ManageEngine®

Desktop Central

User Guide

Table of Contents

Introduction

ManageEngine® Desktop Central

Desktop administration is a never-ending job. Configuration requests ranging from simple Drive Mapping configuration to software installation keep the administrators on their toes. With increasing requests and a growth in the number of desktop, it becomes more difficult to keep up with escalating demand on limited manpower.

Desktop Central enables configuring and managing desktop from a single point. With the pre-defined configuration options, administrators can perform almost all the regular desktop administration / management activities with ease. The ability to execute custom script gives complete administration control over the desktop. The Web-based user interface allows for applying the configuration to a single or group of desktop using a powerful filtering capability.

Desktop Central ensures that the configurations are applied to the desktop and the status is made available to the administrator to provide an end-to-end configuration experience.

In addition to the remote configuration options, it also provides you with an automated patch management system that helps you to manage and apply Windows patches and hot fixes.

The Inventory Management module provides the hardware and software details of the devices in the network. In enables you to manage the software licenses and detect any unauthorized software that are being used.

Remote Desktop Sharing enables you to gain access to a desktop in the network to be controlled remotely.

Desktop Central provides the complete history of the configurations applied to the users, computers, and by configuration types in the form of reports that can be used for auditing the deployed configurations.

In addition to the configurations reports, it also provides Active Directory reports for Sites, Domains, Organization Units, Groups, Computers, etc., which gives you a complete visibility into the Active Directory.

The User Logon Reports provides an up-to-date user logon details like the logon time, logoff time, logon computer, reported logon server, etc. It maintains the history of the logon details that can be used for auditing purposes.

The following sections will help you to get familiar with the product:

- Getting Started: Provides you the details of system requirements, product installation and startup.
- Configuring Desktop Central: Helps you to customize our product to suit your working environment.
- Windows Configurations: A step-by-step guide to define and deploy configurations to remote Windows users and computers.
- Configuration Templates: Provides the details of configuration templates and helps you to define configurations from Templates
- Software Installation: Helps you to install Windows software to the users and computers of the domain from remote.
- Patch Management: Details the steps involved in managing the Windows Patches and hot fixes. It helps you to automate the patch management process.
- Hardware and Software Inventory: Guides you to collect the hardware and software inventory details of your network and view the reports.
- Active Directory Reports: Helps you to view the reports of the Active Directory components.
- Windows Tools: Provides the list of Windows tools like Preventive Maintenance Tools, Remote Tools, etc., and the steps in using them.
- User Logon Reports: Helps you get an up-to-date- details of the user logon and history.
- Appendix: This section includes, Interpreting Error Messages, Knowledge Base, FAQs, Known Issues and Limitations of Desktop Central, and Glossary.

Release Notes

Release Notes for 8.0.0

Enhancements

1. Support for MS SQL Database has been included
2. The image format of the screenshot attachments sent using the Help Desk Requests from Desktop Central icon in system tray is made configurable.
3. Support for user environment variables in Custom Script has been introduced.
4. 'Show deployment progress' and 'Skip deployment' options introduced in Install/Uninstall software configuration.
5. Configurations deployed to an OU or Active Directory Group will automatically be applied to any new computers/users that gets added to that OU or group
6. Option to deploy configurations immediately has been included for computer configurations.
7. Option to exclude specific USB device instance from being blocked has been included.
8. Option to exclude computers based on the processor type has been included.
9. Option to save an existing configuration as a new configuration has been included.
10. Apply Always Option is enabled for Power Management,Shared Network Printers,File Folder Operations,Services,Firewall and Permission Management Configurations.
11. File Folder Configuration has been enhanced to support copying files via HTTP to make them work across WAN.
12. Templates for disabling automatic updates for Adobe Reader,Adobe Shockwave,Java and Microsoft Reboot Notification on specific computers have been added.
13. Deployment Options like deployment time, reboot policies, etc., can now be saved and loaded from templates for software, patch and servicepack deployments.
14. Remote Control initiated computer's IP audit is introduced in Action Log Viewer.

15. Remote Control now has the functionality of prompting even the user is not logged in or the computer is locked.
16. Administrators can also configure the color quality for the remote connections to optimize the bandwidth. The color quality and compression level can be set at the remote office level, which will be common for all the computers in that remote office.
17. Support for viewing User Access Control (UAC) dialogs of the remote computers has been included in Remote Control. This is applicable only for client computers running Windows Vista or Windows 7 OS.
18. Remote Control will now provide the history of remote connections established using Desktop Central with the duration of each sessions.
19. Remote Control has been enhanced with an option to connect with "View Only" mode.
20. Option to make User Confirmation permanent has been included in Remote Control.
21. Software Metering is a new functionality introduced. This can be used to get the software usage for the selected applications.
22. Inventory Alert notifications has been enhanced to include the ability to customize the alert messages.
23. Software License Management has been enhanced to include the ability to add multiple license purchases and to associate a license to a resource.
24. Disk Usage report now includes a detailed view to get the drive specific usage statistics.
25. Software Metering engine has been optimized to address the performance issues.
26. Option to disable Software Metering feature has been included.
27. A new report to view the computers running specific services has been included.
28. SM Bios reported version details are included in the Inventory, Computer Hardware Details.
29. Automatic retrieval of warranty information for Lenovo computers has been included.
30. Option to specify the DNS name of the Distribution Server along with its IP Address while creating a remote office has been included.
31. SoM page has been enhanced to include Agent Installation, Uninstallation and Last Upgraded time.
32. Moving Desktop Central installation from one computer to the other is made easy with the option to provide the details of the new computer in the user interface.
33. Automatic synchronization of computers between Active Directory and SoM has been included to detect the deleted and newly added computers.
34. Introduced a new feature called Scheduled Reports which enables you to receive query reports, custom reports and predefined reports in specific formats and a at a specific time.
35. Ability to automatically scan to fetch the systems' warranty has been included for Dell, HP and Toshiba computers.
36. Reports based on system warranty has been included under Inventory Reports.
37. HTTP Software Repository location for packages in software deployment can be changed.
38. Automated Patch Deployment has been enhanced to improve performance.
39. Patch Management has been enhanced to include an option to mark a patch as "Approved", "Decline", etc., in Download Patches, All Supported Patches and Latest Patches Views.
40. Memory usage during Patch Deployment has been optimized.
41. Option to download a patch again in the Download Patches View has been added.

42. Option to schedule an Automated Patch Deployment task on a specific day of the week in a month has been included.
43. Long lived TCP connections are used to enhance on-demand actions.
44. Windows 7 (x86 and x64) Service Pack 1 and Windows 2008 R2 (x64) Service Pack 1 is Supported.
45. IP scope feature is introduced ,which can auto change Agents Remote Office setting on the client computer according to the Scope defined in Desktop Central.

Bug Fixes

1. Issue in recreating the agents even when there is no change in agent properties has been fixed.
2. Application error in dcconfig.exe during user logoff has been fixed.
3. Black screen when sending screenshot attachment from agent tray icon helpdesk issue is fixed.
4. Issue in remote control service getting crashed while closing a remote session has been fixed
5. Issue in registering the Desktop Central Agent as a windows service after agent up-gradation has been fixed.
6. Issue in displaying the wrong execution status when the patch or the configuration is not applicable in one or more computers has been fixed.
7. Issue in order of deploying configuration as Collection is fixed.
8. Issue in repeatedly processing the user configuration when multiple users login to a computer has been fixed.
9. Issue in showing the correct update time in the execution status view of the configurations has been fixed.
10. Issue in applying configuration has been fixed.
11. Issue in adding target computers/users from a remote office where the length of remote office name exceeds 50 characters has been fixed.
12. Issue in deploying Software and Patches when the installation option is selected as "Install during Startup" has been fixed.
13. Issue in connecting to a remote computer having multiple IP Addresses has been fixed.
14. Support for capturing/rendering the transparent windows in Remote Control has been included.
15. Issue in establishing remote connections from Inventory and Patch views has been fixed.
16. The issue related to upgrading agents in remote office names that contain Latin alphabets has been fixed.
17. Issue in taking Remote Control of Windows 2003 Server that has an active Remote Desktop Connection has been fixed.
18. Issue in high memory usage in software metering has been fixed.
19. Issue with Microsoft Office 2010 product key fetch is fixed.
20. Issue in modifying the license details of the software when the software name contains an '&' character has been fixed.
21. Issue in displaying the hard disk details of computers running non-English versions of Windows OS has been fixed
22. Issue in showing negative values in Physical Memory for a computer when flash memory is detected has been fixed.

23. When a prohibited software that is awaiting administrators approval is disabled (not prohibited), the users where it was detected earlier will continue to see the warning on every logon. This has been fixed.
24. Issue in sending test email while creating a scheduled report has been fixed.
25. Issue in scheduled prohibited software report has been fixed.
26. Issue in showing a wrong login time in User Logon History reports has been fixed.
27. Issue in deleting the software install-able from the client computers after successful installation of the software has been fixed.
28. Issue in listing folders with special characters (apostrophe and comma) in network browser has been fixed.
29. Issue in showing the Managed Computers in the Scan Systems and All Managed Systems view under the Patch Management has been fixed.
30. Issue in Automate Patch Deployment has been fixed.
31. Issue in showing a wrong start time of the "Automated Patch Deployment" task in the email notification has been fixed.
32. Issue in showing Patch Deployment status as "Reboot Pending" even if the system has been restarted has been fixed.
33. Issue in patch download due to transaction timeout has been fixed.
34. Issue in retrying Automated Patch Deployment tasks has been fixed.
35. Distribution Server service startup issue has been fixed.

Release Notes for 7.0.1

Enhancements

1. Desktop Central Server performance has been optimized.
2. Free Edition limit extended to manage up to 25 computers.
3. Support for scheduled backup of the database used by Desktop Central has been added.
4. Role based administration has been introduced. You can define roles specifying the modules and access levels, which can be delegated to users.
5. In Define Target Microsoft Windows 7 and Microsoft Windows Server 2008 R2 have been added in the exclude OS list.
6. Custom group filter has been added for 'Software Usage by Computer' report.
7. Computer Name column added in e-mail alerts of Prohibited Software/New Hardware Detected/New Software Detected.
8. Computer Details view enhanced to include the system details like installed Windows Services, local users and groups in that computer.
9. Exclude Custom Groups option has been added for Auto-Uninstallation of Prohibited Software.
10. User Notification before Auto-Uninstallation of Software has been added.
11. "Logged On Users" column included in Inventory Reports.
12. Asset Data from Desktop Central can now be integrated with ManageEngine ServiceDesk Plus.
13. The Computer Details view of the Inventory Reports will now include the Serial Numbers of Monitor and Hard Disk.
14. License Management enhanced with the ability to attach license files and invoices to the software. You will also be able to add license details of software that are not detected in your network.

15. System Vulnerability Summary will now include additional system details like the operating system, service pack version, etc.
16. Support for deploying patches for Non-Microsoft applications has been included.
17. You will now be able to specify the type of updates with the severity levels while adding the Automated Patch Deployment task.
18. Vulnerability Summary, which includes the application and missing patch information, of the computer can now be exported to PDF/CSV/XLS formats.
19. 'Manager' column has been added in 'All User Accounts' Report under AD Reports category.
20. Option to create and save Custom Query Reports has been included.
21. Remote Office agent communication (Distribution Server / Direct Communication) can now be modified from the SoM page.
22. Remote Office details can now be imported using a CSV file.
23. Inclusion of Alerts for Distribution Server.
24. Apache web server has been integrated to improve the performance for large network of computers.
25. Support for deploying File and Shared Printer Configurations to Windows Vista, Windows 2008 and Windows 7 computers have been added.

Bug Fixes

1. Issue with Non-English Computer names displayed in Network Browser is fixed.
2. Issues related to Active Directory computers with names exceeding 15 characters have been fixed.
3. 'java.lang.Exception: NetBIOS and DC name cannot be null' issue while clicking on the workgroup name in SoM page has been fixed.
4. Issue with selecting all computers while adding computers in SoM has been fixed.
5. Issue in displaying computer message box on Vista and above has been fixed.
6. Issue in showing a pop up in Windows 2000 computers stating non-availability of a DLL file has been fixed.
7. Remote Office names sorted in filters.
8. Issue in installing agents on Vista and above when UAC is enabled has been fixed.
9. Agent side fix for inventory scanning.
10. Issue with Microsoft Office 2007 Productkey fetch is fixed.
11. Prompt User issue in Remote Control has been fixed for Multiple User Login of Vista/2008 Server/Windows 7.
12. Issue in Schedule Vulnerability Update is fixed.
13. Issue in Reboot Policy during Patch installation is fixed.
14. Issue in deploying the patches that have dependent patches has been fixed in the Automated Patch Deployment process.
15. Time interval issue in Filter has been fixed for all reports.
16. Number of characters allowed in the NOTES field of AD Reports has been increased.

Release Notes for 7.0.0

Enhancements

1. Distribution Server introduced to reduce the bandwidth consumption in managing computers across WAN

2. Support to block/unblock specific USB Devices included
3. Desktop Central internationalized to manage computers running non-English version of operating systems
4. Support for Windows 2008, Windows Vista, and 64-bit included
5. Power Management Reports has been introduced.
6. Ability to create Custom Reports has been included
7. Automatic Patch Deployment enhanced with the ability to define multiple tasks.
8. Install / uninstall silent switches of popular software now comes pre-filled
9. Option to automatically uninstall the prohibited software from the managed computers has been included.
10. Support for applying user configurations when you switch from one user to another has been included for Windows Vista and Windows 2008.
11. Custom group creation has been enhanced by listing the computers/users in a tree view with search and filter options.
12. Option to enable/disable trimming of column values in reports has been included
13. IP Printer and Shortcut configurations can now be deployed to computers.
14. A new report "Software Product Key" has been added under Inventory module.
15. Support for viewing Remote Desktops from Firefox 3.0 and above has been included.

Bug Fixes

1. Desktop Central Server performance has been optimized.
2. Desktop Central agent binaries have been digitally signed.
3. Issue in deploying patches in bulk has been fixed.
4. Issues in Drive Mapping and Folder Redirection Configurations have been fixed.
5. Issue in updating the patch database manually has been fixed.
6. Issue in downloading patches and service packs has been fixed.
7. Issues with dynamic variables has been fixed.
8. Issue while deploying configurations with multiple targets has been fixed.
9. Issues related to child domain networks has been fixed
10. Issue in showing duplicate listing of computers in the SoM page has been fixed.

Release Notes for 6.0.3

1. Adding multiple packages while defining an install software configuration is introduced.
2. Introduced MS-Office Patching Support and service pack installation.
3. Commercial Software Grouping is introduced in Inventory module.
4. Provision added to terminate Windows Remote Desktop connection and establish connection with Remote Control of Desktop Central.
5. Introduced Connect with IP option in Remote Control.
6. Ctrl+Alt+Del for Vista OS is handled in Remote Control.
7. Introduced IP range in the Define target Section of Configurations.
8. Sending AD Reports by E-Mail is introduced.
9. Introduced Rebranding Option to change Desktop Central logo.
10. Added 64-Bit OS Support for Inventory, Patch Management, Software Deployment and Remote control.
11. Added Windows 2008 OS support for Desktop Central Agents.
12. Provision to change E-Mail domain for Help Desk emails is added.

Release Notes for 6.0.2

1. Support for managing computers across WAN included.
2. In software deployment, environment variable support is added for the network paths, pre, post installation scripts. Eg: %ProgramFiles% --> C:\Program Files
3. Support for establishing remote connection from Mozilla has been added.
4. Options to lock/unlock remote computers and to black-out remote monitors have been added in Remote Desktop Sharing.
5. Scheduled installation is added in Patch deployment configuration.
6. Prohibited Software Report is added in Inventory.
7. Export PDF option is included In Computer Details of Inventory Management.
8. Provision added to delete an already defined message box through message box configuration.
9. Option added to apply configurations on every logon/bootup.
10. Automatic detection of Windows Firewall and adding necessary exceptions (required for Desktop Central server) is handled.

Release Notes for 6.0.0

1. Support for Windows Workgroup added
2. Support for configuring desktop in multiple domains has been added.
3. Support for creating custom groups of users and computers has been added. The groups can then be chosen as target for deploying configurations/patches/software.
4. Wake on LAN tool included.

Release Notes for 5.0.0

1. Hardware and Software Inventory module included.
2. Support for installing EXE packages in addition to MSI
3. Support for Configuration Templates Added.

Release Notes for 4.0.5

1. Microsoft Non Security Patches are supported for deployment.
2. Provided an option to delete the failed download patches from patch configuration download status page. Also, provided an option to deploy from download status page.
3. "Fix on Errors" option for Check Disk system tool is added.
4. Provision to define SoM with individual computers.
5. Added multiple OUs support in SoM definition.

Release Notes for 4.0.4

1. Provision added for multiple user login in Desktop Central with different access roles.
2. Folder Redirection configuration has been enhanced to copy the local folder contents to the redirected folder.
3. ActiveX Component used for Desktop Sharing is signed for security reasons.
4. Active Directory Reports loading performance has been improved.

5. Status update and additional filtering options have been added for "Install Software" configuration.

Release Notes for 4.0.3

1. System Tools that can be scheduled on multiple client machines have been added.
2. New configurations, File and Folder Operations and Permission Management, have been added
3. Patch Management enhanced to include support for installing service packs of Microsoft products.

Release Notes for 4.0.2

1. Active Directory Reports enhanced to include over 90+ granular reports of the individual components.
2. Included User Logon Tracking Reports for an up-to-date user logon details with history.
3. Ability to schedule report update interval has been included.
4. Enhanced Remote Desktop Sharing with the ability to change the screen resolution.
5. New look and feel for better usability.

Release Notes for 4.0.1

1. Ability to connect to remote desktops through web browser using Remote Desktop Sharing.
2. Added Power Management configuration to define and apply power schemes to the client computers.
3. Option for instant and manual installation of agent software on the client computers.
4. Option to uninstall agent software from client computers.
5. Number of users, computers, and container details are added in Resource Browser.
6. Improved usability of Add configuration and SoM page screens.
7. Issues related to persisting Active Directory computer details in database is fixed.

Release Notes for 4.0.0

1. Patch Management module included - enables automatic detection of the required patches, download and install in the affected systems.
2. Computer configurations to manage windows local groups, users, and to install patches have been included.
3. Scheduler configuration has been added to schedule tasks for users.
4. Reports relating to Patch Management have been included.
5. Ability to view and audit the tasks executed using Desktop Central has been added.

Release Notes for 3.0.1

1. Configuration based reports have been enhanced with more details.
2. Provision to remember view settings like the page size, sort order etc. across logins.
3. Overall usability is enhanced for the product.

4. Provision to change the admin credential alone in Scope Of Management (SOM) settings page.
5. Issues in Active Directory reports with large number of users is fixed.
6. Issues with multiple ip addresses given in target exclude is fixed.
7. Issue with creating shortcut in User Quick Launch Bar is fixed.

Release Notes for 3.0.0

The key features of this release are:

1. Ability to define configurations for users and computers in the Windows 2000/2003 domain from a central point.
2. Out-of-the-box configurations include Alerts, Message Boxes, MS Office, Display, Outlook, Drive Mapping, Path, Environment Variable, Registry Settings, Folder Redirection, Security Policies, Internet Explorer, Shared Printer, IP Printer, Shortcut, Launch Application, Windows Installer, Firewall, Services, Legal Notice, Custom Scripts, and Common Folder Redirection.
3. Ability to run custom scripts to get complete administration control over the domain.
4. Multiple configurations can be defined and deployed to users or computers simultaneously using Collections.
5. Ability to define selective targets for applying the configurations. Targets can be either single user/computer or all users/computers belonging to a Site, Domain, OU, or Groups.
6. Ability to view the status of the deployed configurations from the Desktop Central client.
7. Ability to suspend, modify, and redeploy defined configurations.
8. Comprehensive reports for the defined configurations and other Active Directory components.

Contacting ZOHO Corporation

ZOHO Corp. Headquarters

Web site	www.zohocorp.com
Corporate Office	**Zoho Corporation** 4900 Hopyard Rd, Suite 310 Pleasanton, CA 94588 USA Phone: +1-925-924-9500 Fax : +1-925-924-9600 E-mail: info@manageengine.com
	Zoho Corporation Private Limited DLF IT Park, Block 7, Ground floor, No. 1/124, Shivaji Garden, Nandambakkam Post, Mount PH Road, Ramapuram Chennai 600 089 Phone: +91-44-22707070 Fax: +91-44-22707172 E-mail: info@manageengine.com
	Zoho Corporation Pte Ltd C/o Cananex Singapore Pte Ltd Block 1003 Bukit Merah Central #05-23 Inno-Center, Singapore 159836 Main Line : 63344486 Fax: 62819188 Mobile: 97552882 Contact Person: Ong Yang Peng Email: yangpeng.ong@cananex.com.sg

Sales

You can buy ManageEngine Desktop Central from anywhere in the world. To buy our product contact us in the following ways:

- Fill out our sales request form to receive a call from our sales personnel
- Send us an e-mail at sales@manageengine.com

- Call the ZOHO Corp. headquarters or send us a fax. The numbers are as follows:

- Phone: +1-925-924-9500
- Fax: +1-925-924-9600

Technical Support

One of the value propositions of ZOHO Corp. is excellent support to its customers. During the evaluation phase the support program is extended to you free of charge. Please send your technical queries to desktopcentral-support@manageengine.com.

Use the following support format while sending e-mails to the support team:

- Edition of the product (Free, Standard, Professional, or Enterprise Edition)
- Version of the operating system you are using. For example, Windows 2003.
- Version of the browser you are using. For example, Firefox 1.5 or Internet Explorer 5.5.
- Details of the problem
- Steps to reproduce the problem

Alternatively, you can select the **Support** tab from the client window. It has the following options that will allow you to contact us:

- Request Support: Submit your technical queries online
- Need Features: Request for new features in Desktop Central
- User Forums: Participate in a discussion with other Desktop Central users
- Contact Us: Speak to our technical team using the toll free number 1-888-720-9500

How Desktop Central Works?

ManageEngine Desktop Central is a Web-Based windows desktop administration software that helps administrators to effectively manage the desktops from a central point. It provides Configurations, Inventory Management, Patch Management, Service Pack Installation, Software Installation, Desktop Sharing, System Tools, Active Directory Reports and User Logon Report.

