run on a secure and centrally managed remote server.RemoteApp in conjunction with Active Directory® Domain Services (AD DS) can control access to the remote application based on the user’s credentials and helps ensure that sensitive data doesn’t leave the corporate data center. | The **Office Worker** and **Task Worker** scenarios use Windows Server 2008 Remote Desktop Services and RemoteApp. |
| Remote Desktop Services Gateway redirects the **Mobile Worker** on the Internet to a Remote Desktop Services session that runs applications on a central server on the corporate network if access to internally-hosted applications is required.RD Gateway in conjunction with AD DS can control access to the remote session based on the user’s credentials. | The **Mobile Worker** scenario uses Windows Server 2008 Remote Desktop Services and RD Gateway. |
| Microsoft Application Virtualization 4.5 (App-V) allows IT to control which applications get deployed to the user’s local computer through group membership. | App-V for all applicable Windows Optimized Desktop scenarios. |
| The virtual desktop infrastructure enables centralized storage, execution, and management of Windows 7 ‑based virtual machines within the data center. The Remote Desktop Protocol (included with Windows 7) enables **Access from Home** workers to connect to these virtual machines that are hosted within a secure and centrally managed corporate data center. | The **Access from Home** scenario uses Windows Server 2008 Remote Desktop Services, RD Gateway, and VDI (Hyper-V™, System Center Virtual Machine Manager, a third-party connection broker [such as Citrix XenDesktop,] and Windows Virtual Enterprise Centralized Desktop) |

Table 4. Challenge: Secure Confidential Local and Portable Data

| **Applicable Scenarios: O M**Using BitLocker™ to encrypt local operating system and data will protect confidential information. BitLocker To Go™ provides data protection for removable storage devices such as USB flash drives and portable hard drives. |
| --- |
| **How specific solution components address the challenge** | **Solution Components** |
| With respect to the **Office Worker** and **Mobile Worker** scenarios, BitLocker protects confidential data on desktop and mobile computers when the computers are recycled, or are lost or stolen. | Windows BitLocker Drive Encryption and BitLocker To Go for all Windows Optimized Desktop scenarios.  |
| With respect to all scenarios, encrypting the Windows Server operating system will protect confidential data if the data center is compromised, while requiring the encryption of all portable devices will protect data if the devices are lost. |

Table 5. Challenge: Maintain High Levels of Continuity and Provide Flexibility to Access Multiple Desktop Environments

| **Applicable Scenarios: O M T**High levels of business continuity and flexible access to multiple desktop environments can be achieved by centralizing storage and dynamically provisioning applications, application data, user data, and user profiles. |
| --- |
| **How specific solution components address the challenge** | **Solution Components** |
| Collectively, these products and technologies allow users move from one computer to another and continue to work seamlessly because their applications, data, and user profile are dynamically provisioned over the network. This dynamic provisioning and centralized management of data, applications, and settings also enables the “replaceable PC” and "free seating" scenarios.App-V, when used in streaming mode, speeds dynamic provisioning by streaming only those portions of the application that are needed for the first launch.In case of a lost, stolen, or faulty computer, the **Office Worker** and **Mobile Worker** can quickly move to a different computer to resume work with little or no downtime. | Microsoft Application Virtualization 4.5 (App-V), System Center Configuration Manager R2 and Windows 7 (folder redirection, client-side caching, roaming user profiles) for all Windows Optimized Desktop scenarios. |
| In the "free seating" scenario, the **Task Worker** can quickly move between shared terminals and resume work with little or no downtime using Remote Desktop Services. |
| The client-side caching feature of Windows 7 keeps a synchronized copy of the user’s data and profile on the local client computer (for the **Office Worker** and **Mobile Worker**.) |

**Table 6. Challenge: Address Compatibility Issues Between Applications or Between an Application and the Operating System**

| **Applicable Scenarios: O M**Application virtualization can address compatibility issues between applications. Desktop virtualization can allow users to run legacy applications on virtualized environments that host earlier versions of the operating system.  |
| --- |
| **How specific solution components address the challenge** | **Solution Components** |
| App-V enables installation and execution of applications within separate virtual environments. This allows the **Office Worker** and **Mobile Worker** to run applications that are otherwise incompatible with each other and cannot exist within the same desktop environment. | Microsoft Application Virtualization 4.5 (App-V) and Microsoft Enterprise Desktop Virtualization for **Office Worker** and **Mobile** **Worker** scenarios. |
| Microsoft Enterprise Desktop Virtualization allows you to create an instance of a previous version of the operating system in a virtual environment that can be used to host applications that are incompatible with the latest version of the Windows operating system. IT can therefore upgrade the **Office Worker** and **Mobile Worker** to the latest version of the Windows operating system and use Microsoft Enterprise Desktop Virtualization to run incompatible applications. |

Table 7. Challenge: Improve Data Access Responsiveness for Workers in Low-Bandwidth Locations

| **Applicable Scenarios: O M**BranchCache™ in Windows Server 2008 R2 caches content from remote file and Web servers within the branch location, so that any additional users accessing the same content can do so more quickly.  |
| --- |
| **How specific solution components address the challenge** | **Solution Components** |
| When IT enables BranchCache, a copy of data accessed from an intranet site or a file server is cached locally within the branch office. BranchCache supports common protocols for Web content (HTTP and HTTPS) and file servers (SMB), enabling it to work with a wide variety of application types. BranchCache only retrieves data from headquarters when the user requests it. Because it is a passive cache, it decreases bandwidth utilization between headquarters and the branch. This allows the **Office Worker** and **Mobile Worker** who are in low-bandwidth locations to download files quickly. | Microsoft Windows Server 2008 R2 to support the low-bandwidth variation of **Office Worker** and **Mobile Worker** scenarios. |

Table 8.