- Desktop Central LAN Architecture
- Desktop Central WAN Architecture

Desktop Central LAN Architecture

The figure below depicts the Desktop Central Architecture. The details of the individual components are given below:

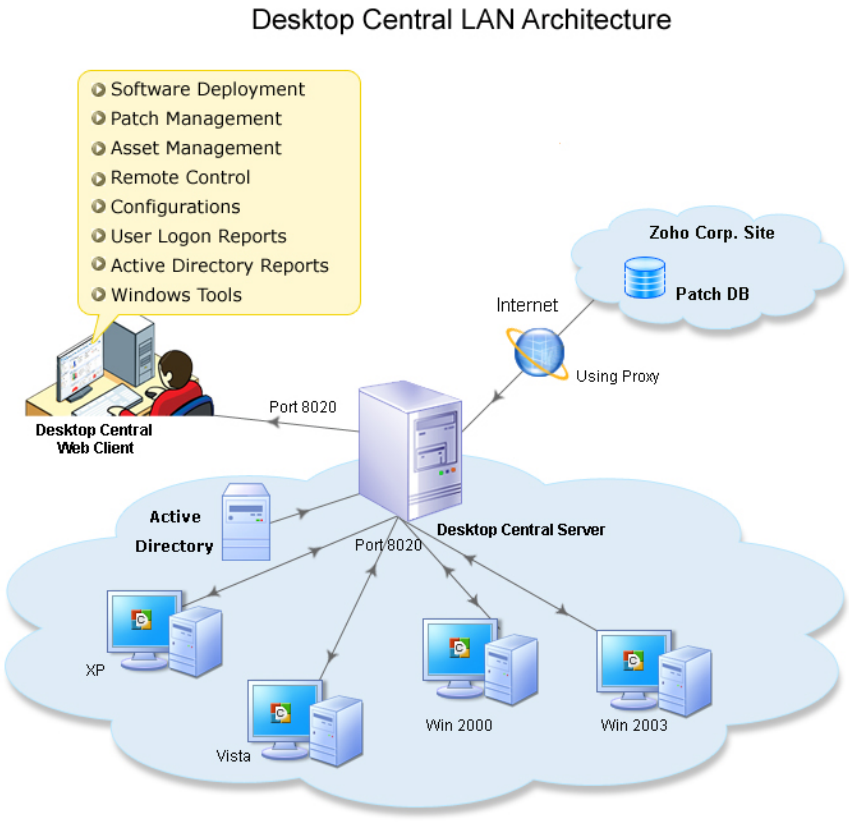


Fig: Desktop Central Architecture for LAN

Server Component

Desktop Central Server is located at the enterprise (customer site) is responsible for performing various Desktop Management activities. It pushes the Desktop Central agent to the client machines, deploys configurations, initiates scanning for Inventory and Patch Management, and generates reports of the Active Directory Infrastructure Components to effectively manage the desktops in the enterprise network. It is advised to keep the Desktop Central server always running to carry out the day-to-day Desktop Management activities. All these actions can be initiated from a web-based administration console in a few simple clicks.

Agent Component

Desktop Central Agent is light-weight software that gets installed in the client systems that are being managed using Desktop Central. It acts as a worker to carry out the operations as instructed by the Desktop Central Server. It is also responsible for updating the Desktop Central Server with the status of the deployed configurations. The
agent periodically pulls the instructions from the Desktop Central Server and executes the tasks. The agent contacts the server at the following intervals:

1. For user-specific configurations - during user logon and every 90 minutes thereafter till the user logs out of the computer.
2. For computer-specific configurations - during system startup and every 90 minutes thereafter till the system is shutdown.

Patch Database

The Patch Database is a portal in the ManageEngine site, which hosts the latest vulnerability database that has been published after a thorough testing. The Desktop Central Server periodically synchronizes this information and scans the systems in the enterprise site to determine the missing patches. Subsequently, the patches are installed to fix the vulnerabilities.

The communication between the Desktop Central Server and the Patch Database is through the Proxy Server or a direct connection to internet. The required patches will be downloaded from Microsoft website and stored locally in the Desktop Central Server before deploying the patches to the client computers. Hence, each client computer (agent) will take the patch binaries from the Desktop Central Server.

Web Console

- Provides a central control point for all the desktop management functions.
- Can be accessed from anywhere: LAN, Remote Offices, and Home through Internet/VPN.
- No separate client installations are required.

Active Directory

For Active Directory based Domain setup, the Desktop Central Server queries the Active Directory to generate out-of-the-box reports for Sites, Domains, Organization Units, Groups, Computers, etc., which gives you a complete visibility into the Active Directory.

Ports Used by Desktop Central

Ports to be opened on the Agent

To enable remote installation of the Agent, you should open these ports.

- 135 : Used to enable remote administration.
- 139 & 445 : Used to enable sharing of files and printers.

Ports to be opened on the Server

- 8020: Used for agent-server communication and to access the Web console
- 8383: Used for secured communication between the agent and the Desktop Central server
- 8443: Used for the Remote Control feature with secured communication
- 8444: Used for the Remote Control feature
- 8031: Used to transfer files in a secure mode while accessing a remote computer using Remote Control
- 8032: Used to transfer files while accessing a remote computer using Remote Control
- 8027: Used to complete on-demand tasks like inventory scanning, patch scanning, remote control, remote shutdown and moving agents from one remote office to another

Desktop Central WAN Architecture

Desktop Central supports managing Computers in a distributed setup like branch/remote offices and for mobile users (eg. Sales Persons). The figure below depicts the Desktop Central Architecture for managing computers in WAN. The details of the individual components are given below:

Desktop Central WAN Architecture

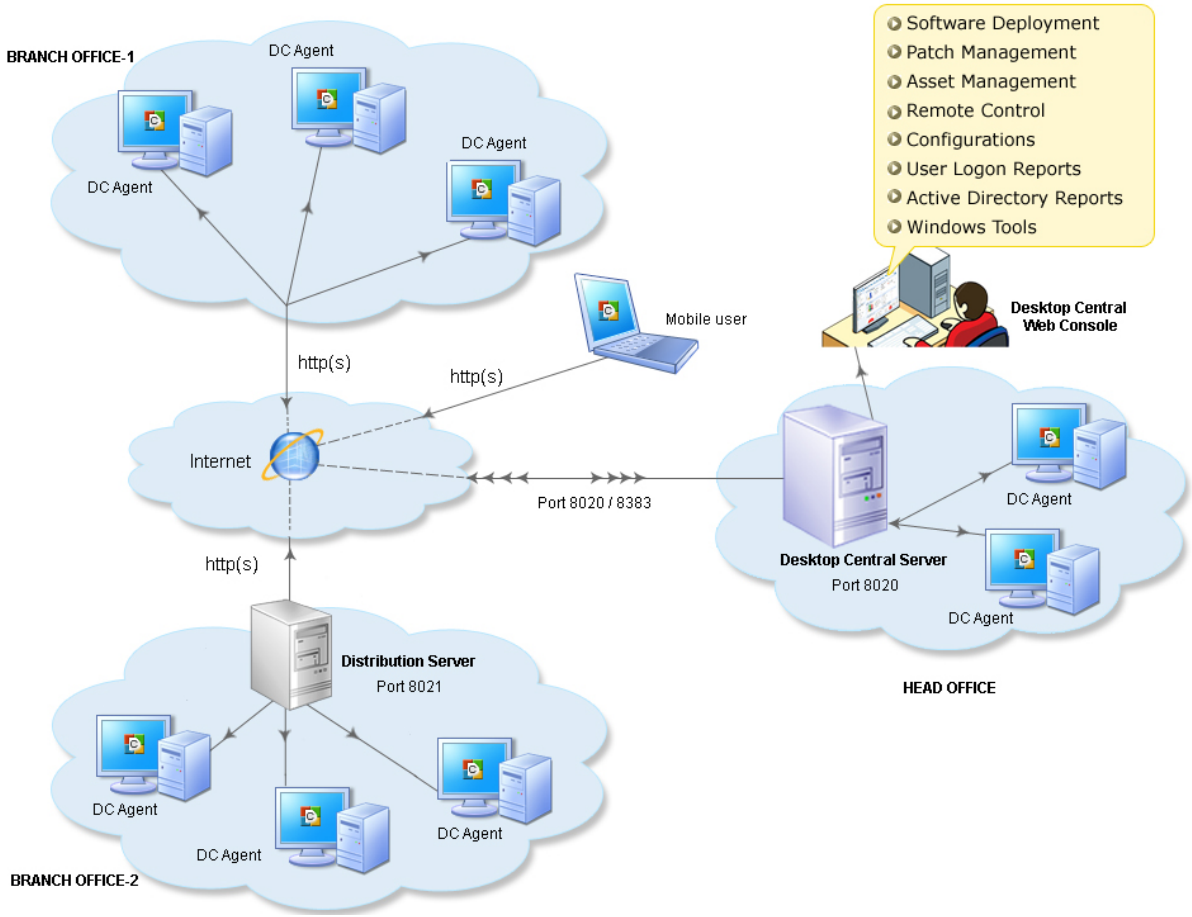


Fig: Desktop Central WAN Architecture

Advantages

- Simple, fast, and an affordable solution for your desktop management needs.
- Low bandwidth utilization
- Network-neutral desktop management.
- No separate VPN infrastructure is required.
- Secured communication between the Server and the Agent.
- Centralized management of computers from a single console.

Server Component

Desktop Central Server has to be installed in your LAN (say, the head office) and has to be configured as an EDGE device. This means that the designated port (default being 8020 and

is configurable) should be accessible through Internet. You need to adopt necessary security standards to harden the OS where the Desktop Central Server is installed. Agents from all the remote locations report to this Desktop Central Server.

The Server acts as a container to store the configuration details and, upon request, provide the instructions to the agents. It is advised to keep the Desktop Central server always running to carry out the day-to-day Desktop Management activities.

Distribution Server Component

Desktop Central Distribution Server is light-weight software that is installed in one of the computers in the Branch Offices. This agent will communicate with the Desktop Central Server to pull the information for all the computers in that branch. The agents that reside in the branch office computers will contact the Distribution Server to get the information available to them and process the requests.

- Low bandwidth utilization as only one agent will contact the Server periodically
- Pulls the configuration details, software packages, patches to be installed, etc., from the Desktop Central Server and makes it available for the rest of the computers in the branch.
- Supports secured mode of communication (SSL/HTTPS) with the Server.
- Distribution Server installation is one-time and subsequent upgrades will be automatically performed.

Agent Component

Desktop Central Agent is light-weight software that is installed in the client systems that are being managed using Desktop Central. It acts as a worker to carry out the operations as instructed by the Desktop Central Server.

- Unobtrusive light-weight component.
- Can either be installed manually or through the logon script in all the computers that are being managed using Desktop Central. However, for computers in the local LAN, the agents will be automatically installed.
- Agent installation is one-time and subsequent upgrades will be automatically performed.
- For computers in the same LAN as that of the Desktop Central Server, the agent will periodically connect to the Server to PULL the configurations available for them, deploys them and updates the status back to the Server.
- For computers in Branch Offices, the agent will contact the Master Agent to PULL the configurations available for them, deploys them and updates the status back to the Server.

Web Console

- Provides a central control point for all the desktop management functions.

- Can be accessed from anywhere: LAN, Remote Offices, and Home through Internet/VPN.
- No separate client installations are required.

Ports Used by Desktop Central

Ports to be Opened on the Agent

To enable remote installation of the Agent, you should open these ports.

- 135 : Used to enable remote administration.
- 139 & 445 : Used to enable sharing of files and printers.

Ports to be Opened on the Server

- 8020: Used for agent-server communication and to access the Web console
- 8383: Used for secured communication between the agent and the Desktop Central server
- 8443: Used for the Remote Control feature with secured communication
- 8444: Used for the Remote Control feature
- 8031: Used to transfer files in a secure mode while accessing a remote computer using Remote Control
- 8032: Used to transfer files while accessing a remote computer using Remote Control
- 8027: Used to complete on-demand tasks like inventory scanning, patch scanning, remote control, remote shutdown and moving agents from one remote office to another.

Ports to be Opened on the Distribution Server

- 8021: Used for communication between the agents in Remote Offices and the Distribution Server
- 8384: Used for secured communication between the agents in Remote Offices and the Distribution Server

Installation & Setup

This sections guides you in installing Desktop Central and performing the required configurations. Setting up Desktop Central can only be done by users with administrative privileges in Desktop Central.

The following sections describes how to get started with Desktop Central.

System Requirements

Hardware Requirements for Desktop Central Server

No. of Computers Managed	Processor	RAM	Hard Disk Space
Upto 250 Computers	Single processor Intel P4 ~1.5 GHz	1 GB	2 GB*
251 to 500 Computers	Single processor (Intel P4 or Xeon 2.0 Ghz (Dual Core), 800+ Mhz FSB, 4 MB cache)	2 GB	2 GB*
501 to 1000 Computers	Single processor (Intel Xeon ~2.4 Ghz Dual Core, 800+ Mhz FSB, 4MB cache)	4 GB	3 GB*
1001 to 3000 Computers	Dual processor (Intel Xeon ~2.0 Ghz Dual Core, 1000 Mhz FSB,4 MB cache)	4 GB	5 GB*
3001 to 5000 Computers	Dual Processor (Intel Xeon processors Quad-Core at 2 ~ 3 GHz, 1000+ MHz FSB, 4 MB Cache)	6+ GB @ 667 Mhz. ECC	20 GB (HDD speed @ 7200 ~ 10,000 rpm)
5001 to 10000 Computers	Quad Processor (Intel Xeon processors Quad-Core at 2 ~ 3 GHz, 1000+ MHz FSB, 4 MB Cache)	8+ GB @ 667 Mhz. ECC	50 GB (HDD speed @ 7200 ~ 10,000 rpm)

* May dynamically grow according to frequency of scanning

When managing computers above 1000, it is advisable to install Desktop Central on a Windows 2003 Server Enterprise Edition

Hardware Requirements for Distribution Server

No. of Computers Reporting to the Distribution Sever	Processor	RAM	Hard Disk Space
Upto 250 Computers	Single processor Intel P4 ~1.5 GHz	512 MB	1 GB*
251 to 500 Computers	Single processor Intel P4 ~1.5 GHz	1 GB	2 GB*
501 to 1000 Computers	Single processor (Intel P4 or Xeon 2.0 Ghz (Dual Core), 800+ Mhz FSB, 4 MB cache)	2 GB	2 GB*

* Hard disk space may grow depending on the number of software and patches that are deployed.

Hardware Requirements for Desktop Central Agent

Hardware	Recommended
Processor	Intel Pentium
Processor Speed	1.0 GHz
RAM	512 MB
Hard Disk Space	30 MB*

* May dyanamically grow depending on the operations performed on the client computer

Software Requirements

Supported Platforms

ManageEngine Desktop Central supports the following Microsoft Windows operating system versions:

Desktops

- Windows 2000 Professional
- Windows XP Professional
- Windows Vista
- Windows 7

Servers

- Windows Server 2000
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

and **Terminal Clients**

Supported Browsers

ManageEngine Desktop Central requires one of the following browsers to be installed in the system for working with the Desktop Central Client.

- Internet Explorer 5.5 and above
- Netscape 7.0 and above
- Mozilla Firefox 1.0 and above

Preferred screen resolution 1024 x 768 pixels or higher

Installing Desktop Central

Supported Operating Systems

Desktop Central can be installed on computers running the following operating systems (both 32-bit and 64-bit):

- Windows 2000 Professional
- Windows XP Professional
- Windows Vista
- Windows 7
- Windows 2000 Server
- Windows 2003 Server
- Windows 2008 Server
- Windows 2008 R2 Server
- Virtual Servers (VM Ware)

Pre-requisites for Installing Desktop Central Server

1. Desktop Central has to be installed in any of the operating systems mentioned above. It can either be installed on the Domain Controller or in any Workstation/Server in the network.
2. Ensure that the hardware requirements are met in accordance to the number of computers being managed using Desktop Central.
3. It is recommended to have a Static IP Address for the computer where Desktop Central Server is installed. This is because, the agents installed in the client computers communicates with the Desktop Central Server using this IP Address.
4. You should install the product as an administrator, since the product is installed and run as an Windows Service.

Ports Used by Desktop Central Server

Desktop Central Server uses the following ports:

1. TCP Port 8020 - Used for HTTP communication between the server and the agent
2. TCP Port 8383 - Used for HTTPS communication between the server and the agent (***Secure***)

3. TCP Port 8443 - Used for Remote Desktop Sharing (***Secure***)
4. TCP Port 8444 - Used for Remote Desktop Sharing
5. TCP Port 8031 - Used for File Transfer (***Secure***)
6. TCP Port 8032 - Used for File Transfer

If you are running any third party firewall in the computer where Desktop Central Server is being installed, open these ports by configuring the firewall. If you are running Windows Firewall, these ports can also be automatically be opened in the firewall from the SoM page (post installation) from the Desktop Central Console.

Installing Desktop Central Server

Desktop Central is distributed in the EXE Format. Run the **self-extracting EXE** with an Install Shield program for installation and follow the instructions provided. The installation wizard will guide you through a series of instructions like the installation directory, web server port, etc. You can either install the product with the default values or can change the values as required. If you are changing the web server port (default is 8020), ensure that you open the appropriate port in the firewall.

Upon successful installation of the product, all the required components like the web server, database server, etc., are automatically installed.

Uninstalling Desktop Central Server

It is recommended to uninstall the agent from the client computers prior to uninstalling the product. If the client computers are in the same LAN as that of the Desktop Central Server, the agents can be uninstalled from the SoM page of the Desktop Central Console. However, the agent in the remote office computers have to be removed manually. Refer to the online Knowledge base for the steps to remove the agent from remote office computers.

To uninstall Desktop Central, select **Start --> Programs --> ManageEngine Desktop Central --> Uninstall**.

If you have uninstalled the product before removing the agents and if you wish to remove later, refer to the online knowledge base for steps.

Working with Desktop Central

Starting Desktop Central

To start Desktop Central, select **Start** --> **Programs** --> **ManageEngine Desktop Central** --> **Start Desktop Central**

On starting the Desktop Central, the client is automatically launched in the default browser.

The following processes are started along with the Desktop Central:

- java.exe - Desktop Central Server
- mysqld-nt.exe - Database Server
- wrapper.exe - For system tray operations

When Desktop Central is started in Windows XP / Windows 2003 machines with firewall enabled, Windows will pop up security alerts asking whether to block or unblock the the following programs as shown in the images below:

1. mysqld-nt - Database server
2. Java(TM) 2 Platform Standard Edition binary - Java.

You should **Unblock** these programs to start Desktop Central.

Fig: MySQL Alert

Fig: Java Alert

Launching the Desktop Central Client

To launch the Desktop Central client,

1. open a Web browser and type http://hostname:8020 in the address bar. Here the hostname refers to the DNS name of the machine where Desktop Central is running.
2. Specify the user name and password as **admin** in the respective fields and click **Login**.

Steps to Perform after Initial Login

When you login to Desktop Central for the first time, perform the following steps:

1. Define the scope of management - Scope can be limited to a small set of computers or the whole domain.
2. Define and apply configurations to either users or computers. The applied configurations will take effect during user logon for user configurations and during reboot for computer configurations.
3. View the status if the configurations applied to the users/computers.
4. Setup Software Deployment Module
5. Setup Patch Management Module
6. Setup Inventory Management
7. Configure AD Reports Update Interval and Enable User Logon Reports

Stopping Desktop Central

To stop Desktop Central, select **Start --> Programs --> ManageEngine Desktop Central --> Stop Desktop Central**

Installing Service Pack

Desktop Central periodically provides Service Packs which provide new features (requested by the customers), fixes for certain bugs and document updates in the form of HTML files. Service Packs can be downloaded from the Web site, and updated into ManageEngine Desktop Central using the Update Manager tool.

Note: Ensure that no application is running when applying the Service Pack. This prevents any files used by the application from being over-written. For example if the Desktop Central is running, stop the server and then install the service pack.

Important: You should login to the computer with the Domain Administrator credential as specified in the Scope of Management to install a Service Pack.

The steps to apply a Service Pack are as follows:

1. Stop Desktop Central Server.
2. Start Update manager by executing the script **UpdateManager.bat** file located in *<Desktop Central Home>/bin* directory.
3. Click **Browse** and select the Service Pack file (.ppm) to be installed. Click **Install** to install the Service Pack.
4. You can go through the Readme file of the Service Pack by clicking the **Readme** button.

Note: On clicking **Install**, the tool checks whether there is enough space for the installation of the service pack. If there is no enough space, the tool informs you about the lack of space. You must clear the space and then proceed with the installation.

Licensing the Product

Desktop Central is available in four variants- **Free**, **Standard**, **Professional**, and **Enterprise** Editions

Download the product from the Website.

The **Free Edition**, **Standard Edition**, **Professional Edition** and **Enterprise Edition**, come packaged as a single download. During the evaluation phase, the **Enterprise Edition** is installed, and can be evaluated for 30 days. After 30 days, it is automatically gets converted to the **Free Edition**, unless the **Standard/Professional/Enterprise Edition** license is purchased. Given below is the comparison matrix of the features available in the various editions:

Feature	Standard	Professional	Enterprise	Free Edition**
Software Deployment	✗	✓	✓	✓
Patch Management	✗	✓	✓	✓
Asset Management	✗	✓	✓	✓
Remote Control	✓	✓	✓	✓
Service Pack Deployment	✗	✓	✓	✓
Windows Configurations	✓	✓	✓	✓
USB Device Management	✗	✓	✓	✓
Power Management	✓	✓	✓	✓
System Tools	✓	✓	✓	✓
User Logon Reports	✓	✓	✓	✓
Active Directory Reports	✓	✓	✓	✓***
Managing Desktops Across WAN	✓	✓	✓	✓
Manage Desktops of Roaming Users	✓	✓	✓	✓
Multi-Technician Support	✓	✓	✓	✗

Feature	Standard	Professional	Enterprise	Free Edition**
Distribution Server for Bandwidth Optimization	✗	✗	✓	✓

** **Free Edition** can be used to manage up to 25 desktops.

*** Granular reports on Active Directory are not available in the Free Edition.

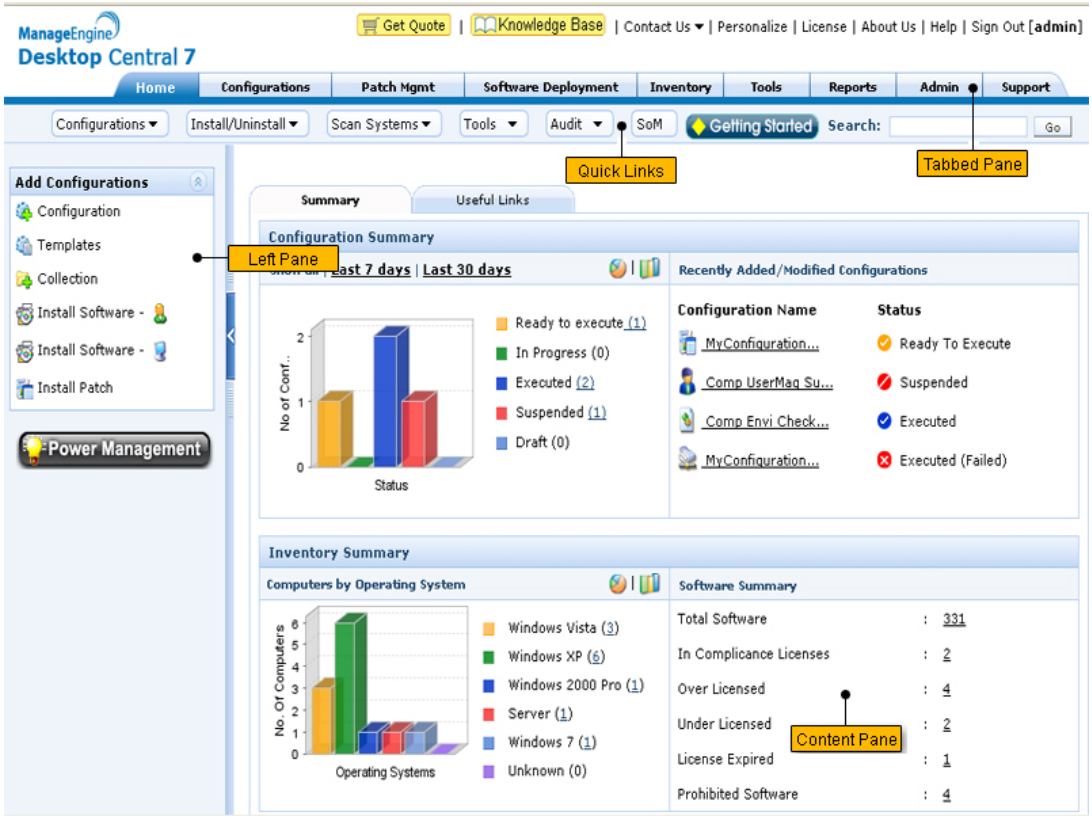
For purchasing the license or for any pricing related queries, please contact sales@manageengine.com.

To upgrade from a Trial/Free Edition to Standard/Professional/Enterprise Edition

1. When you purchase the product, the license file will be sent through e-mail, which can be used to upgrade the product.
2. Click the **License** link available in the top right corner of the Desktop Central client. This opens the License details of the product.
3. Click the **Upgrade Now** link and select the license file received from ManageEngine using the **Browse** button.
4. Click **Upgrade** button to upgrade.

Understanding the Client UI

Desktop Central client presents complex desktop management information to administrators in a clear, well organized, and easily understandable manner. The Client is a multi-pane interface with tabs and quick links on the top pane, tab-specific links on the left pane, and object-specific views on the right pane. The home page looks similar to the one shown below:



Tabbed Pane

Tabs provides easier navigation between various modules/features of Desktop Central. Each tab represent a specific module/feature in Desktop Central. The content of the left pane varies depending on the tab selected. The following are the tabs present in the product:

- **Home**: The home tab provides a quick summary of the configurations defined in the form of charts. Apart from the configuration summary, it also provides Inventory summary and the health/patch status of the network.
- **Configurations:** The configurations tab provides the core functions of the product. It has links to define configurations and collections and view the defined configurations based on the type and status.
- **Patch Mgmt**: This provides the details of the available and missing patch details along with options to install them.
- **Software Deployment:** Provides options to create MSI and EXE package repository, which can then be used to deploy software to the windows machines in the network.
- **Inventory:** Provides the details of the software and hardware inventory of the network. It allows you to manage software licenses and prohibited software.
- **Tools:** The Tools tab provides ability to share a remote desktop and control it through a Web browser. You can also schedule a task to run various system tools like Disk Defrag, Check Disk, and Disk Cleanup on different machines in the network.
- **Reports:** The reports tab provides a comprehensive reports of the defined configurations based on users, computers, and type. It also provides ready-made reports of the Active Directory components. For more details about the available reports, refer to Viewing Reports topic.
- **Admin**: The admin tab helps you to customize the product to your environment. It helps you to define the scope of management, manage inactive users in your domain, manage MSI/EXE files and scripts, apart from other personalization options. For further details, refer to Configuring Desktop Central section.
- **Support:** The support tab helps you to reach us for your needs, such as getting technical support, requesting new features, participating in user discussions, and so on. It also provides self-diagnostic details about the product.

Apart from the tabs, it also has the following links on the top right corner:

- **Contact Us**: To reach us to support, feedback, sending logs, joining web conference to troubleshooting, etc.
- **Personalize**: To customize the skin, password, and session expiry time.
- **License**: To upgrade to the licensed version of the software and to view the license details.
- **About Us**: To view the product version details.
- **Help**: To view the product help documentation.
- **Sign Out**: To sign out the client.

Quick Links

Quick links enables you to navigate to the frequently used pages instantly.

Left Pane

The navigation links in left pane enables navigation across the various features in the tab. The left-side navigation links changes dynamically according to the tab selected.

Content Pane

The content pane displays the specific view of the currently selected item from the tabbed pane, quick links or the left pane.

Setting Up Desktop Central

After installing Desktop Central, the administrator has to setup the various modules in Desktop Central by making the required configurations.

Note: The steps/configurations described in this section can only be performed by users with administrative privileges in Desktop Central.

Follow the links to learn more:

- Configuring Desktop Central for Windows Vista / 2008
- Working with the Scope of Management
- Configuring Agent Tray Icon Settings
- Configuring Mail Server
- Configuring Help Desk Integration
- Managing Custom Scripts
- Configuring Server Settings
- Creating Custom Groups
- Personalizing the Client Settings
- Authenticating Users via Active Directory
- Migrating Desktop Central Server
- User Administration
- Setting Up Software Deployment
- Setting Up Patch Management
- Setting Up Asset Management
- Setting Up User Logon Reports
- Setting Up Active Directory Reports

Configuring Desktop Central for Windows Vista / 2008 / Windows 7

This is applicable only if you install Desktop Central Server in Windows Vista, Windows 2008 or Windows 7.

For running Desktop Central Service in Windows Vista, Windows 2008 or Windows 7 operating systems, you need to specify user credentials with administrative privileges. This is not required for other operating systems like Windows XP, 2003 Server, etc.

Specifying Admin User Credentials for Windows Vista / Windows 2008 / Windows 7.

When you install Desktop Central server in Windows Vista / Windows 2008 / Windows 7 and start, the Desktop Central client will show a page asking for the user credentials with administrative privileges on that computer. Specify the user name and password of an user account that has administrative privileges on the computer where Desktop Central Server is installed. The user specified here can be either a domain user or a local user with admin privileges.

It is recommended to set the password of the user specified here to "**Password Never Expires**". When the password of this user changes, Desktop Central Server will not be able to start as the credentials will fail.

Defining the Scope of Management

After successful installation, the first thing you do is to define the Scope of Management(SoM) to use the features of Desktop Central. The SoM refers to the list of computers that are managed using Desktop Central. The managed computers can be from Active Directory, Workgroup, or any other directory service like Novell eDirectory. The managed computers can be either in the same LAN or in any remote location that are connected through VPN or Internet.

Following the Scope of Management section, you can proceed with:

- Adding Domain/Workgroup
- Managing computers in LAN
- Managing computers in WAN

Adding Domain / Workgroup

A windows network is typically based on Windows Active Directory, Workgroup, or Novell eDirectory. When you install desktop Central in your network, it automatically discovers all the domains and workgroups available in your network. Novell eDirectory based network are discovered and managed as workgroups in Desktop Central.

Discovering Domains / Workgroups

To view the discovered domains/ workgroups or to initiate the discovery, select **Admin tab --> Scope of Management (SoM) --> Add Computers**. This will discover all the available domains and workgroups and list them under Discovered Networks.

Adding Domains

Domain can be added in Desktop Central in two ways:

1. From the auto-discovered list available in the **SoM --> Add Computers** page by clicking the **Edit** link corresponding to the domain.
2. By Manually adding the domain - If for some reason, one or more domains are not discovered, you can use the **Add Domain** link available in the same page to add domains manually.

Both the above options will open the **Add Domain** dialog for accepting the following information:

Parameter	Description	Type
Domain Name	Name of the domain. This is usually the netbios or the pre-2000 name of the domain	Mandatory
Network Type	Select "Active Directory" option	Mandatory
Domain User Name	This should be the domain user name that has administrative privileges in all the computers of that domain. It is recommended to have a dedicated domain admin user account for Desktop Central whose password policy is set to "Never Expire"	Mandatory
Password	Password of the domain admin user	Mandatory
AD Domain Name	The DNS name of the Active Directory Domain	Mandatory
Domain	The name of the domain controller. If you have multiple	Mandatory

Parameter	Description	Type
Controller Name	domain controllers, provide the name of the domain controller that is nearest to the computer where Desktop Central Server is installed	

If you have problems in adding the domains, refer to our online knowledge base for possible reasons and solutions.

Adding Workgroups

Similar to domains, Workgroups can be added in Desktop Central in two ways:

1. From the auto-discovered list available in the **SoM --> Add Computers** page by clicking the **Edit** link corresponding to the workgroup.
2. By Manually adding the workgroup- If for some reason, one or more workgroups are not discovered, you can use the **Add Domain** link available in the same page to add workgroups manually.

Both the above options will open the **Add Domain** dialog for accepting the following information:

Parameter	Description	Type
Domain Name	The name of the workgroup	Mandatory
Network Type	Select "Workgroup" option	Mandatory
Admin User Name	A common user name which has administrative privileges in all the computers within that workgroup. It is recommended to have a dedicated user account for Desktop Central whose password policy is set to "Never Expire"	Mandatory
Password	The password of the common admin user	Mandatory
DNS Suffix	This is required to uniquely identify a computer within a workgroup. For example, if you have a computer with the same name in two different workgroups, the DNS suffix is used to identify it uniquely	Optional

If you have problems in adding the workgroups, refer to our online knowledge base for possible reasons and solutions.

	Note: Computers in Novel eDirectory based network are managed as Workgroups in Desktop Central.

Changing the Domain or Workgroup Credentials

Desktop Central establishes a remote connection to the managed computers to perform the various Desktop Management activities like agent installation / upgradation, patch/inventory scanning, and remote desktop sharing, which requires an admin credential. The credential provided when adding a domain/workgroup is used for this purpose. When the username/password provided while adding the domain/workgroup has changed later due to password expiry or other reasons, you need to update the correct credentials from the **Admin tab --> SoM** page to avoid getting "Access Denied" errors while performing any remote operations.

To update the credentials, click the **Edit Credentials** button available in the SoM page. Select the Domain/Workgroup from the select box, update the username/password and click **Update Domain Details**.

Synchronizing Computers from Active Directory

Synchronizing computers from Active Directory will help you find the computers that are newly added, but or not managed in Desktop Central and the computers that have been deleted from the Active Directory. This helps you to quickly add or remove computers from being managed using Desktop Central. The synchronization will happen at a specified time everyday and can be configured to notify you whenever a change is detected.

To enable synchronization follow the steps below:

1. Select **SoM --> AD Sync** tab
2. Click **AD Sync Settings** link from the right, below the AD Sync tab.
3. Select **Enable AD Sync**
4. Specify the time at which the sync should happen. The time should be specified in 24 hour format and the sync will happen at the same time everyday.
5. Click **Choose Domains/OUs** to select the domains and OUs that you would like to sync. This will only list the domains and OUs for which the credentials have been specified.

   Note: If you do not see all the domains, you should check and specify the credentials first from SoM --> Computers --> Edit Credential.
6. If you wish to be notified on any change, select "**Enable Email Notification**" and specify the "To Address", subject and message.
7. Click **Save**

Next Steps

The next step is to add and install the agent in the client computers that have to be managed using Desktop Central. The following sections will detail the steps:

- Managing Computers in LAN - To add and install the agent in the client computers from the same LAN where Desktop Central Server is installed
- Managing Computers in WAN - To add and install the agent in the client computers from remote locations like branch offices and mobile users.

Managing computers in LAN

Desktop Central installs an agent in all the client computers that have to be managed using Desktop Central. The agent properties can also be customized prior to installing the agents. For details on customizations, refer to Configuring Agent settings.

Installing Agents

Installing Agents from Desktop Central Console

1. The client computers can be added from **Admin tab --> SoM --> Add Computers** button. This will list the domains and workgroups that have been added.
2. Click the Select Computers link pertaining to a domain/workgroup. This opens the Select Computers dialog listing all the available computers of the domain/workgroup.
3. Select the computers that have to be managed using Desktop Central and click OK. You can also manually specify the computer names instead of choosing them from the list. The selected computers gets added to the Selected Computers table in the Add Computers view.
4. Repeat steps 2 and 3 for adding computers from multiple domains/workgroups.
5. Select the "Start Agent Installation Immediately" check box to install the Desktop Central agents in the selected computers immediately. When this option is not selected, the computers are only added. You need to install the agents later to manage them.
6. Select the Configure Agent Settings option for configuring the agent properties and post installation actions.
7. Click Done to add the selected computers. All the selected computers gets added to the Scope of Management.

The Scope of Management page will list all the computers that are being managed by Desktop Central along with the status of the agent installation and the agent version.

Agents can also be installed at a later stage, by selecting the computers from **Admin --> SoM** page and clicking the **Install Agent** button from the Desktop Central Console

If you have problems in installing the agents, refer to our online knowledge base for possible causes and solutions.

Installing Agents Using Windows GPO

Agent installation through the console might fail due to various reasons like some security restrictions, firewall configurations, etc. There is a possibility that even after trying the resolutions provided in the online knowledge base, the installation can still fail. In such cases, you can install the agents with a startup script using Windows GPO. The agents gets installed during the next computer startup.

Refer to the online knowledge base for the steps to install the agents using Windows GPO

Installing Agents Manually

You can also install the agents manually, by downloading the agent program from:
http://<host name>:<port number>/agent/DesktopCentralAgent.msi
where,
<host name> refers to the machine running Desktop Central and
<port number> refers to the Web port to access the client, the default being 8020.
Double-click the msi file to install the agent manually.

Uninstalling Agents

To uninstall the agents from the computers, select the desktops from the list and select Uninstall Agent from the Actions box.

Removing the Computers

To remove the computers from the list, select the computers and select Remove Computer from the Actions box. The Desktop Central agents have to be uninstalled prior to removing a computer from the scope.

Managing Computers in Wide Area Networks (WAN)

A WAN is a computer network that enables communication across a large area that could include communication across cities, states and countries. Most companies operate from a head office, located in a city, and have branch offices located in other areas within the city, the state, the country or even in another country. These branch offices are known as remote offices.

As a system administrator, you must do the following:

- Ensure that the computers in the head office and branch offices are monitored efficiently
- Manage computers of roaming or mobile users who connect to the network using the Internet

One of the main challenges that you could face, while managing computers in a WAN, are with the bandwidth allocated. There could be bandwidth issues that reduce the speed of data-transfer between computers at the head office and those at the branch office. This could result in costs associated with bandwidth utilization.

Managing Computers Across a WAN

There are two options to manage computers, across a WAN, using Desktop Central. The option that you choose depends on the number of computers you are going to manage at your remote office. The options available, enable you to use either of the following:

- Distribution servers and WAN agents: It is recommended that you use this option if you are managing more than 10 computers in a remote office.
- WAN agents only: It is recommended that you use this option if you are managing less than 10 computers in a remote office.

Using Distribution Servers and WAN Agents

A distribution server is a server that is located in a remote office. This server communicates with the Desktop Central server, which is located at the head office, to get information; for example information about configurations to deploy. It synchronizes its repositories, related to configurations, patches, service packs and software applications, with those located in the Desktop Central server. This takes place at specific intervals.

WAN agents are installed in computers in a remote office. After the synchronization, between the distribution server and the Desktop Central server is complete, the WAN agents will download information related to patches, service packs and software applications to be

deployed, from the distribution server. This information is downloaded locally using the LAN in the remote office.

Desktop Central's technology related to distribution servers helps you plan and control bandwidth utilization (including associated costs) for your remote office. This technology addresses bandwidth-related issues, improves the efficiency and the level of control that network managers and administrators can use while managing computers in remote locations.

Before you start managing computers in a remote location you are required to do the following:

- Add a remote office
- Deploy a distribution server to a remote office
- Deploy WAN agents to computers managed using the distribution server

Adding a Remote Office (with a distribution server)

Before you can start managing computers in a remote office, you are required to add a remote office and create a distribution server. To add a remote office and create a distribution server using your Desktop Central server, follow the steps given below:

1. Select **Admin** tab
2. In the **Global Settings** section, click **Scope of Management**
3. Select the **Remote Office**s tab
4. Click **Add Remote Office**
5. Enter a name for the remote office
6. In the Desktop Central Server Details section, specify the IP address and port numbers for the Desktop Central server

	The IP address is already entered in the given field. Change this address only if you have a secondary IP address for the Desktop Central server. The information for the HTTP and HTTPS ports are already entered (8020 and 8030 respectively). Change the port numbers if you have specified ports other than these while installing the Desktop Central server.

7. In the Communication Details section, select **Through Distribution Server**.
8. In the Distribution Server Details section, enter the following information:

o Domain NetBios name
o Computer name
o IP address of the computer on which the distribution server will be installed

	It is recommended that you have a dedicated computer as your distribution server. This computer should have a static IP address. This will ensure that you have hassle-free communication between the WAN agents and the distribution server.

- DS FQDN/DNS Name (optional)
- HTTP and HTTPS port numbers for the distribution server

The HTTP and HTTPS ports are used for communication between the WAN agents and the distribution server. The default ports of the distribution server 8021 (HTTP) and 8384 (HTTPS). You can use different ports if required.

- Replication interval time

The replication interval time is the interval at which the distribution server synchronizes its repositories with those in the Desktop Central server. The default interval is two minutes. However you can customize the replication interval if required.

- Data-transfer rate

9. In the Distribution Server/WAN Agent to Desktop Central Server Communication section, check the following check boxes:
   - Enable Secured Communication (HTTPS)
   - Proxy Configuration. Enter information about the proxy host, user name and password.
10. In the computers to be managed section, add the computers that you want to manage using the distribution server. To add computers to be managed, follow the steps given below:

    a. Select the required domain or workgroup

    b. Select the required organization units or computers

    c. Click **Add**

If you know the name or the IP address of the computers that you want to manage in the remote location, add them in the given field using commas.

11. Click **Add**

You have added a remote office and created a distribution server. You are now required to deploy this distribution server to a specific remote office.

Deploying Distribution Servers To Remote Offices

After you have added a remote office and created a distribution server, you are taken back to the Remote Offices tab view in the Scope of Management page. In the Managed

Computers column, against the name of the remote office you have created, the status will be **Agent is not installed**. You are required to deploy and install the distribution server in the required remote office.

To deploy a distribution server to the required remote office, follow the steps given below:

1. Select **Admin** tab
2. In the **Global Settings** section, click **Scope of Management**
3. Select the **Remote Office**s tab
4. In the **Download Agent** column, against the remote office you added, click the Download WAN Agent + Distribution Server icon
5. Save the .zip file in the computer on which you want to install the distribution server

You are required to login as the administrator, on the computer in which you want to install the distribution server, to save the required file in it.

6. Extract the contents of the zip file
7. Open a command prompt. To open a command prompt, follow the steps given below:
    a. Click **start>Run**
    b. Enter cmd
    c. Click **OK**
8. Navigate to the working folder (this is the folder which you have extracted the .zip file in). For example: C:\Remote-Office\dssetup
9. Run the command setup.bat
10. Select option 1 to deploy the distribution server

You have deployed the distribution server to the required remote office. Refer to the Agent Installation section for information on how to install WAN agents.

Deploying WAN Agents in Computers in Remote Offices

You are required to install WAN agents in the computers you want to manage, in a remote office, using a distribution server. A WAN agent can be installed:

- While deploying a distribution server
- After deploying a distribution server

Deploying WAN agents while deploying a distribution server

To deploy a WAN agent while deploying a distribution server, follow the steps given below:

a. Open a command prompt. To open a command prompt, follow the steps given below:
    a. Click **start>Run**
    b. Enter cmd
    c. Click **OK**
b. Navigate to the working folder (this is the folder which you have extracted the .zip file in, while deploying the distribution server). For example: C:\Remote-Office\dssetup
c. Specify which computers the WAN agents have to be installed in by editing the computers.txt file
d. Run the command setup.bat file
e. Select option 2
f. Specify the administrator's user name and password when prompted

This can be a domain administrator or a user who has administrator privileges in all the computers where WAN agents have to be installed. The user name should be prefixed with the name of the domain or the workgroup.

For example, the user name of an administrator who is deploying WAN agents in computers, which are in the zohocorp domain, could be zohocorp\administrator.

You have deployed both the distribution server and WAN agents to computers in a remote office.

Deploying WAN agents after deploying a distribution server

To deploy a WAN agent after deploying a distribution server, follow the steps given below:

a. Open a command prompt. To open a command prompt, follow the steps given below:
    a. Click **start>Run**
    b. Enter cmd
    c. Click **OK**
b. Navigate to the working folder (this is the folder which you have extracted the .zip file in, while deploying the distribution server). For example: C:\Remote-Office\dssetup
    3. Specify which computers the WAN agents have to be installed in by editing the computers.txt file
4. Run the command setup.bat

5. Select option 3
6. Specify the administrator's user name and password when prompted

This can be a domain administrator or a user who has administrator privileges in all the computers where WAN agents have to be installed. The user name should be prefixed with the name of the domain or the workgroup.

For example, the user name of an administrator who is deploying WAN agents in computers, which are in the zohocorp domain, could be zohocorp\administrator.

You have deployed WAN agents to computers in a remote office.

Using WAN Agents Only

When you manage less than 10 computers, typically, there are no bandwidth-related issues. In such cases, you can manage computers in your remote office using WAN agents only.

Before you start managing computers in a remote office using WAN agents only, you are required to do the following:

- Add details of a remote office (single remote office or multiple remote offices)
- Install WAN agents in the computers in the remote office

Adding a Remote Office (without a distribution server)

If you are managing in branch/remote offices, you need to add the details of the branch/remote offices and generate Desktop Central Agent for each of your branch/remote office. This agent has to be installed in the managed computers of that branch. To add the details of the remote offices, follow the steps below:

1. Select **Admin** tab
2. In the **Global Settings** section, click **Scope of Management**
3. Select the **Remote Office**s tab

You will see a list of all the remote offices that are added. In that list, you will see a remote office which is called Local Office. This is related to the LAN where the Desktop Central server is located. The remote office Local Office is added by default.

4. Click **Add Remote Office**
5. Enter a name for the remote office
6. In the Desktop Central Server Details section, specify the IP address and port numbers for the Desktop Central server

This IP Address should be common for all the Remote offices and will be used by the agents in the remote office computers to contact the Desktop Central server. If this IP Address is changed, the agent MSI for remote offices will be recreated. You need to reinstall the agents in all the remote computers.

7. In the Communication Details section, select **Direct Communication**.
8. In the WAN Agent to Desktop Central Server Communication section, do the following:
    a. Specify the communication interval

The communication interval is the interval at which the WAN agents in the computers in the remote office, contact the Desktop Central server for information. The default communication interval is two minutes. However, this value can be configured if required.

b. Check the following check boxes:
    a. Enable Secured Communication (HTTPS)
    b. Proxy Configuration. Enter information about the proxy host, user name and password.

9. In the computers to be managed section, add the computers that you want to manage using the distribution server. To add computers to be managed, follow the steps given below:

    a. Select the required domain or workgroup

    b. Select the required organization units or computers

    c. Click **Add**

If you know the name or the IP address of the computers that you want to manage in the remote location, add them in the given field using commas.

10. Click **Add**

You have added a remote office.

Adding Multiple Remote Offices

You can add multiple remote offices simultaneously by importing details of the remote offices, using the CSV import option.

To add multiple remote offices simultaneously, follow the steps given below:

1. Click the **Admin** tab
2. In the **Global Settings** section, click **Scope of Management**
3. Click the **Remote Offices** tab
4. Click **Import Remote Offices**
5. Click **Choose File** and select the required CSV file
6. Click **Import**

You have imported multiple remote offices simultaneously. These will be listed in the Remote Offices tab.

Information about CSV files

This section gives you information about CSV files.

File specifications

- The first line of a CSV file is the header specifying the column names.
- The Remote Office name is a mandatory field and all the other fields are optional. If left blank, the default values will be added to those fields.