Challenge: Provide Offline Access to Files and Data

| **Applicable Scenarios: M**Folder Redirection and Offline Files allow anytime access to files stored on a server. |
| --- |
| **How specific solution components address the challenge** | **Solution Components** |
| Folder Redirection and Offline Files provide a convenient way for users to access files stored on a central server when not connected to the corporate network. Windows 7 improves Offline Files performance by reducing initial wait times and enables IT professionals to better manage these technologies. For example, they can use Group Policy to prevent specific types of files (such as music files) from being synchronized to the server. Administrators can also control when offline files are synchronized with the server, set up specific time intervals for synchronization, block-out other times for purposes of bandwidth management, and configure a maximum “stale” time after which files must be resynchronized. | Folder Redirection and Offline Files for the **Mobile Worker** scenario. |

**Table 9.
Challenge: Deliver a Low-Cost Hardware Solution That Maintains High User Productivity
Challenge: Maintain Privacy and Confidentiality**

| **Applicable Scenarios: T C**Organizations can reduce hardware costs by adopting a PC cascade strategy in which old PCs from Office workers are given to Task and Contract Workers. This allows companies to extend the life of existing hardware while maintaining a familiar Windows environment for end users. For newer hardware that can support a modern operating system, organizations can use Windows 7 in conjunction with Remote Desktop Services to connect to centralized servers. **Assumption:** Storing confidential information on a centrally managed server will promote privacy and confidentiality. |
| --- |
| **How specific solution components address the challenge** | **Solution Components** |
| Windows Fundamentals for Legacy PCs is a lightweight operating system that is well suited for older hardware. This operating system supports the Remote Desktop Protocol, thereby enabling users to connect remotely to servers running Windows Server 2008 Remote Desktop Services (for the **Task Worker**), or virtual machines hosted on a Windows Server 2008 Hyper-V Server (for the **Contract Worker**). In this manner, this technology helps extend the life of older hardware. | Windows Fundamentals for Legacy PCs for both the **Task Worker** and **Contract Worker** scenarios. |
| The Remote Desktop Protocol (included with the Windows operating system) enables the **Contract Worker** to use their laptops and **Access from Home** workers to use their home computers to connect to virtual machines that are hosted within a secure and centrally managed corporate data center. Allowing users to connect to centralized desktops increases flexibility for end-users, but does not reduce overall IT infrastructure costs. | Windows Server 2008 Remote Desktop Services, RemoteApp, Hyper-V technology, System Center Virtual Machine Manager, Windows Virtual Enterprise Centralized Desktop for **Contract Worker** and **Access from Home**. |

Table 10.

Challenge: Ensure PC Integrity by Allowing Installation of Only Approved Applications and Devices

| **Applicable Scenarios: O M T**AppLocker™ is a flexible and easily administered mechanism that enables IT professionals to specify exactly what is allowed to run on user PCs.  |
| --- |
| **How specific solution components address the challenge** | **Solution Components** |
| AppLocker provides simple, powerful Group Policy Objects for specifying which applications can run, providing IT professionals with the flexibility to allow users to run the applications, installation programs, and scripts they need to be productive. | Windows 7 AppLocker |

# Step 5: Evaluate Relevant Windows Optimized Desktop Scenarios

Having identified the relevant Windows Optimized Desktop scenarios for your organization and investigated the manner in which the solutions address the challenges of each scenario, your next step should be a formal evaluation of the solutions for the scenarios that apply to your organization.

A formal evaluation would include a pilot study using a prototype deployment and a detailed business study (such as TCO and ROI) involving domain experts such as architects and business planners.

Conclusion

There is a growing expectation that people will be able to work from anywhere and have access to their data at any time. While this increases productivity, it also introduces additional management and security burdens for an organization’s IT department. Although it is important to deliver flexible configurations, provide offline access to data and applications, and enable people to customize their desktop environment, IT departments are also required to manage which applications users should have access to, ensure data is backed up, and provide an option to centrally execute applications that use sensitive data or require high data transfer bandwidth.

Traditionally, the desktop computing model has been one where the operating system, applications, and user data and settings are bonded to a single computer, making it difficult for users to move from one computer to another in case of upgrades or a lost or stolen mobile computer. Depending on the usage scenario and business needs, the right level of balance between user flexibility and centralized control is likely to be different across various organizations and even across user groups within each organization. The Windows Optimized Desktop Scenarios give organizations the ability to choose the client computing scenarios that best meet the unique needs of their businesses.

This assessment guide helps IT pros understand the capabilities of Windows Optimized Desktop technologies, determine which scenario(s) are right for their user communities, and review prerequisites and guidance in planning for desktop virtualization.

## Key Takeaways

After reading this guide and running the Windows Optimized Desktop Scenario Selection Tool, the reader should:

* Understand the different Windows Optimized Desktop scenarios.
* Be able to identify which scenarios apply to their organization.
* Understand the product and technology solutions from Microsoft that address the challenges faced by the organization in terms of relevant Windows Optimized Desktop scenarios.

# Appendix A: Products and Technologies

The Windows Optimized Desktop uses the following Microsoft products and technologies to support desktop optimization.

Windows 7 Enterprise

The Windows Optimized Desktop relies on the following features of Windows 7 Enterprise.

* **Folder redirection**. Allows users and administrators to redirect the path of a folder to a centralized server. This feature provides data protection in the event of local system failure. The data is safe on the central server even if the local computer needs to be completely replaced. The data can also be backed up as part of routine system administration without requiring any action on the part of the user.
* **Roaming user profiles**. Enables the redirection of locally stored data and user profiles to a remote server.
* **Client-side caching**. Provides offline file synchronization capabilities to enable consistent access to local copies of files and data that are usually stored on a remote file server.
* **BitLocker Drive Encryption and BitLocker To Go** provide data protection for storage devices such as hard disk drives and USB flash drives. BitLocker To Go gives system administrators control over how removable storage devices can be used and the strength of protection required. Administrators can require data protection for writing to any removable storage device while still allowing unprotected storage devices to be used in a read-only mode.Through Group Policy, administrators can also require strong passwords or a smart card for protected removable storage devices or control which devices can be connected to the computer at all.
* **DirectAccess** enables users to access the corporate network with their PCs any time they have an Internet connection, without the extra step of initiating a VPN connection.
* **BranchCache** caches content from remote file and Web servers in the branch location so that users can more quickly access this information. The cache can be hosted centrally on a server in the branch location, or can be distributed across user PCs. To take advantage of BranchCache, IT professionals need to deploy Windows Server 2008 R2.
* **AppLocker** is a flexible and easily administered mechanism that enables IT professionals to specify exactly what is allowed to run on user PCs. With this capability, IT professionals can realize the improved security, operational, and compliance benefits of application standardization. AppLocker provides simple, powerful, rule-based structures for specifying which applications can run, providing IT professionals with the flexibility to allow users to run the applications, installation programs, and scripts they need to be productive.
* **Enterprise Search Scopes** provide users with an improved and seamless search experience across local and networked corporate data directly within Windows Explorer.
* **RemoteApp and Desktop Connections** allow users from both managed and unmanaged Windows 7 PCs to easily subscribe to RemoteApp programs, RD Session Host desktops and RD Virtual Host desktops (VDI). Icons for their applications are displayed in the users start menu and automatically kept up to date.

For the Windows Optimized Desktop, Windows 7 Enterprise is an important part of the solution for the following scenarios:

* Office Worker
* Mobile Worker
* Contract Worker
* Access from Home

For more information about Windows 7 Enterprise, see [www.microsoft.com/windows/enterprise/products/windows-7-enterprise.aspx](http://www.microsoft.com/windows/enterprise/products/windows-7-enterprise.aspx)

Windows BitLocker Drive Encryption and BitLocker to Go

BitLocker and BitLocker To Go combine to provide data protection in Windows 7 Enterprise and Windows 7 Ultimate for client computers and in Windows Server 2008 R2. Specifically, these technologies:

* Encrypt all data stored on the Windows operating system volume and configured data volumes. BitLocker To Go encrypts portable drives such as USB memory sticks.
* Use the Trusted Platform Module (TPM) to help ensure the integrity of components used in the earlier stages of the startup process. It "locks" any BitLocker-protected volumes so that they remain protected even if the computer is tampered with when the operating system is not running.
* Provide enhanced protection against data theft or exposure on computers that are lost or stolen, and more secure data deletion when computers that are protected with BitLocker are decommissioned.
* Can be centrally managed via Group Policy.

For the Windows Optimized Desktop, BitLocker is an important part of the solution for the following scenarios:

* Office Worker
* Mobile Worker

For more information about BitLocker Drive Encryption, see
<http://technet.microsoft.com/en-us/windows/aa905065.aspx>

For more information about BitLocker To Go, see:

<http://technet.microsoft.com/en-us/windows/dd408739.aspx>

Microsoft Application Virtualization 4.5 (App-V) and System Center Configuration Manager R2

App-V and System Center Configuration Manager combine the benefits of application virtualization with those of change and configuration management. Specifically, they:

* Enable dynamic provisioning and installation of applications over the intranet and extranet.
* Provide application virtualization capabilities that support continuity. These products combine to enable the user to run an application using a workstation or terminal server without installing the application on the local client operating system. Physical applications install files into the Windows system and Program Files directories, and also make updates to the registry, which can cause file and registry conflicts. Instead of installing files into the Program Files directory and adding entries into the local registry, the virtual application loads into cache and then runs in an isolated virtual environment on the client, so that no changes occur to the local operating system or registry. Office workers are protected from application downtime because application virtualization enables them to access their applications even during unplanned outages or scheduled migration projects. The abstraction from the local operating system allows virtualized applications to be redeployed quickly, without installation, to a replacement or secondary computer, so the office worker can maintain productivity.
* App-V also provides the capability to restore an application’s settings to its original configuration as if it were the first time it was deployed to the desktop computer. This capability lets the office worker perform self-service restoration of an application in the event of misconfiguration on the user’s part.

For the Windows Optimized Desktop, App-V and System Center Configuration Manager are an important part of the solution for the following scenarios:

* Office Worker
* Mobile Worker
* Task Worker
* Contract Worker
* Access from Home

For more information about App-V, see
<http://technet.microsoft.com/en-us/appvirtualization/cc721196.aspx>.