Column names and descriptions

- REMOTE_OFFICE_NAME: Name of the remote office
- POLLING_INTERVAL: Communication Interval / Replication Interval based on the Communication Type. The default value is 2 minutes
- SERVER_IP:The IP Address of the Desktop Central server, which is accessible from the computers in the remote office.
- HAS_DS - The values can be Yes or No. Yes means that the communication type is through the distribution server. If newly added (or the previous values are present in case of modification), the default value is No. If the value is Yes, the following columns are mandatory:
- DS_DOMAIN_NAME: Name of the Netbios domain in the distribution server
  DS_NAME: Name of the computer in which the distribution server will be installed
  DS_IP: IP Address of the computer in which the distribution server will be installed
  DS_PORT: HTTP port through which the distribution server and the WAN agents communicate
  DS_HTTPS_PORT: HTTPS port through which the distribution server and the WAN agents communicate
- PROTOCOL: The mode of communication between distribution server, WAN agents and the Desktop Central server. The default is HTTP.
- HAS_PROXY - The values can be Yes or No. Yes means the communication between the distribution server or WAN agents to the Desktop Central server takes place through the proxy server. If newly added (or the previous values are present in case of modification), the default value is No. If the value is Yes, the following columns are mandatory:
- PROXY_SERVER:Name or IP address of the proxy server
- PROXY_PORT: Proxy port number

- PROXY_USER:User name used to acces the proxy server
- PROXY_PASSWORD: Password of the proxy user account.
- COMPUTERS: Names of the computers in the remote office. If more than one computer is specified, it should be within double-quotes. Example: "john,jerry"

Sample CSV Formats

- REMOTE_OFFICE_NAME,POLLING_INTERVAL,HAS_DS,DS_DOMAIN_NAME,DS_NAME,DS_IP,DS_PORT,DS_HTTPS_PORT,PROTOCOL,HAS_PROXY,PROXY_SERVER,PROXY_PORT,PROXY_USER,PROXY_PASSWORD,COMPUTERS
- RO_1,2,yes,zohocorpin,DSserver1,192.168.1.227,8021,8384,http,yes,web proxy,80,admin,admin,"test,mathi,karups"
- RO_2,3,yes,zohocorpin,DSserver2,192.168.1.232,8021,8384,http,no
- RO_3,10,yes,zohocorpin,DSserver3,192.168.1.222,8021,8384,https,yes,web-proxy,80,admin,admin
- RO_4,30,yes,zohocorpin,DSserver4,192.168.1.233,8021,8384,https,no
- RO_5,2,no,,,,,,http,yes,web-proxy,80,admin,admin
- RO_6,3,no,,,,,,http,no
- RO_7,33,no,,,,,,https,yes,web-proxy,80,admin,admin
- RO_8,35,no,,,,,,https,no

Editing Remote Office Parameters

The method of importing CSV files also has an option where you can edit the details of a remote office. Assume that you want to change the name of the proxy server for your remote offices. You don't have to manually edit the proxy details of each and every remote office. You can do this by creating a CSV file that contains only the remote office name and the parameter that needs to be updated. For example,

REMOTE_OFFICE_NAME,PROXY_SERVER
RO_1, web-proxy1
RO_2, web-proxy2

Installing Agents in Computers in Remote Offices

You can install agents in computers in remote offices in:

- Single computers
- Multiple computers

	Desktop Central agents have to be manually downloaded and installed in computers in remote offices. ffice computers. To install an agents in multiple computers in the same location, you can use the command line tool that is provided.

Installing Agents in a Single Computer

1. Click the **Admin** tab
2. In the **Global Settings** section, click **Scope of Management**
3. Click **Download Agent**

	Ensure that you have downloaded the agent with the respective remote office name.

4. Install the agent in the required computer in a specific remote office, manually
5. Extract the .zip file to a directory
6. Open a command prompt. To open a command prompt, follow the steps given below:
    a. Click **start>Run**
    b. Enter cmd
    c. Click **OK**
7. Change the directory to <Extracted_Dir>/directsetup
8. Execute the following command:

```
%systemroot%\\system32\msiexec.exe /i DesktopCentralAgent.msi
ENABLESILENT=yes /qn
```

You have installed an agent in a single computer in a specific remote office

Installing Agents in Multiple Computers

1. Click the **Admin** tab
2. In the **Global Settings** section, click **Scope of Management**
3. Click **Download Agent**

	Ensure that you have downloaded the agent with the respective remote office name.

4. Install the agent in the required computer in a specific remote office, manually
5. Extract the .zip file to a directory
6. Add all the names of the computers in which the agent has to be installed in the computernames.txt file

	Each computer name should be entered in a separate line.

7. Open a command prompt. To open a command prompt, follow the steps given below:
    a. Click **start>Run**
    b. Enter cmd
    c. Click **OK**
8. Change the directory to <Extracted_Dir>/directsetup
9. Run the command setup.bat
10. Specify the user name and password of the administrator, when prompted

	This can be a domain administrator or a user who has administrator privileges in all the computers where WAN agents have to be installed. The user name should be prefixed with the name of the domain or the workgroup. For example, the user name of an administrator who is deploying WAN agents in computers, which are in the zohocorp domain, could be zohocorp\administrator.

You have installed the agent in multiple computers in a remote office.

	The logs.txt file is located in <Extracted_Dir>/directsetup. It has the details about the errors you face during installation, if any.

Modifying Remote Office Details

If you require to change the mode of communication between the WAN Agents and the Desktop Central server, you can modify the remote office details and make the necessary changes. For example, if you have chosen the direct communication mode for a remote office and you want communication to take place through the distribution server, you can modify the details of the remote office.

To modify the details of the remote office, follow the steps given below:

1. Click the **Admin** tab
2. In the **Global Settings** section, click **Scope of Management**
3. Click the **Remote Offices** tab
4. In the **Action** column, click the modify icon against the required remote office
5. Change the required parameters
6. Click **Modify**

	If you have changed the mode of communication from direct communication to communication through the distribution server, you need to re-install and re-start the distribution server in the specified computer. The changes will be implemented only after you complete this task. However, even if you have not completed this task, you can still deploy the configurations, patches, and software applications to the specific remote computer.

You have modified details of a remote office.

Moving Computers Across Remote Offices

You can move computers across remote offices. For example, if you are moving from remote office to another you are required to add your computer to the WAN in that remote office.

Scenario

Each remote office has its own agent. Assume that you are moving from remote office A to remote office B. You must do the following when you are moving computers across remote offices:

- Move the computer physically
- Make the settings to move the computer from one remote location to another in the user interface (UI)

The sequence of operations, mentioned above, will depend on whether you have a proxy connection or not.

When the agent does not use a proxy connection

When the agent does not use a proxy connection to communicate with the Desktop Central server, you can physically move your computer from remote office A to remote office B, the agent from remote office B gets installed in your computer. As there is no proxy connection, it can communicate with the Desktop Central server.

When the agent uses a proxy connection

When the agent uses a proxy connection to communicate with the Desktop Central server, you must make the settings to move the computer from one remote office to another, in the UI, before you physically move your computer.

To move computers across remote offices, follow the steps given below:

1. Click the **Admin** tab
2. In the **Global Settings** section, click **Scope of Management**
3. In the **Computers** tab, select the required computers
4. In the **Move To** list, select the name of the remote office to which you want to move your computer to

	You can create a new remote office with or without a distribution server. To create a new remote office with a distribution server, refer to the Adding a Remote Office (with a distribution server) section. To create a new remote office without a distribution server, refer to the Adding a Remote Office (without a distribution server) section.

You have created a request to move computers across remote offices. If the office you are moving to is a local office (LAN), the computers that you have specified will be moved immediately. This is because the Desktop Central server can contact the agent in the computer, that you have requested to move, immediately. However, if the office you are moving to is a remote office (WAN), the computers that you have specified will be moved only when the agent (in the specified computers) contacts the Desktop Central server agent during the two-minute communication interval.

	If the agent does not contact the Desktop Central server within the time interval, the request will be removed from the Desktop Central server. You will then have to create a new request.

Adding an IP Scope

IP Scope refers to the IP addresses, in IP subnets, used by all the remote offices managed using Desktop Central. These IP addresses are assigned to the network in each remote office.

You define an IP Scope when you want to transfer computers, automatically, from one remote office to another.

	If there is no movement or a rare chance of moving computers between remote offices, you do not need to define an IP Scope for your remote offices. In this case, you can move your computers, if required, by using the **Move to** list in the **Computers** tab in the **Scope of Management** page. For more information, click here.

When a computer (or a laptop) is transferred to a new remote office, a new IP address is automatically assigned to that computer (or laptop) by the DHCP server in the remote office network. The Desktop Central agent then determines whether the new IP address, that was

assigned, is within the IP range of the new remote office. You can add an IP Scope for remote offices as well as local offices.

If you are moving computers only between specific remote offices, you should assign an IP Scope only for those remote offices.

To add an IP Scope, follow the steps given below:

1. Click the **Admin** tab
2. In the **Global Settings** section, click **Scope of Management**
3. Click the **IP Scope** tab
4. Click **Add Scope**
5. In the **Select Remote Office** list, click the required remote office name
6. Select either of the following types of IP Scope:

- **IP Address Range**: Enter the start and end IP addresses
- **Subnet**: Enter the subnet mask and subnet IP address

7. Click **Save**

You have added an IP Scope.

You can add more than one IP Scope to a remote office. To add more than one IP Scope, follow the steps from step number 4.

Configuring Agent Settings

Desktop Central installs an light-weight non-intrusive agent on the computers that have to be managed using Desktop Central. You have an option to configure the settings for these agents.

Agent General Settings

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Agent Settings** link available under Global Settings.
3. The **General Settings** tab is selected by default. You can specify the following from here:
    1. **Server IP Address -** The IP Address of the computer where Desktop Central server is installed is displayed here. The agents residing in the client computers communicate to the Desktop Central server using this IP Address. Desktop Central automatically detects the server IP Address whenever Desktop Central Server is started. If you wish to automatically detect and save the IP Address, select the **Automatically detect and save the IP Address change** option.
    2. **Enable Secured Communication** - Select this option, if the communication between the Agent and the Desktop Central Server should be secured (HTTPS)
    3. **Disable Uninstallation Option in Control Panel** - Selecting this option will ensure that users do not uninstall the Desktop Central Agents from their computer.
    4. **Perform Patch Scanning** - Select this option if Patch Scanning has to be initiated immediately after the agent installation. If this option is not selected, Patch Scanning will only happen when it is scheduled or when On Demand scanning is initiated.
    5. **Perform Inventory Scanning** - Select this option if Inventory Scanning has to be initiated immediately after the agent installation. If this option is not selected, Inventory Scanning will only happen when it is scheduled or when On Demand scanning is initiated.
    6. **Enable Firewall Settings** - Desktop Central requires the Windows Firewall running in the client computers to be configured for using all its features. Select this option to configure the firewall for enabling Remote Administration, DCOM, File and Printer Sharing, and Simple File Sharing in Windows XP.
4. Click **Save Changes**.

Agent Tray Icon Settings

Desktop Central provides an option to display the Agent Icon in the System Tray of all the managed computers. The users can perform the following actions using the system tray:

1. Initiate Patch Scanning
2. Initiate Inventory Scanning
3. Pull and apply configurations that are available to them
4. Send requests to Help Desk for specific needs.
5. When User Logon Reports is enabled, the user will be able to view his/her login history.

Follow the steps below to configure the Tray icon settings:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Agent Settings** link available under Global Settings.
3. Select the **Agent Tray Icon** tab and specify whether to display the icon in the system tray of the managed computers. When choosing this option, you can choose the following:
    1. Show Patch, Inventory, and Configuration Menus
    2. Show Last Logon Details
    3. Show Information Balloons While Processing Configurations, Patch Scanning and Inventory Scanning
4. Click **Save Changes**

Configuring Mail Server

Desktop Central has an option to send a notification by email when the patches are downloaded and are ready to be installed. Email Alerts are also sent for notifying the Inventory related events. To send email, the mail server has to be configured. Follow the steps given below to specify the mail server details:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Mail Server Configuration** link. This opens the Configure Mail Server Settings page.
3. Specify the name and port of the mail server.
4. **Email Type :** Indicates the type of mail email despatching (For example: SMTP, SMTPS).
5. **TSL Enabled :** Option to enable Transport Layer Security (TLS).
6. If it requires authentication, select the Requires Authentication check box and specify the user name and password.
7. Click **Save** to save the configuration.

Configuring Help Desk Integration

Desktop Central provides an option to integrate with Help Desk. With this, users will be able to send their help desk queries and requirements so that they are attended by help desk professionals.

Steps to Integrate with Help Desk

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Help Desk Settings** link available under Global Settings.
3. The **Help Desk Settings** tab is selected by default.
4. Specify the Email addresses of the help desk professionals.
5. If you have not already configured the Mail Server Settings, specify the details here.
6. Click **OK** to save the changes.

When you integrate with Help Desk, the users will have an additional menu as "Send Help Desk Requests" in the Agent icon that is shown in the system tray of the managed computers. It may be noted that the Agent Tray icon should have been configured to be shown to get this working.

Customizing the Ticket Subjects and Messages

Desktop Central has a set of pre-defined request templates that will be available under the Tickets tab. The administrators has an option to modify the subject and messages to suit their need. This helps them to automate the Help Desk Ticketing system based on the mail subject. To add or modify a ticket, follow the steps below:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Help Desk Settings** link available under Global Settings.
3. Select the **Tickets** tab. This will list all the pre-defined ticket templates.
4. Click **Add Ticket** to add a new template or select a template and click **Edit** to modify.
5. Specify the Subject and the Message and click **OK**

The templates specified here will appear in the users' desktop when they click the Desktop Central icon from the system tray.

Integrating Desktop Central with ServiceDesk Plus

ServiceDesk Plus is a Web-based help desk and asset-management software. It enables you to integrate your help-desk requests and assets to help you manage your IT infrastructure effectively. You can integrate the following features of Desktop Central with ServiceDesk Plus:

- Data related to hardware and software assets
- Help-desk requests
- Deploying software packages
- Complete UI Integration - This makes you access all the features of Desktop Central from the ServiceDesk Plus console.

Benefits

Integrating the features mentioned above with ServiceDesk Plus enables you to do the following:

- Get comprehensive information about IT assets like hardware and software assets installed in the computers in your network
- Log service and configuration requests, made by users as tickets automatically
- Install software packages from the ServiceDesk Plus console

Steps to Integrate

The pre-requisites and the steps for integration vary for every feature that you wish to integrate. The links below will guide you through the integration:

- Integrating Asset Data with ServiceDesk Plus
- Automatically Log Help Desk Requests as Tickets in ServiceDesk Plus
- Include Software Install / Uninstall option under the Actions menu of a Help Desk request in ServiceDesk Plus
- Make a complete UI integration between ServiceDesk and Desktop Central

Integrating Asset Data

Desktop Central scans the computers in your network periodically and collects data related to hardware and software assets that are installed. Information related to hardware and software applications is updated by Desktop Central. This data is synchronized with ServiceDesk Plus.

If both Desktop Central and ServiceDesk Plus scan the computers in your network for data related to hardware and software assets the existing information will be overwritten with the latest information.

Prerequisites

Before you integrate details about assets with ServiceDesk Plus, you must ensure the following:

1. Ensure that the build numbers conform to the details given below:
   - Desktop Central: Professional Edition, Build number 70017 or later versions
   - ServiceDesk Plus: Professional Edition, Build number 7601 or later versions
2. Run both Desktop Central and ServiceDesk Plus in your network
3. Manage all the computers in your network using Desktop Central

Integrating Desktop Central with ServiceDesk Plus

To integrate ServiceDesk Plus with Desktop Central, follow the steps given below:

1. Click the **Admin** tab
2. In the **Global Settings** section, click **ServiceDesk Plus Settings**
3. In the **ServiceDesk Plus Settings** section, check the **Enable ServiceDesk Plus Integration** checkbox
4. In the **Service Desk Server Plus Details** section, specify the following details about the **ServiceDesk** Plus Server:

    1. IP address/DNS name
    2. Port number
    3. Required communication protocol

1. In the **Features to Integrate** section, select IT Asset Data checkbox
2. Click **Save**

If you select HTTPS mode of communication, Select the Product Type :If you are using an standalone installation of ServiceDesk Plus product, select the ServiceDesk Plus option. If you wish to integrate with the ServiceDesk module within IT360 product, select IT360 option.

you must provide the SSL certificate of ServiceDesk Plus. copy the file **"sdp.keystore"** located in **<ServiceDesk Plus Installation Home>/server/default/conf** directory to

your local computer and Browse to select this file here.
If you are using IT360 product with HTTPS communication enabled, copy the file **"it360.keystore"** located in **<IT360 Installation Home>/servicedesk/server/default/conf** directory to your local computer and Browse to select this file here.
If you are using a third-party SSL certificate, like GoDaddy, you need to provide the keystore file that you have generated.

If you are using a third-party SSL certificate, you must also provide information regarding the alias name you provided when generating the keystore file and the password for the keystore.

Checking the third party SSL keystore alias name and password

Ensure that the keystore alias name and the keystore file password are correct when using a third-party SSL certificate in your ServiceDesk Plus installation.

Determining the password required to access the keystore file

To determine the password required to access the keystore file, follow the steps given below:

1. Navigate to the **server.xml** file. The path is**<ServiceDesk_Home>\server\default\deploy\jbossweb-tomcat50.sar**
2. Determine the value of the parameter **keystorepass**

You have determined the password required to access the keystore file. You can use this password to determine the alias name of the keystore.

Determining the alias name of the keystore file

To determine the alias name of the keystore file, follow the steps given below:

1. Using the command prompt, navigate to **<ServiceDesk_Home>\jre\bin**
2. Execute **keytool -list -v -keystore <ServiceDesk_Home>\server\default\conf\sdp.keystore -storepass <ServiceDesk KeyStore File Password>**

You will find the alias name of the keystore file here.

Note : If you are using a PFX Certificate File, then Specify the "asc" as ServiceDesk Keystore Alias Name
See also: Integrating ServiceDesk Plus with Desktop Central, Deploying Software Applications, Sending HelpDesk Requests as Tickets

Logging Help Desk Requests as Tickets

Desktop Central enables you to contact their support team by logging help desk requests. This feature can be integrated with ServiceDesk Plus. Integrating this feature with ServiceDesk Plus enables you to log helpdesk-related requests in ServiceDesk Plus as tickets using Desktop Central.

You can also use predefined templates available in the Tickets tab to send requests. These templates comprise of predefined messages. You can modify the subject and content of these messages as required and send the tickets as requests using the tray icon of Desktop Central. You can also add tickets if required.

Benefits

The benefits include the following:

1. Submit requests without logging in
2. Send requests using predefined templates and can even attach screenshots automatically.
3. Use customizable subject lines to configure the HelpDesk application and enable automatic assignment of tickets
4. Configure settings in Desktop Central to log the following asset-related alerts as tickets in ServiceDesk Plus. These include alerts related to:

- Recently added hardware
- Commercial software applications that have recently been installed or uninstalled
- Prohibited software applications that have recently been installed
- Software compliance issues related to expired licenses or under licensed software applications

Prerequisites

Before you begin logging helpdesk-related requests as tickets or sending them using e-mail, you must ensure the following:

1. Ensure that the build numbers conform to the details given below:
2.

- Desktop Central: Professional Edition, Build number 70133 or later versions
- ServiceDesk Plus: Version 8.0 or later versions

3. Run both Desktop Central and ServiceDesk Plus in your network
4. Manage all the computers in your network using Desktop Central

Logging Help Desk Requests & Alerts as Tickets in ServiceDesk Plus

To log help desk requests and alerts from Desktop Central as tickets in ServiceDesk Plus, follow the steps given below:

1. Click the **Admin** tab
2. In the **Global Settings** section, click **ServiceDesk Plus Settings**
3. In the **ServiceDesk Plus Settings** section, check the **Enable ServiceDesk Plus Integration** checkbox
4. In the **Service Desk Server Plus Details** section, specify the following details about the ServiceDesk Plus Server:
    1.
        1. IP address/DNS name
        2. Port number
        3. Required communication protocol

5. In the **Features to Integrate** section, select Log Help Desk Requests as Tickets checkbox
6. Click **Save**

If you select HTTPS mode of communication, Select the Product Type : If you are using an standalone installation of ServiceDesk Plus product, select the ServiceDesk Plus option. If you wish to integrate with the ServiceDesk module within IT360 product, select IT360 option.

you must provide the SSL certificate of ServiceDesk Plus. copy the file **"sdp.keystore"** located in **<ServiceDesk Plus Installation Home>/server/default/conf** directory to your local computer and Browse to select this file here.
If you are using IT360 product with HTTPS communication enabled, copy the file **"it360.keystore"** located in **<IT360 Installation Home>/servicedesk/server/default/conf** directory to your local computer and Browse to select this file here.
If you are using a third-party SSL certificate, like GoDaddy, you need to provide the keystore file that you have generated.

/f you are using a third-party SSL certificate, you must also provide information regarding the alias name you provided when generating the keystore file and the password for the keystore.

Checking the third party SSL keystore alias name and password

Ensure that the keystore alias name and the keystore file password are correct when using a third-party SSL certificate in your ServiceDesk Plus installation.

Determining the password required to access the keystore file

To determine the password required to access the keystore file, follow the steps given below:

1. Navigate to the **server.xml** file. The path is**<ServiceDesk_Home>\server\default\deploy\jbossweb-tomcat50.sar**
2. Determine the value of the parameter **keystorepass**

You have determined the password required to access the keystore file. You can use this password to determine the alias name of the keystore.

Determining the alias name of the keystore file

To determine the alias name of the keystore file, follow the steps given below:

1. Using the command prompt, navigate to **<ServiceDesk_Home>\jre\bin**
2. Execute **keytool -list -v -keystore <ServiceDesk_Home>\server\default\conf\sdp.keystore -storepass <ServiceDesk KeyStore File Password>**

You will find the alias name of the keystore file here.

Note : If you are using a PFX Certificate File, then Specify the "asc" as ServiceDesk Keystore Alias Name

See also:

1. Integrating ServiceDesk Plus with Desktop Central,
2. Integrating Asset Data,
3. Deploying Software Applications

Deploying Software Applications

You can integrate the Software Deployment feature in Desktop Central with ServiceDesk Plus. This allows you to create or use existing packages in the Desktop Central server to deploy software applications. The ServiceDesk Plus server and the Desktop Central server are synchronized automatically.

Prerequisites

Before you integrate details about assets with ServiceDesk Plus, you must complete the following tasks:

1. Ensure that the build numbers conform to the details given below:
   - Desktop Central: Professional Edition, Build number 70133 or later versions
   - ServiceDesk Plus: Enterprise Edition, version number 8.0 or later versions
2. Run both Desktop Central and ServiceDesk Plus in your network
3. Manage all the computers in your network using Desktop Central

Enabling Software Deployment from ServiceDesk Plus

4. To enable software deployment from ServiceDesk Plus, follow the steps given below:
   - Click the **Admin** tab
   - In the **Global Settings** section, click **ServiceDesk Plus Settings**
   - In the **ServiceDesk Plus Settings** section, check the **Enable ServiceDesk Plus Integration** checkbox
   - In the **Service Desk Server Plus Details** section, specify the following details about the ServiceDesk Plus Server:
     - IP address/DNS name
     - Port number
     - Required communication protocol
   - In the **Features to Integrate** section, select Software Deployment checkbox
   - Generate and authentication key and provide it here.
   - Click **Save**

If you select HTTPS mode of communication, Select the Product Type :If you are using an standalone installation of ServiceDesk Plus product, select the ServiceDesk Plus option. If you wish to integrate with the ServiceDesk module within IT360 product, select IT360 option.

you must provide the SSL certificate of ServiceDesk Plus. copy the file **"sdp.keystore"** located in **<ServiceDesk Plus Installation Home>/server/default/conf** directory to your local computer and Browse to select this file here.
If you are using IT360 product with HTTPS communication enabled, copy the file

"it360.keystore" located in **<IT360 Installation Home>/servicedesk/server/default/conf** directory to your local computer and Browse to select this file here.
If you are using a third-party SSL certificate, like GoDaddy, you need to provide the keystore file that you have generated.

/f you are using a third-party SSL certificate, you must also provide information regarding the alias name you provided when generating the keystore file and the password for the keystore.

Checking the third party SSL keystore alias name and password

Ensure that the keystore alias name and the keystore file password are correct when using a third-party SSL certificate in your ServiceDesk Plus installation.

Determining the password required to access the keystore file

To determine the password required to access the keystore file, follow the steps given below:

1. Navigate to the **server.xml** file. The path is**<ServiceDesk_Home>\server\default\deploy\jbossweb-tomcat50.sar**
2. Determine the value of the parameter **keystorepass**

You have determined the password required to access the keystore file. You can use this password to determine the alias name of the keystore.

Determining the alias name of the keystore file

To determine the alias name of the keystore file, follow the steps given below:

1. Using the command prompt, navigate to **<ServiceDesk_Home>\jre\bin**
2. Execute **keytool -list -v -keystore <ServiceDesk_Home>\server\default\conf\sdp.keystore -storepass <ServiceDesk KeyStore File Password>**

You will find the alias name of the keystore file here.

Note : If you are using a PFX Certificate File, then Specify the "asc" as ServiceDesk Keystore Alias Name

1. **Configure Desktop Central Settings in ServiceDesk Plus:**
   - Click Admin --> Desktop Central Server Settings

- Specify the details of the Desktop Central installation like Server Name/IP, Port and the communication details.
- Click **Save**

2. Enable the option to display the install or uninstall software applications option in the Actions menu option in ServiceDesk Plus. You can enable this option in the **Service Catalog** in the Help Desk section in ServiceDesk Plus.

See also: Integrating ServiceDesk Plus with Desktop Central, Generating an Authentication Key

Complete UI Integration with ServiceDesk Plus

Desktop Central UI can be completely integrated with ServiceDesk Plus giving ServiceDesk Plus users complete access to desktop management functions.

Prerequisites

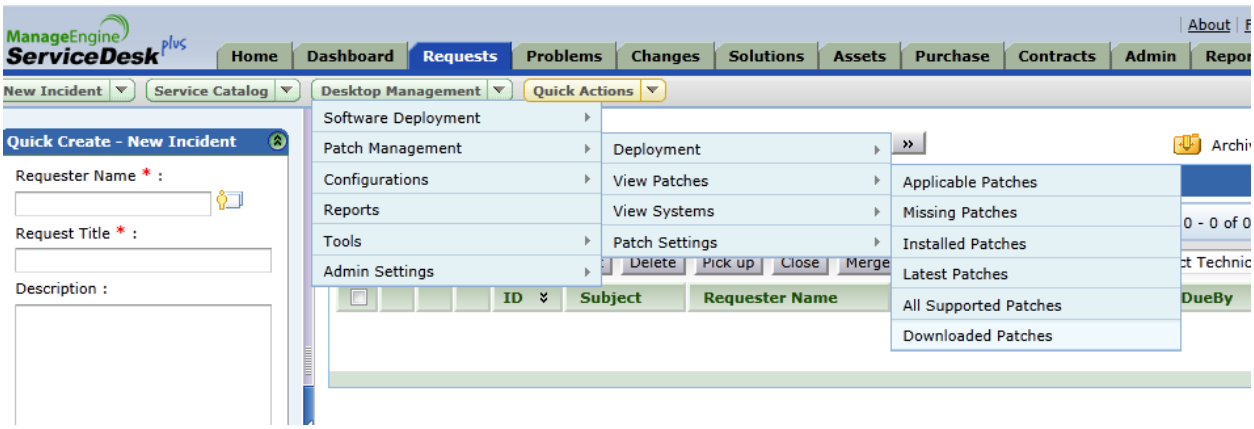
1. Ensure that the build numbers conform to the details given below:
2.
   - Desktop Central: Professional Edition, Build number 70242 or later versions
   - ServiceDesk Plus: Build Number 8017 or later versions
3. Run both Desktop Central and ServiceDesk Plus in your network
4. Manage all the computers in your network using Desktop Central

Steps to Integrate Desktop Central UI with ServiceDesk Plus

To integrate Desktop Central UI with ServiceDesk Plus, configure Desktop Central Server Settings in ServiceDesk Plus

1. Click Admin --> Desktop Central Server Settings
2. Specify the details of the Desktop Central installation like Server Name/IP, Port and the communication details.
3. Select the Enable Desktop Management Menu option.
4. Click **Save**

After configuring the Desktop Central Settings, ServiceDesk Plus users, will be able to see a Desktop Management Menu in the ServiceDesk Plus UI



Whenever a user is created in ServiceDesk Plus who has access to Desktop Management menu, the same user will get created in Desktop Central as well.

Enabling Desktop Management Menu for ServiceDesk Plus Users

Having integrated the UI of Desktop Central with ServiceDesk Plus, the next thing you do is to enable this menu for ServiceDesk Plus users. The Desktop Management menu, by default, will be visible to all users with administrative privileges in ServiceDesk Plus (Build #8020 and above). However, when you configure the Desktop Central Server settings, it will be visible only for whom the menu has been enabled.

To enable the Desktop Management menu for users, follow the steps below:

	You should login to ServiceDesk Plus as a user who has Administrator privileges in ServiceDesk Plus.

1. From the ServiceDesk Plus Web console, select Admin --> Technicians
2. Click the user to whom you should enable Desktop Management menu.
3. Under the Login Details of the user, select "Enable to access Desktop Management Functionality" option
4. Choose what privileges should the user have in Desktop Central:
    1. Admin privilege will have access to all the features
    2. Guest privilege will only have read-only access to Desktop Management functions.
5. Select the required privilege and click Save.
6. Repeat the above steps for every user to whom the Desktop Management menu has to be enabled.

	You cannot enable the Desktop Management menu for yourself. You should ask a fellow administrator to enable it for you.

Generating an Authentication Key

When you want to install or uninstall software applications and log help desk requests as tickets using ServiceDesk Plus, you are required to generate and enter an authentication key while integrating Desktop Central with ServiceDesk Plus. You must make the following settings to generate an authentication key:

- Create a role in ServiceDesk Plus with permission to do the following:
- Install or uninstall software applications using Desktop Central
- Log help desk requests
- Assign the role, you created, to a technician
- Generate an API key

Steps to generate an Authentication Key

To generate an authentication key, follow the steps given below:

1. Creating a role with required permission
    a. Login to the ServiceDesk Plus console
    b. Click the **Admin** tab
    c. In the **Users** section, click **Roles**
    d. Click **Add New Role**
    e. Enter the name of the role
    f. Enter a description about the role
    g. In the **Advance Permission** section, you have to enable required permissions
        a. To enable auto-ticketing, select the **Add** checkbox available under **Requests**.
        b. To enable Software Deployment, select the **Install/Uninstall Software** checkbox available under **Assets**
    h. Click **Save**
2. Assigning the role that was created to a technician and generating the Authentication Key
    a. Login to the ServiceDesk Plus console
    b. Click the **Admin** tab
    c. In the **Users** section, click **Technicians**
    d. Click **Add New Technician**
    e. Enter the following information about the technician:

    - Personal details
    - Contact information
    - Cost details
    - Department details

b. Assign the required groups for the technician

	The groups that you assign to the technician should have ticket-creation permission in ServiceDesk Plus.

c. Select the required permissions
d. Check the **Enable login for this technician** checkbox. Enter the following details for the technician:
   - Login name
   - Password
   - Domain name

e. Select **Enable Custom Privileges**
f. Assign the role you created
g. In the API key details section, click **Generate**
h. Enter the date on which you want the key to expire
i. Click **Generate**

	This key is entered when a technician key is required for Web service API requests.

j. Click **Save**

	You can also edit an existing technician's role and enable login.

4. Pasting the API key in Desktop Central
   a. Login to the Desktop Central server
   b. Click the **Admin** tab
   c. In the **Global Settings** section, click **ServiceDesk Plus Settings**
   d. In the **Authentication Details** section, enter the API key you generated in the ServiceDesk Plus console
   e. Click **Save**

You have generated the API key using the ServiceDesk Plus console and entered it in the ServiceDesk Plus settings in the Desktop Central server.

See also:

Sending HelpDesk Requests
Deploying Software Applications

Managing Custom Scripts

Custom script files are used to configure the software settings, trigger events, etc in the computer of a network. The custom script files can be batch (.bat), command (.cmd), Windows Script Host (WSH) files. The WSH files includes the VBScript (.vbs), Java Script (.js), Perl (.php), REXX, and Python files.

The important custom Script files can be stored in Inventory so that they can be used in future. The custom scripts used in the Custom Script configuration are automatically added to the inventory. The custom scripts available in the inventory can also be used while adding the **Custom Script** Configuration.

Adding the Script Details

To add the script details to Desktop Central, follow these steps:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Script Repository** link in the **Admin Links** pane. This invokes the **Script Repository** page.
3. Click the **Add Script** button to invoke the **Add Script** page.
4. Select the script from local disk of the computer or from the shared network location using one of the following options. This field is mandatory.
5. Click **Browse** to select the script either from the local machine or from the network based on your choice above.
6. Enter the description for the script in the **Description** field.
7. Enter the arguments for the script in the **Script Arguments** field.
8. Click the **Add** button. You can find the script added to the table in the **Script Details** page.
9. Repeat steps 3 to 8 for adding more scripts.

Modifying the Script Details

To modify the Script details, follow these steps:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Script Repository** link in the **Admin Links** pane. This invokes the **Script Repository** page.
3. Click the icon under the **Actions** column next to corresponding **Script Name**.
4. Follow the step 4 to step 6 of the Adding the Script Details procedure.
5. Click the **Modify** button.

Removing the Script Details

To remove the Script details, follow these steps:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Script Repository** link in the **Admin Links** pane. The **Script Repository** page is invoked.
3. Click the icon under the **Actions** column next to corresponding Script name. Click **OK** to confirm deletion.

The script will be removed from the **Script Repository** table.

Configuring Server Settings

Server settings like, Web server port, logging level, and other properties can be configured from here. These settings are common to all the users using Desktop Central and not user-specific.

To configure the server settings, select the **Admin tab --> Server Settings** link.

To configure server settings

1. Select the "Start 'Desktop Central' automatically on machine bootup" check box if you wish to start Desktop Central whenever the system is started.
2. Select the "Launch the client upon successful server startup" check box if you wish to open the client whenever the Desktop Central Server is started.
3. Select the "Enable Secure Login (Https)" option to enable https in the client.
4. Click the **Save Changes** button.

To change the log level

1. Select the log level from the **Current Log Level** combo box.
2. Click **Save Changes** button.

Creating Custom Groups

Desktop Central provides an option to create custom group of computers and users, which can be used to as targets for applying the configurations. The advantages of custom groups are:

1. You can have any number of custom groups to group computers and users of a specific department. You can create this once and can use these groups as targets for deploying the configurations.
2. You can add or remove users/computers from groups at any point of time.
3. Groups once created can be used in any number of configurations.

To create a custom group, follow the steps below:

1. Select the **Admin** tab
2. Click the **Custom Groups** link available under the Global Settings. This will list all the Custom Groups that have been created.
3. Click the **Create New Group** button and specify the following values:
    1. Specify a name for the custom group. This should be unique.
    2. Select the Domain or the Workgroup from the list.
    3. Select the **Group Type** as Computers or Users. This will list the available computers/users in the selected domain.

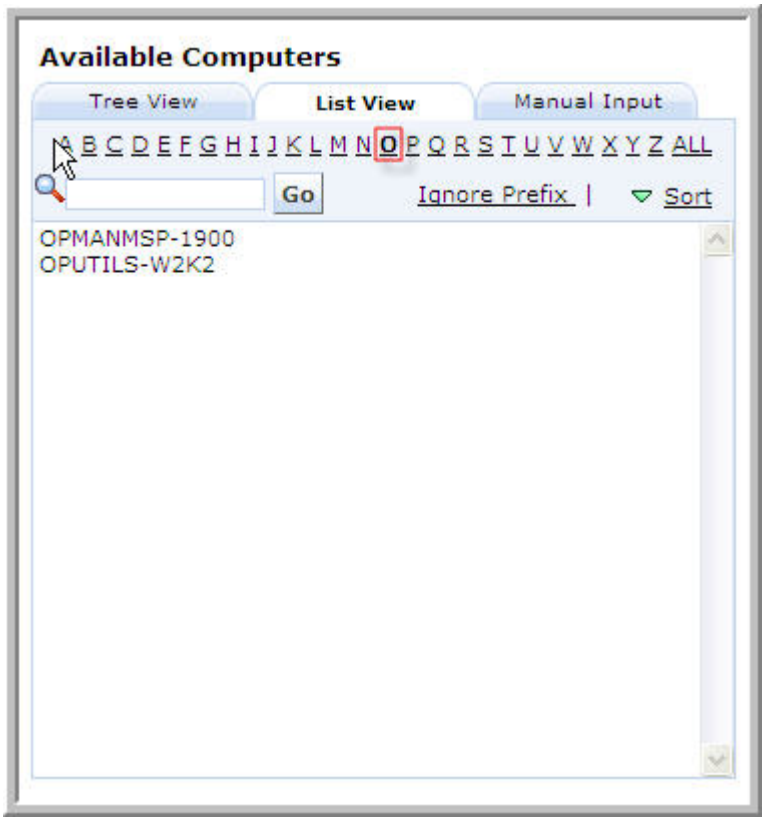
       Tip: By default, the users/computers will get displayed in Tree View. Use List View link to view users/computers as a list. Manual entry of computers/users is possible using Manual Input option.

    4. Select the computers/users and move them to the Added list.
4. Click **Submit** to create the group.
    1. Repeat step 3 & 4 for creating more groups.

List View

1. Click on the **List View** link for the users/computers to be displayed as a list.
2. Click on a particular alphabet to view the users/computers with names that begin with alphabet specified. Use **All** link to list all the users/computers.
3. Click on the **Sort link** to sort the listed user/computer names.

Tip: You can use the "**Ignore-Prefix**" option in combination with your choice of alphabet. This will list all users/computers that have the specified prefix and whose names begin with selected alphabet. For example, the figure belows shows a case where **DC** is specified in Ignore-Prefix and the alphabet chosen is **W**. The resultant list therefore shows all the computers who have '**DC**' as their prefix but whose names begin with alphabet '**W**'.



Manual Input Option

1. Click on the **Manual Input tab** for the users/computers to be manually added.
2. Specify a valid User/Computer in the text field.
3. Click on **>>** button to add the user/computer in the custom group.

	Note: Incorrect User/Computer will not be added and the application will throw an error. In that case, specify the correct User/Computer name and add it again.

4. Click on **Create Group** button to complete custom group creation.

Configuring Deployment Templates

When you deploy a software or a patch using Desktop Central, you can specify multiple Deployment Settings like when to install, whether the user can skip deployments, reboot policies, etc. These deployment settings can be created as a template, which can then be used while defining the configuration. There are several ways to create a deployment template:

- While defining a configuration using the "**Save as Template**" link by providing a name for the template
- Create templates manually from Deployment Template page. You can reach the Deployment Template page from the following places:
- Admin --> Deployment Templates
- Patch Mgmt --> Deployment Templates
- Software Deployment --> Deployment Templates

Follow the steps below to create a template manually:

1. Navigate to the **Deployment Template** page from the Desktop Central client
2. Click **Create Template**
3. Specify a name for the template
4. Choose the required Install Option:
    1. Install during computer startup: Select this option if the patches have to be deployed during computer startup.
    2. Install during 90 minutes refresh interval: Select this option if the patches have to be installed after the computer startup when the next update happens (within 90 minutes)
    3. Either of the above, whichever is earlier
5. If you want the installation to happen only between a specified time of a day, you can specify the Start and End time within which the deployment should begin. The Start Time can also be greater than the End time - in such cases the End time is assumed to be on the following day. For example, if you wish the deployment should happen between 10.00 PM and 4.00 AM, you can specify the Start Time as 22:00:00 and End Time as 04:00:00
6. Specify whether the use can skip the deployment at a later time by selecting the "Allow Users to Skip Deployment". When you do not select this option, the deployment will be forced and the user will not have any control on the deployment.
7. If the deployment progress has to be shown to the users, select "Show deployment progress in the client computers" option.
8. Select the required Reboot Policy:
    1. Do not reboot: Select this option if the client computers should not be rebooted after installing the patches.
    2. Force Reboot when the user has logged in: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines.

3. Force Shutdown when the user has logged in: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines.
4. Allow user to skip Reboot: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines.
5. Allow user to skip Shutdown:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

9. Click **Save** to save the template

The templates thus created can be used to pre-fill the Deployment Settings while you define a Software and Patch Configurations by choosing the required template from the list. You can also change any specific settings after loading the data from the template (and also can save it as a new template using the Save as Template link)

	**Note:** When you define the Software or Patch configuration, you will also have an additional option under "Allow Users to Skip Deployment" as to whether they can skip it as long as they wish or the installation should be forced beyond a specific date. When you specify a date and save it as a Template, this date is not saved on the template.

Configuring Remote Access to the Database in Desktop Central

Desktop Central stores all the information in a database. For example, it comprises information about computers, software applications that are installed, hardware that is installed and details about patches.

You can access this database remotely to get certain information. For example, assume that you require information from the database to help you to generate specific reports that are not readily available and cannot be generated using the Custom Reports feature. You can access the database used by Desktop Central to get this information.

The database is located in the Desktop Central server. You can access this database remotely. However, not everyone has permission to access the database. Only administrators can grant access to computers to connect to the database remotely.

When you are granted permission you can only read the information that is available in the database.

Granting or Revoking Access

This section applies only to administrators.

As an administrator, you may grant or revoke access for computers to access the database, in Desktop Central, remotely. You should grant Read-only access. The user should not be given permission to make changes to the database.

This access may be granted only to allow a user to gather information required to create reports that are not readily available and cannot be created using the Custom Reports feature.

It is highly recommended that you check the usage status periodically and revoke the access to the database from users who:

- Do not require to access the database
- Have access to the database but are not using it

Steps

To grant or revoke remote access to the database in the Desktop Central server, follow the steps given below:

1. Click the **Admin** tab
2. In the **Global Settings** section, click **Remote DB Access**
3. In the **Remote Computer Name** field, enter the name of the computer to which you want to grant remote access

If the computer, from which a user is accessing the database remotely, is in a domain that is different from that of the database, specify the computer name along with its DNS suffix. For example, john.desktopcentral.com

4. In the **Access Type** section, select **Grant** or **Revoke**, as required
5. Click **Save**

You have granted or revoked remote access to the database in the Desktop Central server.

Connecting Remotely to the Database

You can use any ODBC tool like sqlyog to connect remotely to the database in the Desktop Central server. Ensure that the computer from which you are trying to establish a remote connection has been granted access before you try to connect to the database

Checking for Computers With Access

To view the list of the computers which have been granted access to connect remotely to the database in the Desktop Central server, follow the steps given below:

1. Click the **Admin** tab
2. In the **Global Settings** section, click **Remote DB Access**
3. Click the **Computers that have been granted remote access** link

You can now see a list of computers which have been granted access by the administrator to connect remotely to the database in the Desktop Central server.

Details Required to Connect Remotely

You require the following details to connect remotely to the database in the Desktop Central server:

- Mysql Host Address: This refers to the name of the computer where the database server is running. Unless the database server is running in another computer, the

host address will be the same as that of the computer where the Desktop Central server is installed and running.

- Username: This refers to the username that you are required to enter to connect remotely to the database. The username to connect to the database is **root**.
- Password: You do not have to enter a password.
- Port: This refers to the port number that is required to connect to the database. By default, the port number is **23306**. If you have changed the number of the port, specify it before trying to establish the connection to the database.
- Database(s): This refers to the name of the database that you want to connect to remotely. You should enter **desktopcentral** in this field.

Personalizing the Client

Desktop Central provides users with the functionality to configure user accounts based on personal priorities and requirements. The settings option enables you to change an existing password, set the session time, select a theme etc.

These settings are user-specific and each user can have their own settings.

To personalize, select the **Admin tab --> Personalize** link.

To change the **password**

1. Enter the existing password in the **Old Password** field.
2. Enter the new password in the **New Password** field.
3. Enter the new password again for confirmation in the **Confirm Password** field.
4. Click the **Save Changes** button.

The new password get updated. Subsequently, you have to use the new password to login to the client.

To set the session **time**

1. Select the session expiry time in hours from the **Session Expiry Time** combo box to the desired value.
2. Click the **Save Changes** button.

The session expiry time gets updated.

To set the page **refresh** time

1. Specify the time in minutes at which the pages should get refreshed automatically.
2. Click **Save Changes** button.

To configure general settings

1. Select the "Show help card after deploying the configuration" check box if you wish to view the help card after successful deployment of configurations.
2. Select the "Show help card throughout the product" option if you wish to view the help card where ever applicable.
3. Select the "Save view settings" to retain the view per page settings in the reports.
4. Click the **Save Changes** button.

To change the **theme**

1. Select the theme from the available options
2. Click **Save Changes** button.

Authenticating Users via Active Directory

Desktop Central Web Console is the management interface for performing various activities like installing patches, installing/uninstalling software, imposing security restrictions and much more. If an unauthorized person or a hacker gets access to this interface, it allows them to perform some undesirable actions to the extent of taking control of remote computers/servers. While it is possible to restrict users based on specific roles, it does not have any stringent password plocies in place to make users change their passwords more frequently.

If you have an Active Directory based Windows Domain setup, you can make use of the Active Directory's password policy work for you. You can set stringent password policy for your domain users and make them login to Desktop Central using their domain username and password.

Making users authenticated via Active Directory is very simple. You just have to add your domain and specify a domain user. The user will have to use their domain Logon name and Password to login to Desktop Central.

Note: The user should have privileges to login to the domain from the computer where Desktop Central Server is installed.

Migrating Desktop Central Server

Migrating Desktop Central refers to moving the existing installation from one computer to another without losing the data and configuration. There may be may situations where you would need to migrate, like:

- You have been evaluating the product in some test computer and you would like to move this to a dedicated computer or server after you have decided to purchase it.
- The disk space is running low and you wish to move this to a different computer.
- You are upgrading the hardware.

The following are the sequence of operations that have to be performed when migrating Desktop Central Server:

1. Copy the installation directory from the existing installation to the new set up
2. Register the Service in the new set up
3. Change the IP Address and DNS name of the Server in all the agents. This is not required if there is no change in IP Address and DNS name.
4. If you are running database server separately, you should configure it to accept connections from the new IP Address.

For step 3 above, you will provide the details of the new installation in the user interface here. For a step-by-step instructions on migrating the installation, refer to this How To document in our website.