For more information about System Center Configuration Manager, see [www.microsoft.com/configmgr/default.mspx](http://www.microsoft.com/configmgr/default.mspx).

For more information about desktop virtualization, see [www.microsoft.com/windows/enterprise/technologies/virtualization.aspx](http://www.microsoft.com/windows/enterprise/technologies/virtualization.aspx)

Microsoft Enterprise Desktop Virtualization

Microsoft Enterprise Desktop Virtualization enhances deployment and management of virtual images while providing a seamless user experience in a Virtual PC environment independent of the local desktop configuration and operating system. Specifically, it:

* Enables client-hosted desktop virtualization, which provides the Office Worker scenario with the ability to deploy and centrally manage virtual PC images on Windows-based desktops.
* Creates (when used with Microsoft Virtual PC 2007 SP1) the capability to run applications that are not compatible with Windows 7 on a guest virtual machine that runs Windows XP SP2/SP3 or Windows 2000 SP4.
* Provides centralized virtual images management, delivery and update.

For the Windows Optimized Desktop, Microsoft Enterprise Desktop Virtualization is an important part of the solution for the following scenarios:

* Office Worker
* Mobile Worker

For more information about Microsoft Enterprise Desktop Virtualization, see [www.microsoft.com/windows/products/windows7 /enterprise/medv.mspx](http://www.microsoft.com/windows/products/windowsvista/enterprise/medv.mspx).

Virtual Desktop Infrastructure (VDI)

Virtual Desktop Infrastructure (VDI) is the technology that lets users access a full desktop environment remotely. With VDI, physical CPU, memory and disk capacity can be allocated to particular users, which prevents the actions of one user from affecting the experience of other users. Specifically, VDI:

* Enables centralized storage, execution, and management of Windows 7 ‑based virtual machines within the data center.
* Uses Microsoft Hyper-V Server to host virtual machines
* Uses Remote Desktop Services and RD Connection broker to manage user connections to the virtual machines
* Uses System Center Virtual Machine Manager to manage hosted virtual machines. These virtual machines run the Windows 7 operating system under the Windows Virtual Enterprise Centralized Desktop license.

For the Windows Optimized Desktop, VDI is an important part of the solution for the following scenarios:

* Office Worker
* Mobile Worker
* Contract Worker
* Access from Home

For more information about VDI, see [www.microsoft.com/virtualization/solution-product-vdi.mspx](http://www.microsoft.com/virtualization/solution-product-vdi.mspx).

New for Windows Server 2008 R2: Terminal Services is now Remote Desktop Services

Remote Desktop Services (RDS) is the new name for Terminal Services, and reflects the expanded role this feature has in Windows Server 2008 R2. Remote Desktop Services (RDS), one of the core virtualization technologies available in Windows Server 2008 R2, makes it possible to run an application in one location but have it be controlled in another. With RDS presentation virtualization, you can install and manage applications on centralized servers in the datacenter; screen images are delivered to the users, and the user’s client machine, in turn, sends keystrokes and mouse movements back to the server.

Remote Desktop Services is the feature of Windows Server 2008 R2 that provides technologies that enable access to a server running Windows-based programs or the full Windows desktop. Specifically, Remote Desktop Services:

* Decouples an application’s user interface from its execution environment.
* Ensures that only keyboard, mouse, and display information is transmitted over the network. Every user sees only their individual session, which is managed transparently by the server operating system and is independent of any other client session.
* Helps IT efficiently deploy and maintain software in an enterprise environment through this centralized service. This feature is especially relevant for the Task Worker scenario because it supports scaling, especially for LOB applications that are used very frequently and often updated.

For the Windows Optimized Desktop, Remote Desktop Services is an important part of the solution for the following scenarios:

* Office Worker
* Mobile Worker
* Task Worker

For more information about Remote Desktop Services, see [www.microsoft.com/windowsserver2008/en/us/ts-product-home.aspx](http://www.microsoft.com/windowsserver2008/en/us/ts-product-home.aspx).

Microsoft RemoteApp

RemoteApp is a service in the Remote Desktop Services server role of Windows Server 2008 R2 that enables organizations to provide access to standard Windows-based programs executing on the server from virtually any location to users with computers running Windows. Specifically, RemoteApp:

* Allows users to run programs from a RDS server, yet seem as if the programs were running on the local computer, including resizable windows, true multiple monitor support, and notification icons in the system tray area.
* Eliminates confusion between remote and local applications because the application, rather than the entire remote desktop, launches and runs in its own resizable window on the client computer’s desktop.

For the Windows Optimized Desktop, RemoteApp is an important part of the solution for the following scenarios:

* Office Worker
* Task Worker

For more information about RemoteApp, see [technet.microsoft.com/en-us/library/cc731340.aspx](http://technet.microsoft.com/en-us/library/cc731340.aspx). (Note: Terminal Services is now Remote Desktop Services. For more information about the name change, please visit the Windows Server blog at [blogs.technet.com/windowsserver/archive/2008/10/30/TechEd-EMEA\_3A00\_-Terminal-Services-renamed-Remote-Desktop-Services.aspx](http://blogs.technet.com/windowsserver/archive/2008/10/30/TechEd-EMEA_3A00_-Terminal-Services-renamed-Remote-Desktop-Services.aspx).)