Do's

1. It is recommended that you provide the details of the new server in the user interface after you have started the server in the new installation. This is to ensure that agents will be able to contact the new server after picking up the information.
2. You should be running the Desktop Central Server in both the installations till all the agents start reporting to the new server
3. The database server, if running remotely, should be configured to accept connections from the new IP Address.

Dont's

1. You should not download and install the latest executable from our website and just replace the database files. You should copy the entire installation from the old and move it to new.
2. You should not provide the details of the new server in the user interface, if you have not copied the installation and started. This is because that the agents will not be communicating with the server at the old installation once it picks up this

information. If you do not have the Desktop Central server running at the IP Address specified here, the computers cannot be managed.

User & Role Management

Overview

As an administrator, many a time you would have felt mundane routines spill over crucial attention-seeking jobs of your network. Desktop Central answers this concern through its User & Role Management module; delegating routine activities to chosen users with well-defined permission levels. You can easily administer these users that need access to Desktop Central Product web client.

1. Role Management

Some of the most commonly used Roles are specified under Pre-defined Roles. However, you also have the flexibility to define roles that best suit your requirements under the User-defined Roles and grant appropriate permissions. Here's a brief on the Pre-defined and User-defined roles respectively:

User-defined Role

You can tailor-make any number of roles using Desktop Central and give them permissions of your choice based on your personalized needs. These customized roles fall under the User-defined category. For a better understanding let us quickly see how to create a User-defined Role in the following section.

Defining a new Role

Follow the steps mentioned below to create a new User-defined role:

1. Select the Admin tab and click on User Administration. This opens the User Administration page.
2. Select the Role tab and click the Add Role button.
3. Specify the Role Name and a small description about it in the Define Role Section.
4. You can define module-wise permission level for the Role in the Select Control Section. The permission levels are broadly classified into:

Full Control - To perform all operations akin to Administrator role, for the specific module
Read Only - To only view the details in that module
No Access - To hide the module from the User

5. Click on Add button.

	**Note:** The role you have just created will now be available in the Roles list of the user creation module. Role deletion cannot be performed if that role is associated even with a single User. However you can modify the permission levels for all User-defined roles.

Pre-defined Roles

You will find five roles in the Pre-defined category and these include:

1. Administrator
2. Guest
3. Technician
4. Auditor
5. Remote Desktop Viewer
6. IT Asset Manager
7. Patch Manager

Administrator Role: The Administrator role signifies the Super Admin who exercises full control, on all modules. The operations that are listed under the Admin tab include:

1. Defining or modifying Scope of Management
2. Adding Inactive Users
3. Changing mail server settings
4. Changing proxy settings
5. Personalizing options like changing themes, setting session expiry, etc.
6. Scheduling vulnerability database update
7. Scheduling scan settings for Patch Management
8. Editing MSI or Script repository
9. Viewing Actions Logs of Desktop Central

Guest Role: The Guest Role retains the Read Only permission to all modules. A user who is associated to the Guest Role will have the privileges to scan and view various information about different modules, although making changes is strictly prohibited.

Technician Role: The Technician Role has a well defined set of permissions to do specific operations. Users under the Technician role are restricted from performing all the operations listed under the Admin tab. The operations that can be performed by users associated with the Technician Role include:

1. Can define and deploy all types of configurations and collections.
2. Can view all the configurations including those created by other users, reports, etc.
3. Can suspend, modify, or re-deploy the configurations defined by them.
4. Can update the Vulnerability Database.
5. Can perform Scan operations on all modules.

Auditor: The Auditor role is specially crafted for Auditing Purposes. This role will help you grant permissions to auditors view the details of software inventory, check for license compliance, etc.

Remote Desktop Viewer: The Remote Desktop Viewer Role will allow the users associated with it to Invoke a Remote desktop connection and view details of users who had connected to a particular system.

IT Asset Manager: The IT Asset Manager has complete access to the Asset Management module and all the other features are inaccessible.

Patch Manager: The Patch Manager role has complete access to the Patch Management module and all the other modules/features are inaccessible.

Privilege Guideline

Action	Read Permission	Write Permission
Configuration		
Create Configuration	✗	✓**
Patch Mgmt.		
Decline Patches	✗	✓
Automate Patch Deployment	✗	✓
System Health Policy	✗	✓
Install Patch / Service Pack	✗	✓
On Demand Scanning	✓	✓
Software Deployment		
Add Package	✗	✓
Network Share	✗	✓
Install / Uninstall Software for Users / Computers	✗	✓

Action	Read Permission	Write Permission
Inventory		
Group Software	✗	✓
Manage Licenses	✗	✓
Configure Prohibited Software	✗	✓
Configure E-Mail Alerts	✗	✓
On Demand Scanning	✓	✓
Tools		
Add System Tools Task	✗	✓
Schedule Wake on LAN	✗	✓
Immediate Remote Shutdown	✗	✓
Schedule Remote Shutdown	✗	✓
Remote Control		
Edit Settings	✗	✓
Remote Desktop Sharing	✗	✓
Reports		
Enable User Logon Reports Settings	✗	✓
AD Report - On Demand Synchronization	✗	✓

** **Exceptions**:

1. Install Patch / Service Pack Configurations can be defined only if Patch Write permissions are available for both Configuration and Patch modules.
2. Install / Uninstall Software Configurations can be defined only if Write Permissions are available for both Configuration and Software Deployment modules.

2. User Management

Creating a User and Associating a Role

You can associate a User with a Role while creating a New User. To create a user follow the steps mentioned below:

1. Login to Desktop Central client as an Administrator
2. Click the User Management link available under the Global Settings category.
3. This will list all the users that have been created. By default, it has admin and guest users in Administrator and Technician roles respectively.
4. Click the Create New User link.
5. You have two modes of authenticating users into Desktop Central: From Active Directory or Locally.
    1. When you choose to authenticate a user via Active Directory, you should select the domain and specify a user of that domain and their role. These users should use their domain Logon Name and Password to login to Desktop Central Client.
    2. When you choose the local authentication, specify the User Name, Password, and Role
6. Optionally, you can also specify the Email Address and Phone Number of the user.
7. When you have specified the required details, click Create User.
8. The created user gets added to the User table.

Note: When you opt to authenticate a user via Active Directory, the user should have privileges to login to the domain from the computer where Desktop Central Server is installed.

Modifying User details

Desktop Central offers the flexibility to modify the role of users, to best suit your changing requirements. You can do operations like Changing the User Role and Reset User Password at point of time you feel you should.

Deleting a User

At times when you find a user's contribution obsolete, you can go ahead and delete the user from the User List. The user so removed will no more exercise Module Permissions.

Setting Up Software Deployment

The Software Deployment feature in Desktop Central enables you to deploy software remotely as well as distribute software applications to users and computers in a Windows network. The settings that you must make to use this feature are as follows:

- Configure a software repository for a network share
- Configure a software repository for an HTTP upload
- Add and deploy software packages

Configuring Software Repositories

A software repository is a storage location where you can store software packages. You can access these software packages when required and install them on computers in your network. In Desktop Central, there are two types of software repositories:

- Network-share repository
- HTTP repository

Network-share Repository

A network-share repository is used when you want to deploy a software application to multiple computers in a network. It is recommended that you store the software package that you want to deploy in a network share that is accessible from all the computers in the network. The software application will be installed directly in the computers that you specify.

Most software applications have a single installation file like <setup>.exe or the <softwarename>.exe. Other applications have more than one installable file, however, these files are located in the same directory. Some complex applications, like Microsoft Office, have multiple installable files. Here each installable file is located in a different directory. It is recommended that you deploy such applications from a network share that is accessible from all the computers in your network.

Advantages

Using a network-share repository enables you to do the following:

- Ensure that you do not have multiple copies of the same software application in your network
- Fill the details of your network-share repository automatically whenever you add a package
- Save your network bandwidth as executable files are not copied into the computers

Required Permissions

The network-share repository should have the **Read** and **Execute** permission for all the users and computers in the network. You should set the permissions mentioned above for the group **Everyone**. This ensures that the network-share repository is accessible from all the computers in the network.

However, ensure that you do not set the permissions to Read and Execute for all the users and computers in the network when you want to do the following:

- Restrict certain users from accessing the network-share repository directly
- Deploy a software application to users or computers across multiple domains or workgroups.

  For example, assume that your network-share repository is in domain A and you deploy a software application from this repository to a computer in domain B. You should ensure that you do not set the permissions to Read and Execute for all the users and computers in the network.

  In such cases, you can provide user credentials that have the Read and Execute access to the network-share repository in which the software package is stored. Desktop Central will use these credentials to access the repository and deploy the software.

Creating a Network-share Repository

To create a network-share repository, follow the steps given below:

1. Click the **Software Deployment** tab
2. In the **Settings** section, click **Software Repository**
3. Click the **Create a Network Share** option
4. Enter the path for the network share

	If you do not enter a path for the network share, it will automatically be created in the computer where Desktop Central server is installed.

5. Check the **Accessing the Share using Credentials** checkbox
6. Enter a username and password

	If you are creating the network share on a domain computer, prefix the domain name to the username. For example, ZohoCorp\Administrator. If you are creating the network share on a workgroup computer, prefix the computer name to the username. For example, <machinename>\DCAdmin.

7. Click **Save**

You have created a network-share repository.

HTTP Repository

An HTTP repository is used to store executable files before you install them in computers in your network. You can use this repository when you want to deploy software packages to

computers using the HTTP path. You can also change the location of the HTTP repository if required.

The HTTP repository is created automatically when you install Desktop Central. It is located in the same folder as the Desktop Central server. For example, <Desktop Central server>\webapps\DesktopCentral\swrepository. You can change the location of the repository if required.

Advantages

Using an HTTP repository enables you to do the following:

- Install software applications in computers that do not have access to a network-share repository
- Access computers when the computers are unable to access a network-share repository because the required number of connections have been reached
- Do not have to set any permissions when using an HTTP repository

Changing the Location of the HTTP Repository

To change the location of the HTTP repository, follow the steps given below:

1. Click the **Software Deployment** tab
2. In the **Settings** section, click **Software Repository**
3. Click the **HTTP Repository** tab
4. Enter the path of the new location
5. Click **Save**

You have changed the location of the HTTP repository. If you are unable to change the location of the HTTP repository, see Cannot Change the Location of the HTTP Repository

Network Share VS. HTTP Upload

While it is recommended that you have a common software repository, it is not mandatory. You also have an option to upload the executable files in the Desktop Central server from where they are copied into the computers before being deployed. Using this approach will increase your bandwidth overhead as the executable files are copied into each of the computers.

Therefore, it is recommended that you use this approach when you are deploying software applications to computers in a remote location. This is because, in most cases, when you deploy software applications to computers in remote locations you do not have access to the respective network-share repository.

When you want to deploy software packages to computers in a LAN and WAN, create two packages for the same software application. Store one set of packages in the network-share repository. These will be deployed and installed in the computers in the LAN. Store the other

set of packages in the HTTP repository. These will be uploaded and deployed to the computers in the WAN.

When you want to install multiple packages you can zip them and upload. For more information, see How to use the HTTP Path option to deploy software packages that have multiple executable files in different directory structures?

There are a few exceptional scenarios where executable files are copied to computers in your network when using network-share repository. This can happen when you do the following:

- Choose the **Copy Files / Folders** option while defining a configuration to install software applications
- Are required to use user credentials to access the network-share repository
- Use the **Run As** option while installing software packages as a user, other than the administrator

Managing Software Packages

Desktop Central enables you store the commonly used applications, which can be installed on to the client machines as required. The common applications, which includes both MSI and EXE files, are stored under the Software Packages Repository.

The software packages that are added to the repository can then be used while defining the Software Installation Configuration.

Adding MSI/EXE Packages

Desktop Central allows you to add separate packages for MSI and EXE based software applications:

1. Adding an MSI Package
2. Adding an EXE Package

Adding an MSI Package

1. Click the Software Deployment tab. This invokes the **Software Package Repository** page listing the details of the packages that have been added.
2. Click the **Add Package** button.
3. Select the Package type as **MSI** and specify the following details:

Parameter	Description
Package	
Package Name	Name of the Software Package
Select the path type	Select any of the following: 1. Network Path: If the software has to be installed in computers in the same LAN, select this option 2. HTTP Path: If the software has to be installed in

Parameter	Description
	computers in branch offices over the VPN tunnel or internet, select this option
Add Files to Upload	When you select the HTTP Mode, you need to browse and select the installables, which will be uploaded to the Desktop Central Server
MSI File Name with network path	When you select the Network Path option, specify the name of the MSI file with its complete network path. This path should have all the related files and should have necessary read & execute permissions. Example: \\MyServer\MSIApps\Skype\skype.msi.
Advanced Options (optional)	
Installer / Uninstaller Settings	
MSI Root Path	When you choose to copy the installables to individual computers before installing the software, you need to specify the directory to be copied.
MST file name with Network path	For applications that supports customizations prior to installation, you can customize the installation and specify it here. For example, you can customize the MS Office 2003 installation by specifying the license keys, choosing the components to install, etc., using the Microsoft Office Resource Kit Tools. After customization an .MST file gets created. The MST file should also be placed in the network share where all the other installation files are present. Specify the location of the MST file with the network path here. If you are using the copy option while deploying the application, the location of the MST file specified here should be relative to the MSI Root Path. If the MSI Root Path is displayed as \\MyServer\Shares\MSIApps and your MST File is in \\MyServer\Shares\MSIApps\Office2003\Custom.mst,

Parameter	Description
	specify the location as Office2003\Custom.mst. Multiple mst files can be specified as semi-colon separated. Please note that the relative path is required only if you choose to copy the files to the individual computers before installing the software. Else, you can specify the complete network path.
Install Arguments to MSI	Application specific installation parameters can be specified here. For example, for skype, you can specify parameters like installlevel=10. This field can be left blank, if you do not have any application specific arguments.
Uninstall Arguments to MSI	Application specific installation parameters can be specified here. For example, REBOOT=ReallySuppress
Enable Logging for troubleshooting	Select this option to enhance the logging to troubleshooting the deployment errors.
Disable Uninstall option in Add/Remove Programs	Select this option, if you do not want the users to remove the software from Add/Remove Programs.
Package Properties	
Manufacturer	Name of the software vendor
Version	The software version
Language	The software language version
Package Description	Description of the software package
Run Script before Installing Software	
Script / Command Name	Specify the commands or scripts that has to be executed before installing the software. Refer to Executing Scripts in Software installation for more details.
Arguments	Specify the arguments for the pre-installation script, if any
Continue installation if the	Select this option and specify the exit code to check for successful pre-installation process before proceeding

Parameter	Description
exit code is	with the software installation. If the pre-installation fails, the installation will abort.
Run Script after Installing Software	
Script / Command Name	Specify the commands or scripts that has to be executed after installing the software. Refer to Executing Scripts in Software installation for more details.
Arguments	Specify the arguments for the post-installation script, if any.
Successful if the Exit Code is	Select this option and specify the exit code to verify whether post installation has been successful. If post-installation is not successful, the software will not be uninstalled.
Run Script before Uninstalling Software	
Script / Command Name	Specify the commands or scripts that has to be executed before uninstalling the software. Refer to Executing Scripts in Software installation for more details.
Arguments	Specify the arguments for the pre-uninstallation script, if any
Continue uninstallation if the exit code is	Select this option and specify the exit code to check for successful pre-uninstallation process before uninstalling of the software. If the pre-installation fails, the uninstallation will abort.
Run Script after Uninstalling Software	
Script / Command Name	Specify the commands or scripts that has to be executed after uninstalling the software. Refer to Executing Scripts in Software installation for more details.
Arguments	Specify the arguments for the post-uninstallation script, if any.
Successful if the Exit Code is	Select this option and specify the exit code to verify whether post uninstallation has been successful. If post-installation is not successful, the software will not be re-installed.

3. Click **Add Package**. The package gets added to the table below.
4. Repeat steps 3 to 5 for adding more packages.

Adding an MSIEXEC/EXE/ISS/Command Package

1. Click the Software Deployment tab. This invokes the **Software Package Repository** page listing the details of the packages that have been added.
2. Click the **Add Package** button.
3. Select the Package type as **MSIEXEC /EXE/ISS/Command** and specify the following details:

Parameter	Description
Package	
Software Name	Name of the Software Application. Click on the *Select from Pre-Defined Application* link. This opens the *Select Application* dialog. You can make your selection from the pre-defined packages that are listed. Alternatively, you can also select from the prompted list, while typing the application name in the text field.
Select the path type	Select any of the following: 1. *Network Path*: If the software has to be installed in computers in the same LAN, select this option 2. *HTTP Path*: If the software has to be installed in computers in branch offices over the VPN tunnel or internet, select this option
Add Files to Upload	When you select the HTTP Mode, you need to browse and select the installables, which will be uploaded to the Desktop Central Server
Installation Command with switches/arguments	Specify the command to be executed in the client computers for installing the application. The command specified here will be "as such" executed in all the client computers. Make sure that the path to the executables specified in the command is relative to the EXE Root Directory specified above. Examples: 1. msiexec.exe \Skype\skype.msi /qn 2. googlesetup.exe /S

Parameter	Description
Uninstallation Command with switches/arguments	Specify the command to be executed in the client computers for uninstalling the application. The command specified here will be "as such" executed in all the client computers. Make sure that the path to the executables specified in the command is relative to the EXE Root Directory specified above. Example:Skype\uninstall.exe If the uninstaller in the individual computers has to be invoked, you can specify the complete path to the uninstaller. please note that the uninstaller has to be in the same location in all the client computers. You can use environment variables in the path. Examples: C:\WINDOWS\ie7\spuninst\spuninst.exe /q %SystemRoot%\ie7\spuninst\spuninst.exe /q
Advanced Options (optional)	
Installer / Uninstaller Settings	
EXE Root Path	When you select the Network Path option, specify the shared directory from where all the commands will be executed. This directory should have access to all the executables that are required to install the application.
Package Properties	
Manufacturer	Name of the software vendor
Version	The software version
Language	The software language version
Package Description	Description of the software package
Run Script before Installing the Software	
Script / Command Name	Specify the commands or scripts that has to be executed before installing the software. Refer to Executing Scripts in Software installation for more details.

Parameter	Description
Arguments	Specify the arguments for the script, if any
Continue installation if the exit code is	Select this option and specify the exit code to check for successful pre-installation process before proceeding with the software installation. If the pre-installation fails, the installation will abort.
Run Script after Installing the Software	
Script / Command Name	Specify the commands or scripts that has to be executed after installing the software. Refer to Executing Scripts in Software installation for more details.
Arguments	Specify the arguments for the script, if any
Successful if the Exit Code is	Select this option and specify the exit code to verify whether post installation has been successful. If post-installation is not successful, the software will not be uninstalled.
Run Script before Uninstalling the Software	
Script / Command Name	Specify the commands or scripts that has to be executed before uninstalling the software. Refer to Executing Scripts in Software installation for more details.
Arguments	Specify the arguments for the script, if any
Continue uninstallation if the exit code is	Select this option and specify the exit code to check for successful pre-uninstallation process before uninstalling of the software. If the pre-installation fails, the uninstallation will abort.
Run Script after Uninstalling the Software	
Script / Command Name	Specify the commands or scripts that has to be executed after uninstalling the software. Refer to Executing Scripts in Software installation for more details.
Arguments	Specify the arguments for the script, if any
Successful if the Exit Code is	Select this option and specify the exit code to verify whether post uninstallation has been successful. If post-installation is not successful, the software will not be re-installed.

3. Click **Add Package**. The package gets added to the table below.
4. Repeat steps 3 to 5 for adding more packages.

Executing Scripts in Software Installation

Desktop Central allows you to execute scripts in the following cases:

1. Prior to installing the software
2. After installing the software
3. Prior to uninstalling the software
4. After uninstalling the software.

The following needs to be ensured while you specify a script to be executed in any of the above cases:

1. The scripting engine should also be specified in the Script/Command field. For example, if you are specifying a vb script, say test.vbs, you should specify like this: *%SystemDrive%\Windows\cscript \\dc-win2k1\scripts\test.vbs*. In this case the cscript should be in the same location in all the client computers. Alternatively, you can also specify the engine path in a network share like: *\\dc-win2k1\Windows\cscript \\dc-win2k1\scripts\test.vbs*
2. When you select the Copy option while defining the Install Software Configuration, the following needs to be taken care:
    1. When selecting *None*: the script file should be in the network share.
    2. When selecting *Copy file to client machines*: the script should be in the network share.
    3. When selecting *Copy folder to client machines*: The script should be in the same directory or sub-directory as that of the installation file and the path specified should be relative path from that directory.
3. When using absolute path, use the environment variables instead of specifying the path directly. For example, for c: use %SystemDrive%.

Modifying MSI/EXE Packages

To modify the MSI/EXE packages, follow these steps:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Software Repository** link in the **Admin Links** pane.
3. Click the icon under the **Actions** column next to corresponding package.
4. Follow the step 4 and step 5 of the Adding MSI/EXE Packages procedure.
5. Click the **Modify Package** button.

Removing MSI/EXE Packages

To remove the MSI/EXE packages, follow these steps:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Software Repository** link in the **Admin Links** pane.
3. Click the icon under the **Actions** column next to corresponding package. Click OK to confirm deletion.

The package details will be deleted from the table.

Software Deployment Templates

A template is a predefined format that can be applied. The Templates tab in the Software Deployment section comprises of predefined applications that you can use to create packages automatically. This functionality downloads binaries from the respective vendors' Web sites to create packages automatically.

Prerequisites

Ensure that you complete the following tasks before automating the package-creation process using the Templates tab:

- Define valid proxy credentials
- Provide access rights

Creating a package

You can create a single package or multiple packages from the Templates tab. To create a package, follow the steps given below:

1. Click **Software Deployment>Templates**
2. Select the required application

Note: Select multiple applications to create multiple packages.

3. Click the **Create Package** button

Note: You can also use the **Create Package** link available against the package, in the Action column.

4. Enter the required proxy information
5. Click **OK**

You are required to confirm if you want to download the binaries related to the package you have chosen. If you do not want to download the binaries, click **Cancel**.

6. Click **Yes**

The download process of the respective binaries will begin. The download-process status will be updated once the package creation is completed.

7. Click **View packages**

	**Note:** You can click **Close** if you do not want to view the packages. You can cancel the package-creation process. However, you can do this only while creating multiple packages. Packages that have the Yet to Start status will be canceled.

You have successfully created a package. The package can now be modified or deployed like manually created packages.

Accessing the location of a package

When you create a package, you are required to download the package from the vendor's Web site. You can access the executable link for each package location through the application details. To access the executable links for the location of a package, follow the steps given below:

1. Click **Software Deployment>Templates**
2. Click the required application
3. In the **Application Details** window, click on the link against **Location**

	**Note:** You must ensure that the URL of the executable link is added to the exception list in the proxy server.

You can now re-create the package and deploy it.

These links will redirect you to the location from which the package is being downloaded. The possibility of getting a download error reduces if the link is accessible. However, if you get an error while trying to access the link, then you will get an error while trying to download the required binaries, from the Desktop Central server. You should verify the functionality of the executable links for packages only from the system on which the Desktop Central server is installed.

See also: Error While Downloading Binaries

Setting Up Patch Management

This section will guide you through the configurations that have to be performed for managing patches of Windows OS and Applications.