Windows Server 2008 Remote Desktop Gateway (RD Gateway)

RD Gateway is a service in the Remote Desktop Services server role of Windows Server 2008 R2 that allows authorized remote users to connect to Remote Desktop Protocol based (RDP) resources on an internal network, from any Internet-connected device. Specifically, RD Gateway:

* Allows authorized workers to connect to resources on an internal corporate or private network from their mobile computer. The network resources can be terminal servers, terminal servers running RemoteApp programs, or computers with Remote Desktop enabled.
* Provides a comprehensive security configuration model that enables IT to control access to specific internal network resources such as a point-to-point RDP connection, rather than allowing remote users to access all internal network resources.
* Enable mobile users to access server-based applications through the Internet without the need for a Virtual Private Network (VPN).

For the Windows Optimized Desktop, RD Gateway is an important part of the solution for the following scenarios:

* Mobile Worker
* Access from Home

For more information about RD Gateway, see [technet.microsoft.com/en-us/library/cc754010.aspx](http://technet.microsoft.com/en-us/library/cc754010.aspx). (Note: Terminal Services is now Remote Desktop Services. For more information about the name change, please visit the Windows Server blog at [blogs.technet.com/windowsserver/archive/2008/10/30/TechEd-EMEA\_3A00\_-Terminal-Services-renamed-Remote-Desktop-Services.aspx](http://blogs.technet.com/windowsserver/archive/2008/10/30/TechEd-EMEA_3A00_-Terminal-Services-renamed-Remote-Desktop-Services.aspx).)

Windows Fundamentals for Legacy PCs

Organizations can use Windows Fundamentals for Legacy PCs to extend the life of older hardware and improve security and manageability. Specifically, this product:

* Reduces the total cost of computer ownership by extending the life of older hardware.
* Increases desktop manageability by using functionality from the Windows XP platform such as Group Policy objects and automated deployment of security updates.
* Reduces the strain on IT, improves end-user productivity, and helps close security gaps.

For the Windows Optimized Desktop, Windows Fundamentals for Legacy PCs is an important part of the solution for the following main scenarios:

* Task Worker
* Contract Worker

For more information about Windows Fundamentals for Legacy PCs, see [www.microsoft.com/licensing/sa/benefits/fundamentals.mspx](http://www.microsoft.com/licensing/sa/benefits/fundamentals.mspx)

Windows Virtual Enterprise Centralized Desktop (VECD)
VECD is a license that allows for hosting Windows 7 Enterprise client desktops on centrally hosted virtual environments.

For the Windows Optimized Desktop, the VECD license is an important part of the solution for the following main scenarios:

* Contract Worker
* Access from Home

For more information about VECD, see
[www.microsoft.com/windows/enterprise/technologies/virtualization-licensing.aspx](http://www.microsoft.com/windows/enterprise/technologies/virtualization-licensing.aspx)

Hyper-V Technology

Windows Server 2008 Hyper-V technology supports microkernel hypervisor architecture to host multiple guest environments running Windows 7 Enterprise. Specifically, Hyper-V technology:

* Provides a high performance, hypervisor-based server virtualization solution that is built right into Windows Server 2008.
* Enables server consolidation of physical systems into virtual machines, business continuity management through virtual machines, the dynamic datacenter with mobile, on-demand workloads, and simplified test and development environments.
* Integrates and leverages Windows technologies, (like Cluster service, and Active Directory Domain Services), and the System Center family of management solutions.

For the Windows Optimized Desktop, Hyper-V technology is an important part of the solution for the following main scenarios:

* Contract Worker
* Access from Home

For more information about Hyper-V technology, see [www.microsoft.com/windowsserver2008/en/us/hyperv.aspx](http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx).

**System Center Virtual Machine Manager**

A member of the Microsoft System Center suite of management products, System Center Virtual Machine Manager 2007 (VMM) enables enterprise-wide management of virtual machines. System Center Operations Manager provides monitoring of virtual machines managed by VMM. Specifically, VMM:

* Enables rapid deployment of virtual machines.
* Provides centralized control of the “building blocks” of the virtual data center.
* Allows for delegated self-provisioning by authorized end users.

For the Windows Optimized Desktop, VMM is an important part of the solution for the following main scenarios:

* Contract Worker
* Access from Home

For more information about VMM, see [www.microsoft.com/systemcenter/scvmm/default.mspx](http://www.microsoft.com/systemcenter/scvmm/default.mspx).

**System Center Operations Manager**

System Center Operations Manager provides an easy-to-use set of capabilities to monitor the health and performance of organization’s infrastructure, services and applications across environments and operating systems. Operations Manager delivers a unified view of that infrastructure for physical and virtual platforms. System Center Operations Manager monitors virtual machines that are managed by System Center Virtual Machine Manager (VMM). VMM includes multi-vendor virtualization platform support, Performance and Resource Optimization (PRO) and enhanced support of “high availability” host clusters. PRO, in conjunction with System Center Operations Manager, uses administrator-set rules and policies to help dynamically react to poor performance or failure of virtualized hardware, operating systems or applications.

For more information about Operations Manager, see [www.microsoft.com/systemcenter/opsmgr/default.mspx](http://www.microsoft.com/systemcenter/opsmgr/default.mspx).

**Connection Broker**

Windows Optimized Desktop scenarios require a server application to serve as a Remote Desktop Services connection broker. Specifically, the connection broker:

* Controls to which Hyper-V guest the client can connect.
* Defines the security access and roles.

For the Windows Optimized Desktop, a connection broker, whether native or third-party, is an important part of the solution for the following main scenarios:

* Contract Worker
* Access from Home

# Appendix B: Virtualization Technologies

Virtualization technologies are an emerging IT capability and are being successfully applied in organizations to address the challenges of more dynamic infrastructure demands, increasing management and security protections, and supporting a more dynamic work environment. This section describes the following virtualization technologies and how they are applied to Windows Optimized Desktop scenarios:

* User state virtualization
* Presentation virtualization
* Application virtualization
* Client-hosted desktop virtualization
* Server-based desktop virtualization (Virtual Desktop Infrastructure, or VDI)

## User State Virtualization

Traditionally, a user’s desktop or mobile computer contains the authoritative copy of their data and settings. User state virtualization separates the user’s data and settings from the physical desktop or mobile computer, and stores this configuration on a protected centralized server in the data center. The data can, of course, be synchronized so a local copy exists for offline use.

User state virtualization enables the following key benefits within the Windows Optimized Desktop scenarios:

* **Data-backup**. In the event that a user’s computer is damaged, lost, or stolen, the central copy of the user’s data and settings are safe and available to provision to a new computer. The user’s settings can be re-applied to a new computer automatically. This rapid provisioning is often referred to as “replaceable PC.”
* **Migration**. When IT migrates users and computers, user state virtualization makes the transition faster and safer. These migrations could be an upgrade from one operating system to another, such as from Windows XP to Windows 7, or moving from one computer to another such as when a user upgrades to a new computer at the end of an equipment lease.
* **Roaming users**. User state migration makes the user’s data and settings available to the user regardless of the computer they use. This enables users to share computers within the organization and maintains the same computing environment when they use another computer on the network. This ability to use multiple computers within the same facility is often referred to as “hot desking”.

User state virtualization is enabled by the following technology components:

* **Roaming user profiles**. A roaming user profile is registry and file-based user configuration data stored in a specific folder structure that follows users as they log on to and log off from different computers. Roaming user profiles are stored on a central server location such as a file server share. At log on, Windows copies the user profile from the central location to the local computer. When the user logs off, Windows copies changed user profile data from the client computer to the central storage location. This ensures that the user’s configuration data follows users as they roam from one computer to another.
* **Folder redirection**. Folder redirection is a feature available in Windows 7 to change the target location for 10 specific folders found within the user profile, including the user’s Documents, Desktop, AppData, and Favorites folders. This redirection is transparent to the user and installed applications, and gives the user a consistent way of saving data, regardless of the location where the data is physically stored. Folder redirection lets administrators separate user files from their roaming user profile data, which decreases data volume and improves profile synchronization. The best way to use folder redirection is in a domain environment using Group Policy.
* **Client-side caching.** Windows 7 provides offline file synchronization capability to enable consistent access to local copies of files and data that are usually stored on a remote file server. Client-side caching is especially important for user state virtualization because it enables offline access to data redirected to a central server while the user is not connected to the network (for example, if the user is a mobile worker accessing files from a laptop while on the road).

## Presentation Virtualization

Presentation virtualization separates application processing from the interface, making it possible to run an application on the server while it is controlled from a virtual session on the user’s desktop. This centralized execution might run only a single application, or it might present the user with a complete desktop with multiple applications. In either case, several virtual sessions from one or many computers can use the same installation of an application.

Presentation virtualization enables the following key benefits within the Windows Optimized Desktop scenarios:

* **Secure data and applications**. Presentation virtualization helps organizations keep critical intellectual property secure by eliminating the need to store sensitive data and applications on the local device. This reduces the risk of data loss when a laptop is lost or stolen, and secures application communications using secure sockets layer (SSL) without a virtual private network (VPN) infrastructure.
* **Accelerate application deployment**. Presentation virtualization helps organizations deploy applications faster by installing the software once on a server rather than on multiple computers, allows access to new operating systems, and delivers rich applications to devices that cannot run them natively.
* **Improve remote worker efficiency.** Presentation virtualization improves remote worker efficiency by increasing server-based application performance over low-bandwidth connections, launching applications from a Web application, and by accessing RemoteApp programs installed on the local computer.

Presentation virtualization is enabled by the following technology components:

* **Windows Server 2008 Remote Desktop Services**. The Remote Desktop Services server role consists of several sub-components known as “role services.” The Terminal Server role service enables a Windows Server 2008–based computer to host Windows-based programs or the full Windows desktop. Users can connect to a terminal server to run programs, save files, and use network resources on that server. The Terminal Service Gateway (RD Gateway) role service enables authorized remote users to connect to resources on an internal network, from any Internet-connected device that can run the Remote Desktop Connection client. The Terminal Service Web Access (RDS Web Access) role service enables users to access RemoteApp programs and a Remote Desktop connection to the terminal server through a Web site.
* **Microsoft RemoteApp (RemoteApp)**.Thisclient software allows users to run programs from a terminal server, yet seem as if the programs were running on the local computer, including resizable windows, drag-and-drop support between multiple monitors, and notification icons in the notification area. The application, rather than the entire remote desktop, launches and runs in its own resizable window on the client computer’s desktop, which eliminates confusion between remote and local applications. RemoteApp lets IT decide whether to deploy applications directly to the client computer or to a centrally managed Terminal Server host. This provides IT with the flexibility to determine the appropriate deployment methodology for each application. For example, an application that is graphically intensive may be better suited for local deployment to an end-point device, where it can directly use the local graphics subsystem of that computer. However, a client/server application that transmits large amounts of data across the network and requires frequent updates may perform much faster in a centrally hosted RemoteApp configuration.