- Configuring Proxy Server
- Configuring Vulnerability DB Synchronization Interval
- Configuring Automated Patch Deployment
- Configuring System Health Policy
- Declining Patches for Scan

Configuring Proxy Server

Desktop Central periodically updates the vulnerability database with that of the Central Patch Repository that resides at Zoho Corp.'s site. Desktop Central uses this configuration to connect to the internet to update the vulnerability database.

Direct Connection to Internet

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Proxy Configuration** link. This opens the Proxy Settings page.
3. Select the "Direct Connection to the Internet" option and click OK

HTTP Proxy Configuration

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Proxy Configuration** link. This opens the Proxy Settings page.
3. Select the "Manual Proxy Configurations" option and specify the Proxy host, port, user name and password of the HTTP Proxy.
4. Click OK to save the configuration.

FTP Proxy Configuration

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Proxy Configuration** link. This opens the Proxy Settings page.
3. Select the "Manual Proxy Configurations" option.
4. Select Enable FTP option and specify the Proxy host, port, user name and password of the FTP Proxy.
5. Click OK to save the configuration.

Configuring Vulnerability DB Synchronization

The vulnerability or the patch database is a baseline against which the available and missing patches in the machines are determined. The database is periodically refreshed with latest information and placed in the Central Patch Repository. You can specify the interval at which the local vulnerability database be updated with that of the Central Patch Repository. To configure the update interval, follow the steps below:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Schedule Vulnerability Update** link to invoke the Vulnerability Update page.
3. The **Enable Scheduler** is selected by default. To disable scheduler, clear this option.
4. The default update time is 10.00 hrs on weekdays. To modify, select the update interval from any of the following options:

- **Daily** - to update everyday. You need to specify the starting time and starting day.
- **Weekly** - to update on specific day(s) in a week. You need to specify the starting time and the day(s) on which the update should happen.
- **Monthly** - to update on a specific day every month(s). You need to specify starting time, select a day and select a month/months.

5. If you wish a mail to be sent upon successful update, select the **Notify when Task Finishes** check box and provide the email address. You can specify multiple email addresses as comma separated values.
6. Click **Save Changes** to save the configuration.

Configuring Automated Patch Deployment

Desktop Central allows automating Patch Management at various levels. For example, Administrators can:

1. Choose to scan the systems in the network to detect the missing patches.
2. Scan and download the missing patches.
3. Scan, download, and deploy the missing patches.

All the above operations can be done for specific set of target computers like few systems will only be scanned, few other systems will be automatically patched and so on.

Follow the steps below to create scheduled tasks for automating patch management using Desktop Central:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click Automate Patch Deployment link available under Patch Settings
3. Click Add Scheduled Task button and specify the following:
    1. Specify a name for the task
    2. Select the deployment option from any of the following:
    - **Scan the Systems to Identify the Missing Patches**: This is the default option, which scans your network to detect the vulnerable applications.
    - **Scan the Systems and Download the Missing Patches**: Use this option to detect the vulnerable systems/applications in your network and download the corresponding fixes from the Microsoft website.
    - **Download the Missing Patches and Draft the Patch Configuration**: Use this option to automatically download the missing patches from the Microsoft website and create a draft of the Patch Configuration.
    - **Automatically Download and Deploy the Missing Patches**: Use this option to scan the systems periodically to identify the missing patches, download the patches from the Microsoft website, and deploy the patches to the computers.
    3. After selecting the required option, the next step is to schedule the frequency to scan the systems. You have the following options to schedule:
    - **Daily** - to schedule the scan to run everyday. You need to specify the starting time and starting day.
    - **Weekly** - to schedule the scan to run on specific day(s) in a week. You need to specify the starting time and the day(s) on which the scan has to be run.
    - **Monthly** - to schedule the scan to run on a specific day every month(s). You need to specify starting time, select a day and select a month/months.
    - If you wish a mail to be sent upon successful completion of the task, select the **Notify when Task Finishes** check box and provide the email address. You can specify multiple email addresses as comma separated values.
    4. The next step is to select the target computers for which the above operations has to be performed. The target chosen can be a whole domain, site, OU,

Group or specific computers. You can also exclude computers from the chosen targets based on specific criteria.

5. After adding the required target computers, click Create Task.

Repeat the above steps to create more tasks.

Note: It is advisable to schedule the Vulnerability Database synchronization prior to scanning the network systems so that the latest patch information will be available for comparison.

See Also: Patch Management Architecture, Patch Management Life Cycle, Scan Systems for Vulnerability, Patch Reports

Configuring System Health Policy

What is System Health Policy?

Desktop Central periodically scans the systems in your network to identify the missing patches. The missing patches include both the operating system and application patches pertaining to that system. Generally, patches are released with varying severities ranging from Low to Critical. Based on these patch severities, Desktop Central classifies the system into three categories to quickly identify the health status of the systems in the network.

How are the systems classified?

Based on the severity of the missing patches, the systems are categorized as Healthy, Vulnerable, and Highly Vulnerable in Desktop Central. The default health policy is as below:

- Healthy Systems are those that have up-to-date patches installed
- Vulnerable Systems are those that have missing patches in "Moderate" or "Low" severity levels.
- Highly Vulnerable Systems are those that have missing patches in "Critical" or "Important" severity levels.

	**Note:** The patches that are declined will not be considered for arriving at the system health status.

Customizing the Health Policy

Desktop Central allows you to customize this categorization by selecting the patch severity levels for various health states as below:

1. Select the **Admin** tab.
2. Click the **System Health Policy** link available under **Patch Settings**.
3. Select the patch severity levels that are allowed for each states and click **Save Changes**.

	**Note:** It may be noted that you will not be allowed to select the same patch severity in different health states, i.e, if you select Low for Healthy Systems, you will not be allowed to select Low option for Vulnerable and Highly Vulnerable states.

Enabling Patch Approval Process

Desktop Central allows you to automate patch deployment from identifying the missing patches and to deploy them on to the required computers. The automation is done irrespective of the patches and applications. There might be cases where you would like to test a critical patch in few computers before rolling it out to the entire network. In such cases, the Patch Approval Process comes handy. When you enable the patch approval process, no patch will be deployed via Automated Patch Deployment task unless the patches are approved for deployment. You can however deploy them manually to test.

To enable Patch Approval Process,

1. Select **Admin --> General Settings** (available under Patch Settings)
2. Select the "Deploy patches only when they are approved" option and click **Save**

You can approve the patches from any of the patch views like Applicaple Patches, Missing Patches, or Installed Patches. To approve patches, select the required patches and click **Mark As --> Approve** option.

Decline Patches

Desktop Central allows administrtaors to configure the applications and patches that has to be declined from scanning. The patches declined here will not be shown under the missing patches. Administrators can choose to decline:

1. Specific missing patches for individual applications. (**or**)
2. Missing patches of an application as a whole.

To Decline Applications:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click Decline Patch link available under Patch Settings
3. Click on Decline Applications tab.
    1. Select the Applications listed under Available Applications
    2. Click on ">>" button to move them under Declined Applications list.
    3. Click Update. The patches of the Applications listed under Declined Applications will not be scanned for, by Desktop Central.

To Decline Specific Patches:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click Decline Patch link available under Patch Settings
3. Click on Decline Patches tab.
    1. Select patches listed under Available Patches. You can use the "Filter by product" to view product wise patches.
    2. Click on "**>>**" button to move them under Declined Patches list.
    3. Click Update. The patches listed under Declined Patches will not be scanned for, by Desktop Central.

See Also: Patch Management Architecture, Patch Management Life Cycle, Scan Systems for Vulnerability, Patch Reports

Setting Up Asset Management

This section will guide you through the configurations that have to be performed to manage the software and hardware assets.

- Scan System for Inventory
- Manage Software Licenses
- Create Software Groups
- Manage Software Category
- Configure Prohibited Software
- Configure E-Mail Alerts
- Schedule Inventory Scanning

Scan Systems for Inventory

To get the inventory details of the systems, the following conditions have to be met:

- The systems should be added in the Scope of Management
- The systems have to be scanned at least once. You can also configure periodic scanning of systems to get an updated information.
- The systems to be scanned should have WMI Service running and DCOM enabled.

Steps to Enable DCOM

To Enable DCOM in Windows 2000 Computers

1. Select Start > Run
2. Type DCOMCNFG in the text field
3. Click OK.
4. Select Default Properties tab
5. Check the box "Enable Distributed COM in this machine"
6. Press OK

To Enable DCOM in Windows XP Computers

1. Select Start > Run
2. Type DCOMCNFG in the text field
3. Click OK
4. Expand Component Services > Computers > My Computer
5. Righe-click My Computer and select Properties
6. Select Default Properties tab
7. Check the box "Enable Distributed COM in this machine"
8. Press OK

Scan Systems Manually

To Scan the systems manually, follow the steps below:

1. Click the **Inventory** tab to view the Inventory Summary
2. Click the **Scan Systems** link from the left pane available under Actions / Settings.
3. This will list all the systems that are available under the Scope of Management. Select the systems to be scanned for inventory and click San System. To scan all the systems, click Scan All.

The systems will be scanned and the status of the scanning gets updated under the Scan Status column.

Troubleshooting Tips

1. If you do not find the system here, check whether you have added the system under the Scope of Management
2. Check the Agent Status of all the systems; it should be "Agent Installed". For systems with the status as "Not Installed" or "Agent Installation Failed", inventory scanning cannot be performed. You need to reinstall the agents in these systems before scanning them for getting the inventory details.
3. If you get an error as WMI Service is not running, start the WMI Service in the system and try scanning again.
4. If you get an error as Asset Scanning is locked, contact desktopcentral-support@manageengine.com
5. If you get an error as DCOM not enabled, enable DCOM and try scanning again.

Manage Software Licenses

Managing Software Licenses is one of the important aspect of asset management that helps enterprises in being compliant and in planning for additional purchases or during license renewals. In managing the software licenses, you would expect to achieve the following:

- Able to get their software compliant status
- Add the details of their software purchases - both one time and additional purchases of the same software
- Should know the computers using those licenses.
- Should be able to reallocate a license, if it is not used/required, to a different resource that require them
- Help them decide on software renewals and purchases.
- Group different versions of the same software and manage their licenses as a single entity.

Add Software License Details

To Add/Edit Software License details for commercial software, follow the steps below:

1. Click the **Inventory** tab to view the Inventory Summary
2. Click the **Manage Licenses** link from the left pane available under Actions / Settings. This will list the details of all the licenses that have been added. To add or edit the license detail, click the Add License button.
3. Select the software from the list. You should have scanned the Windows systems at least once to have the details of the software here. However you can also specify software that is not in the list.
4. The manufacturer and the software version details are pre-filled and cannot be modified.
5. Specify the number of licenses purchased.
6. Specify the details to whom the software is licensed to (optional).
7. Specify the purchase and expiry date in the respective fields (optional).
8. Add the License file and the Invoice related to the license purchase, if required
9. Add comments, if required.
10. The next steps is to associate these licenses to the computers. This step is optional and is used only for a logical reference.
    1. Select the Installed Computers option to view only the computers that have this software installed or Managed Computers to list all the computers that you are managing using Desktop Central
    2. Select the computer to which you wish to associate the license and move them to the Associated computers list.
11. Click **Save** to update the license details.

The details gets updated in the table below. It includes the following details:

- **Software Name**: Name of the commercial software.
- **Manufacturer**: The software manufacturer (vendor)
- **Licensed To:** To whom the software is licensed.
- **Purchased**: No. of licenses purchased
- **Installed**: No. of licensed software copies that are installed in the network.
- **Purchased Date**: The date of purchase.
- **Expiry Date**: The date of expiry.
- **License Key**: The Purchase license Key details.
- **License File**: The file containing the license particulars for a particular software.
- **Invoice File**: The file containing the Purchase information for a particular software.

You can filter the view based on the compliant status of the software like Under License, Over license, Expired Software, etc.

Adding Additional Licenses

If you have purchased additional licenses for the same software and if you wish to update the information, follow the steps below:

1. Click the **Inventory** tab to view the Inventory Summary
2. Click the **Manage Licenses** link from the left pane available under Actions / Settings. This will list the details of all the licenses that have been added.
3. Click the **Add More** link from the Actions column of the software for which you want to add additional licenses.
4. Specify the Number of licenses you have purchased along with the other details and click **Save**.

Create Software Groups

Desktop Central allows administrators to group software that have to be seen as a single group. For example, if you have different versions of Microsoft Office installed in your network and you wish to view all the Microsoft Office installations as a single software, you can group all the Microsoft Office versions and create a group. This way it is very easy to manage your software licenses. You may have to move all the paid software in your network to Commercial category prior to grouping them.

To create a new Software Group:

1. Click the **Inventory** tab to view the Inventory Summary.
2. Click the **Group Software** link from the left pane available under Actions / Settings. This will list all the software groups that have been created. Click the **Add Software Group** to create a software group.
3. This opens the Add/Modify Software Groups dialog listing all the commercial software installed in your network.
4. Specify a name for this group.
5. Select the software that you wish to group and move them to the Grouped Software list. The software category and the prohibited status of the first software in the selected list will apply to all the software of that group. You can change the position of the software in the selected list by selecting the software and clicking the arrow button on the right.
6. After selecting the required software, click **Save**.

To modify a Software Group:

1. Click the **Inventory** tab to view the Inventory Summary.
2. Click the **Group Software** link from the left pane available under Actions / Settings. This will list all the software groups that have been created.
3. Click the **Edit** icon from the Actions column of the group that you want to edit.
4. Add or remove the software from the group and click **Save**.

To delete a Software Group:

1. Click the **Inventory** tab to view the Inventory Summary.
2. Click the **Group Software** link from the left pane available under Actions / Settings. This will list all the software groups that have been created.
3. Click the **Delete** icon from the Actions column of the group that you want to delete.

Manage Software Category

Desktop Central allows you to categorize the software installed in your network in any of the pre-defined categories. You also have an option to create your own categories and add software to it.

Desktop Central comes with the following pre-defined software categories: Accounting, Database, Development, Driver, Game, Graphics, Internet, Multimedia, and Others. You can modify/delete or assign software to these categories. You can also create your own category.

To add a new software category:

1. Click the **Inventory** tab to view the Inventory Summary
2. Click the **Manage Software Category** link from the left pane available under Actions / Settings. This will list all the software categories that have been added, including the pre-defined categories. Click the **Create New Category** to add a new category.
3. Specify a name for the category.
4. The details of the software available in your network is listed below. Select the software that have to assigned to this new category and click >> button. This is optional. When you do not select any software, an empty category gets created and you can assign software to this category later.
5. Click **Update**. The new category gets added to the table below.

To modify a software category:

1. Click the **Inventory** tab to view the Inventory Summary
2. Click the **Manage Software Category** link from the left pane available under Actions / Settings. This will list all the software categories that have been added, including the pre-defined categories. Click the Edit icon from the Actions column of the category that you want to edit.
3. Rename the category and/or add/remove software to/from this category and click **Update**.

To delete a software category:

1. Click the **Inventory** tab to view the Inventory Summary
2. Click the **Manage Software Category** link from the left pane available under Actions / Settings. This will list all the software categories that have been added, including the pre-defined categories.
3. Click the delete icon from the Actions column to delete individually or select the categories that you wish to delete and click **Delete Category**.

Configure Prohibited Software

Every organization prohibits employees from using certain software. Desktop Central helps prohibit, usage of certain software in accordance to your company policies. Detecting such prohibited software will help tackle compliance issues that might otherwise pop-up. Desktop Central provides an option to add the list of software that are prohibited in the company. You can also configure and receive notification through email and take the necessary action. The auto-uninstall feature allows you to automatically remove the software within a specified time frame, once it is detected in the client machine. However, you can also exempt certain computers from the auto-uninstallation routine.

Adding prohibited software

You can simply add the list of software that is prohibited in the company to be detected during the regular scan cycles. Follow the steps given below to add a prohibited software to the list.

1. Click the **Inventory** tab to view the Inventory Summary
2. Click the **Configure Prohibited Software** link from the left pane available under Actions / Settings. This will list the details of all the software that are already prohibited.
3. Click **Add Prohibited Software**. This is open the Add Prohibited Software dialog listing all the software detected in the managed computers. You should have scanned the Windows systems at least once to have the details of the software here.
4. Select the software that you wish to prohibit and move them to Prohibited List.

   Note: In case you have grouped certain software and you are adding that Software Group under the Prohibited Software List, then all the software in that group will be added.
5. After adding all the software, click **Update**. The software gets added to the prohibited list.

Removing prohibited software

To remove prohibited software, select the software and click **Remove Prohibited Software**. You can select the software that you wish to remove from the prohibited list and

click **Remove Prohibited Software** to eliminate the selected software from the prohibited software list.

Configuring the Auto-Uninstall Policy

Desktop Central's Auto-Uninstall Policy helps you to automatically uninstall the detected prohibited software from the client machines. The uninstallation will happen during the subsequent refresh-cycle. Follow the steps given below to configure the Auto-Uninstall Policy:

1. Select the **Auto-Uninstall Policy tab**.
2. Select **Enable Automatic Uninstallation** check box.
3. Specify the Maximum number of Software that can be uninstalled from a computer during subsequent refresh cycle.

   Note: Increasing this number will cause high CPU usage during Uninstallation. If the software count exceeds this number in a computer, it will be uninstalled during the subsequent refresh cycle.
4. Select **Notify User before Uninstalling** check box and specify any custom message in case you want to prompt to the user before the software uninstallation.

   Note: The user will be notified with an Alert message during logon and whenever the agent detects prohibited software. This functionality will be applicable only if the **Notify User Settings** is configured.
5. Specify the wait-window for the software uninstallation. Say if you want to remove the software three days after it has been detected, then mention 3 in the text box provided.
6. Click on **Save** to save changes.

   Note: Auto-Uninstallation option is available only for .msi based applications. This functionality may not work for .exe based software applications and you will need to remove them manually.

Excluding Computers from Software Uninstallation

In certain occasions, you will need to allow the usage of prohibited software for certain users. One classic example is the usage of chat based applications. Many organizations will upfront prohibit such software. However top-level executives at these organizations might need such applications to communicate with clients, etc. Desktop Central allows you to exempt Auto-Uninstallation on computers in these specific custom groups. You can create a custom group comprising specific computers or can add individual computers to the Exclude list. The following steps will help you exclude groups:

1. Click the **Configure Prohibited Software** link from the left pane available under Actions / Settings of **Inventory** tab. This will list the details of all the software that are already prohibited.
2. Select the checkbox corresponding to the specified software and click the link under Exclusions column. This opens the **Add Exclusions** dialog.

3. Select whether to exclude custom groups or computers.
4. Select the groups/computers and move it to the **Excluded** list.
5. Click on **Save** to save changes.

Configuring Global Exclusion

Similar to excluding computers and custom groups for individual software, you can create a global exclusion list of computers. Computers that are added to the Global Exclusion list, either manually or via custom groups, applies to all the software. This means all these computers can have any of the software that have been marked as prohibited.

To configure global exclusion, click the **Configure Global Exclusion** button and select the required computers/custom group of computers and save.

Configure E-Mail Alerts

Desktop Central generates Email Alerts to notify the following events:

1. When a new hardware is detected in the network
2. When a new software is detected in the network
3. Non Compliance of software licensing policy, i.e., the license is inadequate and have to purchase more licenses to be compliant
4. When a software is being used after its license has expired.
5. When a prohibited software is detected in the network.

To configure email alerts, follow the steps below:

1. Click the **Inventory** tab to view the Inventory Summary
2. Click the **Configure Email Alerts** link from the left pane available under Actions / Settings.
3. Select the alert criteria; select all that apply.
4. Specify the email addresses as comma separated.
5. Click **Update Alert Settings**

Note: For email alerts to be sent, you should have configured your mail server settings.

Schedule Inventory Scanning

To schedule scanning of systems periodically,

1. Click the **Inventory** tab to view the Inventory Summary
2. Click the **Schedule Inventory Scan** link from the left pane available under Actions / Settings.
3. Select the **Enable Inventory Scan Scheduler** check box and specify the frequency at which the scanning has to be performed. You have the following options to choose the interval:
    1. **Daily** - to update everyday. You need to specify the starting time and starting day.
    2. **Weekly** - to update on specific day(s) in a week. You need to specify the starting time and the day(s) on which the update should happen.
    3. **Monthly** - to update on a specific day every month(s). You need to specify starting time, select a day and select a month/months.
4. Click **Save Changes** to save the configuration.

Setting Up User Logon Reports

As a first step, define the Scope of Management. You should only be able to track the user login details for the users logging in from the computers that are within the defined scope. After adding the computers in SoM, you can enable User Logon Reports.

To Maintain User Logon History:

1. Select **Admin --> User Logon Settings** to open the report settings page.
2. Select the **Enable User Logon Reports** and specify the number of days the history has to be maintained.
3. Click **Save Changes**

Setting Up Active Directory Reports

Desktop Central retrieves the information about the Active Directory infrastructure components and provides 100+ out-of-the-box reports. You can schedule the report update interval to get an up-to-date details.

To configure the AD report update interval:

1. Select **Admin --> AD Reports Settings** to open the report settings page.
2. Select the **Enable AD Report Scheduler** option.
3. Select the Domains for which the reports needs to be generated. If no domains are selected, the scheduler will be disabled.
4. Select the Scan Mode to specify whether to update all the objects or only the modified objects
5. Specify the update interval as below:
    1. **Daily** - to update everyday. You need to specify the starting time and starting day.
    2. **Weekly** - to update on specific day(s) in a week. You need to specify the starting time and the day(s) on which the update should happen.
    3. **Monthly** - to update on a specific day every month(s). You need to specify starting time, select a day and select a month/months.
6. Click **Save Changes**

To send the reports by Email

Desktop Central provides an option to send the Active Directory reports by email whenever it gets updated. You have an option to select the reports to be e-mailed and the email addresses.

1. Select **Admin --> AD Reports Settings** to open the report settings page.
2. Select the **Enable AD Report Scheduler** option.
3. Select the **Send Reports by Email** option
4. Specify the From, To Address and Email Subject.
5. Click the **Select Reports** button to select the reports to be sent by email.
6. Click **Save Changes**.

After the completion of every scheduled update, the selected reports will be e-mailed to specified email addresses.

User Guide

This section guides you in using Desktop Central to perform the Desktop Management activities. Follow the links to learn more:

- Software Installation
- Patch Management
- Hardware and Software Inventory
- Windows Tools
- Windows Configurations
- User Logon Reports
- Active Directory Reports
- Making Help Desk Requests

Software Installation

Desktop Central enables remote software deployment and distribution to the users and computers of the Windows network. This web-based software deployment configuration helps administrators to install software from a central point. It supports deploying both MSI and EXE based applications that can be installed in a silent mode.

Software Distribution Features

- Supports installing both MSI and EXE based applications.
- Supports Install, Uninstall, Assign and Redeploy options for MSI based applications.
- Supports Install and Uninstall options for EXE based applications.
- Ability to schedule software installations.
- Install Software at a specified time
- Install Software either during or after startup of the computer.
- Option to install the application as a specific-user using the **Run As** option.
- Supports executing pre-installation scripts/commands prior to installation and abort if not successful.
- Option to copy the installables to the client computers before installing the software.
- Ability to create package repository. The packages created once can be reused any number of times to install or uninstall the software.