## Application Virtualization

Application virtualization isolates applications from one another to reduce application-to-application compatibility issues. Using application virtualization allows applications to be installed and run without altering the file system or the system registry.

Application virtualization enables the following key benefits within the Windows Optimized Desktop scenarios:

* **Provisioning**. Application virtualization reduces the need to test applications that are installed on a client computer for compatibility with one another. This capability allows IT to provision applications faster, and deploy applications that would not typically be available to users due to version conflicts.
* **Continuity**. The underlying operating system is protected from configuration changes that usually happen during standard application installation. The isolation between applications also inherently enables applications to be reverted to the previously known good state, or the original deployment setting. With App-V, applications are assigned to users. If a user’s computer fails or is lost or stolen, they simply need a new computer and their applications will be available immediately. There is no need for the user to remember which applications were installed or wait hours for the computer to be rebuilt. The applications are available the moment the user logs on to the new computer.
* **Readily accessible applications**. IT can deliver applications that meet the needs of users regardless of whether the users are in the office, on the road, at a remote site, or holding a meeting at the local coffee shop. IT can stream applications to desktops on-demand over the intranet or the Internet. When the application is in cache, users can work offline without interruptions. IT can deliver applications to remote users who do not have network connectivity by using standalone mode for USB and CD installation.
* **Centralize management of applications**. App-V, combined with System Center Configuration Manager, allows IT to centrally manage, publish, and report on applications to end users. The organization receives all the benefits of a full PC life cycle management solution and the ability to manage both physical and virtual applications using the same infrastructure and workflows that are already in place.
* **Roaming user profiles**. App-V enables the user to roam from desktop to desktop and retain both their application and user settings. If the application has already been loaded into cache, each user who has access to the application will use the same cached version; There is no need to re-stream or reload into cache for each individual user.
* **Transparent, dynamic application updates**. To update applications, administrators replace only the changed files on the App-V server. Network-connected end users have immediate access to the latest version without any downtime for application upgrade.
* **End of life**. To decommission an application, administrators simply remove it from the App-V server and clear the client cache. To remove a particular user's rights, administrators remove access from Active Directory Domain Services. Either of these automatically removes the icon for the application from the user’s desktop the next time the App-V desktop configuration is refreshed.

Application virtualization is enabled by the following technology components:

* **Microsoft Application Virtualization 4.5 (App-V)**. App-V supports application virtualization by hosting client applications in a small virtual environment that contains the registry entries, files, COM objects, and other components needed to run the application. This virtual environment provides a layer between the application and operating system.

App-V is a client/server product that is part of the Microsoft Desktop Optimization Pack for Software Assurance. App-V includes:

* Management Server for centralized control and configuration.
* Streaming Server for lightweight deployment using Real Time Streaming Protocol (RRDSP) or Transport Layer Security (TLS) + RRDSP (RRDSPS).
* App-V Sequencer for creating the virtual application package.
* App-V Desktop Client, which enables the virtualization on a local desktop or mobile computer.

The App-V Remote Desktop Services client, which enables the virtualization on a Terminal Server, is sold separately outside of Microsoft Desktop Optimization Pack for Software Assurance.

* **System Center Configuration Manager 2007 R2**.System CenterConfiguration Manager provides a platform from which IT can deploy and provision operating systems and settings, deploy software and application updates, and perform asset inventory and evaluations. The platform uses multiple Microsoft technologies, including Active Directory Domain Services (AD DS), Windows Management Instrumentation (WMI), and Windows Server Update Services (WSUS); and runs on a central Windows Server‑based computer. Configuration Manager supports application virtualization by providing deployment capability for applications created using App-V. Virtual application packages run on client computers that are managed by Configuration Manager 2007 R2 that have the App-V client installed. These virtual applications are delivered in the traditional software distribution method through advertisements to collections of users or computers, but for virtual applications, streaming from a distribution point is also possible.
* Together, Microsoft Application Virtualization 4.5 and System Center Configuration Manager 2007 R2 provide a full PC life cycle management solution for deploying and managing both physical and virtual applications for enterprise customers. The combination of these two products enables customers to leverage their existing infrastructure investment and seamlessly integrate into existing workflows to package, test, deliver, and manage virtual applications for their end-users alongside physical software packages using one tool. When combined with other capabilities such as operating system deployment, software update management, inventory and license management, as well as model-based configuration management, this combination provides a strong foundation of client-focused services. Building on a platform of Microsoft SQL Server®, SQL Reporting Services, hierarchal site management distribution and scale support for large enterprise workloads, App-V 4.5 and System Center Configuration Manager R2 can handle the distributed, mobile network landscape of today's modern organizations.

## Client-Hosted Desktop Virtualization

Client-hosted desktop virtualization is a solution that enables multiple desktop operating system instances on a single computer. Those instances run in virtual machines that can be customized by the end user for personal use, development or testing, or be delivered and centrally managed by IT.

Desktop virtualization enables the following key benefits within the Windows Optimized Desktop scenarios:

* **Support for legacy applications when upgrading to the latest operating system**. Desktop virtualization lets the user run incompatible applications in a virtual instance of a previous operating system, instead of having to delay the deployment of a new operating system because of issues with incompatibility. Line-of-business applications that cannot be installed or have not been fully tested on the new version of the operating system can operate within their native, supported environment.
* **A secondary desktop environment**. Desktop virtualization lets you deliver IT-configured virtual desktops to end users. The virtual desktop can be managed separately from the physical desktop, which means it can be connected to a different domain, and managed by a different IT group (for example, in the case of subsidiaries or branch offices).
* **Offline work with virtual desktops.** Client-based virtual desktops reside locally on the user’s computer and can operate even when the user is offline, leveraging local hardware and with no dependency on servers.

Desktop virtualization is enabled by the following technology components:

* **Microsoft Virtual PC 2007**.Virtual PC 2007 creates multiple operating systems ("guests") on a single computer ("host"). Each virtual instance of an operating system can be configured separately from the host operating system and applications and all operating system functions such as storage, networking, display, and so on are independent of the host hardware.
* **Microsoft Enterprise Desktop Virtualization**. Part of the Microsoft Desktop Optimization Pack for Software Assurance customers, Microsoft Enterprise Desktop Virtualization enhances deployment, centralized management, and user experience for Virtual PC images. It includes a management server, an images distribution server (based on IIS), and a client component to facilitate the local virtual machine operation and the user experience. Microsoft Enterprise Desktop Virtualization enables the delivery of a Windows XP virtual machine to the user's computer that is running Windows 7 and Microsoft Virtual PC 2007. With Microsoft Enterprise Desktop Virtualization, applications can be launched within the Virtual PC environment seamlessly from the host computer’s Start menu. These applications appear within their own window as if running natively on the host Windows 7 operating system.

## Server-Based Desktop Virtualization (VDI)

Virtual Desktop Infrastructure (VDI) consolidates the desktop environment (data, applications, and settings) on a central server within the data center. Users can access this desktop environment remotely using the Remote Desktop Protocol. In this manner, VDI enables a centrally managed desktop experience. It supports local administration, increases data security, promotes compliance, and simplifies management of the corporate desktop. The VDI solution supports flexible user scenarios that require a more powerful desktop environment with the management and security benefits of a centrally managed desktop environment solution.

Virtual Desktop Infrastructure enables the following key benefits within the Windows Optimized Desktop scenarios:

* **Security**. Virtual Desktop Infrastructure helps organizations keep critical intellectual property secure and supports regulatory compliance efforts by providing a solution to remove specific applications and data from the desktop computer and store and present them from a centrally located and managed server.
* **Full desktop environment**. Supports local administration, client application compatibility, and rich interactive interface.
* **Centrally managed**.Guest images reside on a central server managed in the data center, which provides the ability for IT to maintain desktop environments with minimal overhead.
* **Provisioning**. Server hosted desktop environments that can be quickly provisioned and accessed by users with minimal deployment overhead.
* **Roaming user profiles**. Users access their desktop environment from a centralized server that can be accessed from any network-connected client.

Virtual Desktop Infrastructure is enabled by the following technology components:

* **Windows Server 2008 with Hyper-V™**.Extension to Windows Server 2008 to support microkernel hypervisor to host multiple guest environments running Windows 7 Enterprise.
* **System Center Virtual Machine Manager 2008 (VMM). VMM enables rapid deployment of virtual machines, centralized control of the “building blocks” of the virtual data center, and delegated self-provisioning by authorized end users.**
* **Windows Server 2008 Remote Desktop Services. The Remote Desktop Services component of the Windows Server 2008 operating system provides technologies that enable users to access a virtualized desktop environment from almost any computing device. Users can connect to a terminal server to run programs and to use network resources on that server.**
* **Connection Broker. A third-party server application serves as a Remote Desktop Services connection broker by controlling which Hyper-V guest the client can connect to and by defining the security access and roles.**

# Acknowledgments

The Microsoft Solution Accelerator Team (SAT) would like to acknowledge the team that produced the *Windows Optimized Desktop Scenarios Assessment* guide. The following people were either directly responsible for, or made a substantial contribution to, the writing, development, and testing of this guide.

**Program Managers**

Tejinder Singh

Venkat Panchapagesan

Anupama Vedapuri

**Content Developers**

Chanel Chambers

Michael Sarabosing, *Covestic Inc*

Sean Bethune, *Covestic Inc*

**Product Manager**

Baldwin Ng

**Release Manager**

Gaile Simmons

**Editors**

Hannah Rames, *BuzzBee*

Jennifer Kerns, *Wadeware*

**Subject Matter Experts**

Chanel Chambers

Fei Lu

Jason Leznek

**Testers**

Gargee Sharma (Test lead)

Prakash Thangella, *Longtop*

**Contributors and Reviewers**

Karri Alexion-Tiernan, Greg Amrofell, Alex Balcanquall, Kyle Beck, Tomer Brand, Paul Cooke, Doug Davis, Jeff Johnson, Luis Camara Manoel, Michael Gallegos, Max Herrman, Michael Kaczmarek, Eduardo Kassner Shvadsky, Brian Kelly, Ran Kovahi, Jason Leznek, Fei Lu, Robin Maher, Ran Oelgiesser, Eric Orman, Dan Reger, Ken Revels, Edhi Sarwono, Richard Trusson, Bill Weis, Kelly Wagman, Jeff Wettlaufer, Frank Zakrajsek