The following links guides you to install software from remote using Desktop Central:

- Managing Software Packages
- Installing MSI-based Applications for Users
- Installing EXE-based Applications for Users
- Installing MSI-based Applications for Computers
- Installing EXE-based Applications for Computers
- Uninstalling MSI-based Applications for Users
- Uninstalling EXE-based Applications for Users
- Uninstalling MSI-based Applications for Computers
- Uninstalling EXE-based Applications for Computers

Installing MSI-based Applications for Users

To install an MSI application to the users, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **User Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as MSI.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Install Completely**, **Assign**, or **Redeploy** as the case may be. If you select the **Assign** option, the application will be installed only when the user tries to open the application for the first time.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be installed.
9. Select the users to whom the software has to be installed.
10. Click **Deploy**.

Installing EXE-based Applications for Users

To install an EXE application to the users, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **User Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as EXE.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Install**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be installed.
9. Select the users to whom the software has to be installed.
10. Click **Deploy**.

Installing MSI-based Applications for Computers

To install an MSI application to the computers, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **Computer Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as MSI.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Install Completely**, **Assign**, or **Redeploy** as the case may be. If you select the **Assign** option, the application will be installed only when the user tries to open the application for the first time.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be installed.
9. Select the computers in which the software has to be installed.
10. Click **Deploy**.

Installing EXE-based Applications for Computers

To install an EXE application to the computers, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **Computer Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as EXE.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Install**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be installed.
9. Select the computers in which the software has to be installed.
10. Click **Deploy**.

Uninstalling MSI-based Applications for Users

To uninstall an MSI application for users, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **User Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as MSI.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Remove**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be uninstalled.
9. Select the user objects from which the software has to be uninstalled.
10. Click **Deploy**.

Uninstalling EXE-based Applications for Users

To uninstall an EXE application for the user objects, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **User Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as EXE.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Remove**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be uninstalled.
9. Select the user objects from which the software has to be uninstalled.
10. Click **Deploy**.

Uninstalling MSI-based Applications for Computers

To uninstall an MSI application from the computer objects, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **Computer Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as MSI.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Remove**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be uninstalled.
9. Select the computer objects from which the software has to be uninstalled.
10. Click **Deploy**.

Uninstalling EXE-based Applications for Computers

To uninstall an EXE application from the computer objects, follow the steps below:

1. Click **Add Configuration** link from the Quick Links available below the tabs.
2. Click the **Install Software** link available under the **Computer Configurations**.
3. Provide a name and description for the configuration
4. Select the **Installer Type** as EXE.
5. Select the required package and specify the **Run As** option, if required.
6. Select the **Operation Type** as **Remove**.
7. Select the **Copy** options as required.
8. Specify the time at which the software has to be uninstalled.
9. Select the computer objects from which the software has to be removed.
10. Click **Deploy**.

Patch Management

The steady increase in network vulnerabilities and the sheer volume of software patches that fix these threats, over the years; has created a need for strict and efficient patch management in enterprises to avoid business downtime and to secure themselves against mishaps due to attacks.

The best way to address this problem, is to have a systematic, automated and affordable solution that is robust and manages patches effectively. Desktop Central with its Patch Management module provides the system administrators the ability to respond to computer threats in quick time. All this in compliance to the patch management life cycle and with a fresh perspective to network security.

Patch Management Features

- Uses a hosted Patch Database at Zoho Corp. site to assess the vulnerability status of the network.
- Complete automated Patch Management Solution from detecting the vulnerabilities to deploying the patches.
- Patch based deployment - Deploy a patch to all the affected systems
- System based patch deployment - Deploy all the applicable patches for a system
- Automatic handling of patch interdependencies and patch sequencing
- Reports on System vulnerabilities, Patches,OS, etc.
- Provides an update of the patch deployment status

Follow the links to learn more,

Patch Management Architecture

The Patch Management Architecture

The Patch Management consists of the following components:

- External Patch Crawler
- Central Patch Repository
- Desktop Central Server

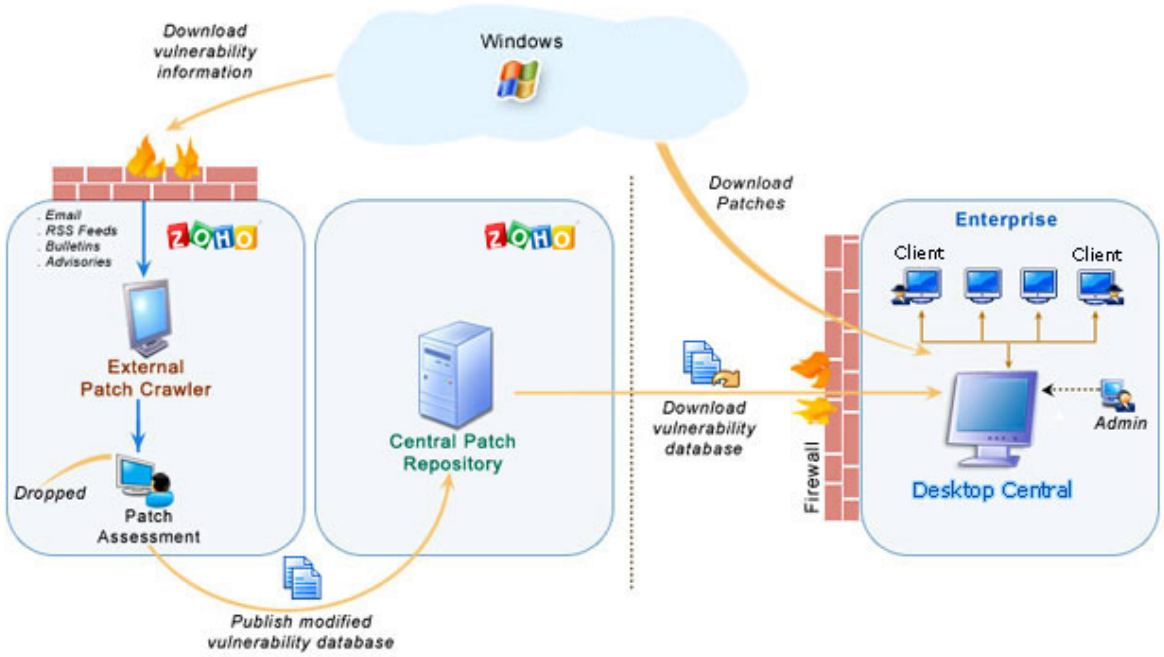


Fig: Patch Management Architecture

The *External Patch Crawler* resides at the Zoho Corp. site and repeatedly probes the internet to draw vulnerability information from the Microsoft website.

Patch download, assessment for patch authenticity and testing for functional correctness is also carried out at this site. The final analysis and data are correlated to obtain a consolidated vulnerability database which serves as a baseline for vulnerability assessment in the enterprise. The modified vulnerability database is then published to the Central Patch Repository for further use. The whole process of information gathering, patch analysis and publishing the latest vulnerability database occurs periodically.

The *Central Patch Repository* is a portal in the Zoho Corp. site, which hosts the latest vulnerability database that has been published after a thorough analysis. This database is exposed for download by the Desktop Central server situated in the customer site, and provides information required for patch scanning and installation.

The *Desktop Central Server* is located at the enterprise (customer site) and subscribes to the Central Patch repository, to periodically download the vulnerability database. It scans the systems in the enterprise network, checks for missing and available patches against the comprehensive vulnerability database, downloads and deploys missing patches and service packs, generates reports to effectively manage the patch management process in your enterprise.

How it Works?

Patch Management using Desktop Central is a simple two-stage process:

- Patch Assessment or Scanning
- Patch Download and Deployment

Patch Assessment or Scanning

Desktop Central periodically scans the systems in your windows network to assess the patch needs. Using a comprehensive database consolidated from Microsoft's bulletins, the scanning mechanism checks for the existence and state of the patches by performing file version checks, registry checks and checksums. The vulnerability database is periodically updated with the latest information on patches, from the Central Patch Repository. The scanning logic automatically determines which updates are needed on each client system, taking into account the operating system, application, and update dependencies.

On successful completion of an assessment, the results of each assessment are returned and stored in the server database. The scan results can be viewed from the web-console.

Patch download and deployment

On selecting the patches to be deployed, you can a trigger a download or a deploy request. At first the selected patches are downloaded from the internet and stored in a particular location in the Desktop Central server. Then they are pushed to the target machines remotely, after which they are installed sequentially.

See Also: Patch Management Life Cycle, Setting Up Patch Management Module, Scan Systems for Vulnerability, Patch Reports

Patch Management Life Cycle

Desktop Central Patch Management module consists to the following five stages:

1. Update Vulnerability Details from Vendors
2. Scan the Network
3. Identify Patches for Vulnerabilities
4. Download and Deploy Patches
5. Generate Status Reports

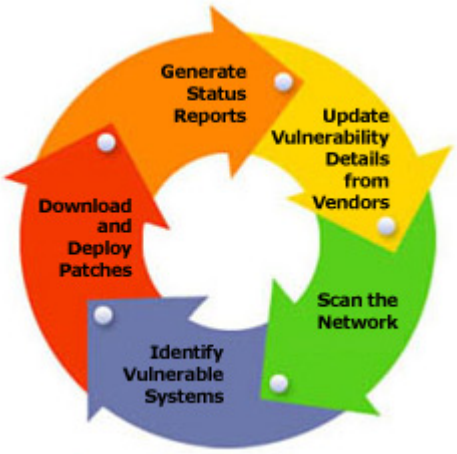


Fig: Patch Management Life Cycle

Update Vulnerability Details from Vendors

- Be up-to-date with the latest patch related information from the various sources.
- Download patches and run extensive tests to validate the authenticity and accuracy of patches

Scan the Network

- Discover and identify the systems in the network based on the defined Scope of Management.

Identify Patches for Vulnerabilities

- Assess the vulnerabilities in the systems periodically.
- Analyze what patches are missing and what are installed.

Download and Deploy Patches

- Download the required patches from the vendor site.
- Deploy patches in the missing systems.
- Verify and validate the accuracy of patch installation

Generate Status Reports

- Generate reports of various patch management tasks.
- Monitor the patching progress in the enterprise.

See Also: Patch Management Architecture, Setting Up Patch Management Module, Scan Systems for Vulnerability, Patch Reports

Scan Systems for Vulnerability

Desktop Central periodically scans the systems in your Windows network, to determine the vulnerable systems/applications. The latest status of the scan and the scan reports can be accessed by clicking the **Scan Status** link available under the **Patch Mgmt** tab. The following details are shown here:

- **Computer Name**: The DNS name of the computer being scanned.
- **OS Name**: The operating system of the computer being scanned.
- **Agent Status**: Specifies whether the agent is installed in the system or not.
- **Agent Version**: Specifies the agent version.
- **Last Scan Status**: The status of the previous scan.
- **Last Scan Time**: Time at which the scan was performed. Clicking this link will open the Vulnerable Systems Report for that system.

It also provides a graphical representation of the scanned systems. You can initiate the scan for any specific system by selecting the system and clicking the Scan Now button or can initiate the scan for all the systems by clicking the Scan All button.

To reschedule the scan, refer to the Configure Patch Scan Mode and Scan Interval

See Also: Patch Management Architecture, Patch Management Life Cycle, Setting Up Patch Management Module, Patch Reports

Installing Missing Patches

After identifying the missing patches in your network, the next step is to install the patches to fix the vulnerability. You can install the patches using Desktop Central by any of the following ways:

From the Applicable and Missing Patches Views

- By clicking the  icon from the action column of the patches.
- By selecting the patches and clicking the **Install Patches** button.

Both the above options will open the Installing Patches Configuration with the selected patches added. You can then select the targets and deploy the patches.

From the Latest and All Supported Patches Views

By selecting the patches and clicking the **Install Patches** button, opens the Installing Patches Configuration with the selected patches added. You can then select the targets and deploy the patches.

From the All Managed, Vulnerable, and Highly Vulnerable Systems Views

1. Click the Missing Patches link to view the missing patches of that system.
2. Select the patches and click the Install Patches button.

This opens the Installing Patches Configuration with the selected patches added. You can then select the targets and deploy the patches.

From the Install Patches Configuration

Like any other configuration, you can manually define a configuration for installing patches in computers.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Patch Views

Viewing Applicable Patches

The Applicable Patches view provides the details of the patches that affects the applications/systems in your network. The patch list also include the patches that are already installed in your network.

To view the list of the applicable patches, click the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack.

The network snapshot depicts the health and patch status of the systems in the network.

The details of the applicable patches shown in the tabular form include:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Patch Description**: A brief description about the patch.
- **Patch Type**: Refers to whether this patch applies to Microsoft OS/Applications or Non-Microsoft Applications like Adobe, Java, etc.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Approve Status**: This refers to whether the patch has been approved for bulk deployment via Automated Patch Deployment. This is significant only if you have enabled Patch Approval prior to buld deployment. You can also approve or decline a patch by selecting the appropriate option from the "Mark As" menu.
- **Release Date**: Refers to the date of release of the patch by the vendor.
- **Download Status**: Refers to the status of the patch download on the Desktop Central Server.
- **Affected Systems**: Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed.
- **Installed Systems**: Refers to the count of the systems where the patch has been installed.
- **Missing Systems**: Refers to the count of the systems that do not have the patches installed yet.
- **Failed Systems**: Refers to the number of systems on which the patch deployment has failed. Clicking the count will list the details of the failed computers, from where you can redeploy.

Installing Patches

You can install the patches by selecting the patches to be installed and by clicking the **Install Patches** button.

This will open the Installing Patches Configuration, with the selected patches added. Select the targets and deploy the configuration.

You can also click the Missing Systems count from where you can select the required systems and select **Install Patches** to deploy.

Bulletin Details

Bulletin details includes the following:

- Bulletin ID: The advisory article provided by the vendor which contains information about the vulnerability and patch availability.
- Posted On: The date of release of this bulletin.
- Updated On: The date of last update to this bulletin.
- FAQ Page: Links to the FAQ section in the Microsoft site for this bulletin.
- Q Number: Links to the knowledge base article available in the Microsoft web site.
- Issue: Details of the related issue.
- Bulletin Summary: A brief summary of the bulletin.
- Patch Details: The name of the patch and the affected products.

Patch Details

The following patch details are shown:

- Patch ID: A unique reference ID in Desktop Central for every patch
- Patch Name: The name of the patch
- Bulletin ID: The Bulletin ID pertaining to this patch
- MS Knowledge Base: The knowledge base article corresponding to this patch.
- Severity: The severity of the patch.
- Reboot: Specifies whether a system reboot is required on installing the patch.
- Download Status: Determines whether the patch is downloaded from the net (vendor site) and is made available in the Desktop Central's Patch Repository for deployment.
- Location Path: The complete download URL of the patch.
- Superseding Bulletin ID: Refers to the Bulletin ID pertaining to the patch that has taken its place.
- CVEID:
- BugTraq ID:

It also provides the details of the changes made to the files and registries on installing this patch.

See Also: Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Latest Patches

The Latest Patches view lists the details of the patches pertaining to the recently released Microsoft Bulletins.

To view the Latest Patches, select the Latest Patches link under the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack.

The following details of the patches are displayed:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Download Status**: Determines whether the patch is downloaded from the net (vendor site) and is made available in the Desktop Central's Patch Repository for deployment.
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Patch Description**: A brief description about the patch.
- **Patch Type**: Refers to whether this patch applies to Microsoft OS/Applications or Non-Microsoft Applications like Adobe, Java, etc.
- **Reboot**: Specifies whether the patch installation requires a system reboot or not.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Approve Status**: This refers to whether the patch has been approved for bulk deployment via Automated Patch Deployment. This is significant only if you have enabled Patch Approval prior to buld deployment. You can also approve or decline a patch by selecting the appropriate option from the "Mark As" menu.
- **Release Date**: Refers to the date of release of the patch by the vendor.

You can initiate the following actions from here:

- **Download**: Selecting the required patches and clicking Download will download the patch from the vendor site and make it available in the Desktop Central's Patch Repository for deployment.
- **Install Patches**: Selecting the required patches and clicking Install Patch, will open the Install Patch Configuration page from where you can select the targets and deploy.

See Also: Viewing Applicable Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Missing Patches

The Missing Patches view provides the details of the patches that affects the applications/ systems in your network, which are not installed.

To view the list of the missing patches, click the **Missing Patches** link under the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack.

The severity of the missing patches are depicted in a graph.

The details of the missing patches shown in the tabular format include:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Patch Description**: A brief description about the patch.
- **Patch Type**: Refers to whether this patch applies to Microsoft OS/Applications or Non-Microsoft Applications like Adobe, Java, etc.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Approve Status**: This refers to whether the patch has been approved for bulk deployment via Automated Patch Deployment. This is significant only if you have enabled Patch Approval prior to buld deployment. You can also approve or decline a patch by selecting the appropriate option from the "Mark As" menu.
- **Release Date**: Refers to the date of release of the patch by the vendor.
- **Download Status**: Refers to the status of the patch download on the Desktop Central Server.
- **Affected Systems**: Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed.
- **Installed Systems**: Refers to the count of the systems where the patch has been installed.
- **Missing Systems**: Refers to the count of the systems that do not have the patches installed yet.
- **Failed Systems**: Refers to the number of systems on which the patch deployment has failed. Clicking the count will list the details of the failed computers, from where you can redeploy.

Installing Patches

You can install the patches by selecting the patches to be installed and by clicking the **Install Patches** button.

This will open the Installing Patches Configuration, with the selected patches added. Select the targets and deploy the configuration.

You can also click the Missing Systems count from where you can select the required systems and select **Install Patches** to deploy.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Installed Patches

The Installed Patches view provides the details of the patches that are installed in your network.

To view the list of the installed patches, click the **Installed Patches** link under the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack.

The severity of the installed patches are depicted in a graph.

The details of the missing patches shown in the tabular format include:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Patch Description**: A brief description about the patch.
- **Patch Type**: Refers to whether this patch applies to Microsoft OS/Applications or Non-Microsoft Applications like Adobe, Java, etc.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Approve Status**: This refers to whether the patch has been approved for bulk deployment via Automated Patch Deployment. This is significant only if you have enabled Patch Approval prior to buld deployment. You can also approve or decline a patch by selecting the appropriate option from the "Mark As" menu.
- **Release Date**: Refers to the date of release of the patch by the vendor.
- **Download Status**: Refers to the status of the patch download on the Desktop Central Server.
- **Affected Systems**: Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed.

  To install multiple patches, select the patches and click Install Patches, which will open the Patch Configuration from where you can select the targets and deploy.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Supported Patches

The All Supported Patches view provides the details of all the patches released by Microsoft Corporation that are supported by Desktop Central.

To view the supported patches, click the **All Supported Patches** link under the **Patch Mgmt** tab. You can filter the view based on the application and service pack by selecting the appropriate product and service pack. The following details are shown:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Download Status**: Determines whether the patch is downloaded from the vendor's website and is made available in the Desktop Central's Patch Repository for deployment.
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Patch Description**: A brief description about the patch.
- **Patch Type**: Refers to whether this patch applies to Microsoft OS/Applications or Non-Microsoft Applications like Adobe, Java, etc.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Approve Status**: This refers to whether the patch has been approved for bulk deployment via Automated Patch Deployment. This is significant only if you have enabled Patch Approval prior to buld deployment. You can also approve or decline a patch by selecting the appropriate option from the "Mark As" menu.
- **Release Date**: Refers to the date of release of the patch by the vendor.
- **Reboot**: Specifies whether the patch installation requires a system reboot or not.
- **Superceded By**: Indicates that the patch is outdated and have another patch that is more recently released and has taken its place.

This information is retrieved from the Central Patch Repository that resides at the Zoho Corp.'s site periodically.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Healthy Systems, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Healthy Systems

Healthy systems are those that have all the security patches installed. To view the healthy systems in your network, click the **Healthy Systems** link under the **Patch Mgmt** tab.

The following details about the healthy systems are shown here:

- **Computer Name**: The name of the system.
- **OS Name**: The operating system of the computer.
- **Total Patches**: Total count of the patches applicable to this system. Click this link to view the details of the patches.
- **Installed Patches**: Total count of the patches that are installed. Click this link to view the details of the patches.
- **Missing Patches**: Count of the patches that are missing in the system. Click this link to view the details of the patches.
- **Informational Patches**: Total count of informational patches. Click this link to view the details of the patches.
- **Obsolete Patches**: Total count of obsolete patches. Click this link to view the details of the patches.
- **Health**: The health of the system.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Vulnerable Systems, Viewing Highly Vulnerable Systems

Viewing Vulnerable Systems

Vulnerable systems are those that do not have one or more Moderate/Low rated patches installed. To view the Vulnerable systems in your network, click the **Vulnerable Systems** link under the **Patch Mgmt** tab.

The following details about the vulnerable systems are shown here:

- **Computer Name**: The name of the system.
- **OS Name**: The operating system of the computer.
- **Total Patches**: Total count of the patches applicable to this system. Click this link to view the details of the patches.
- **Installed Patches**: Total count of the patches that are installed. Click this link to view the details of the patches.
- **Missing Patches**: Count of the patches that are missing in the system. Click this link to view the details of the patches.
- **Informational Patches**: Total count of informational patches. Click this link to view the details of the patches.
- **Obsolete Patches**: Total count of obsolete patches. Click this link to view the details of the patches.
- **Health**: The health of the system.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Highly Vulnerable Systems

Viewing Highly Vulnerable Systems

Highly Vulnerable systems are those that do not have one or more Critical/Important rated patches installed. To view the highly vulnerable systems in your network, click the **Highly Vulnerable** link under the **Patch Mgmt** tab.

The following details about the highly vulnerable systems are shown here:

- **Computer Name**: The name of the system.
- **OS Name**: The operating system of the computer.
- **Total Patches**: Total count of the patches applicable to this system. Click this link to view the details of the patches.
- **Installed Patches**: Total count of the patches that are installed. Click this link to view the details of the patches.
- **Missing Patches**: Count of the patches that are missing in the system. Click this link to view the details of the patches.
- **Informational Patches**: Total count of informational patches. Click this link to view the details of the patches.
- **Obsolete Patches**: Total count of obsolete patches. Click this link to view the details of the patches.
- **Health**: The health of the system.

See Also: Viewing Applicable Patches, Viewing Latest Patches, Viewing Missing Patches, Installing Missing Patches, Viewing Installed Patches, Viewing Supported Patches, Viewing Healthy Systems, Viewing Vulnerable Systems

Viewing Patch Reports

The Patch Reports provides you with detailed information about the vulnerable systems in your network and the patch details to fix the vulnerability. Desktop Central determines the vulnerability of the systems by periodic scanning to check whether the applicable patches have been installed. The following reports helps you to check your network vulnerability:

- Vulnerable Systems Report
- Vulnerable Patches Report
- Supported Patches Report

Viewing Vulnerable Systems Report

The Vulnerable Systems Report provides you a snapshot of the healthy and vulnerable systems in your network.

To view the report, click the **Vulnerable Systems Report** link available under the **Reports** tab. The details of the managed systems and their related patches are shown here:

- **Computer Name**: The name of the system.
- **OS Name**: The operating system of the computer.
- **Total Patches**: Total count of the patches applicable to this system. Click this link to view the details of the patches.
- **Installed Patches**: Total count of the patches that are installed. Click this link to view the details of the patches.
- **Missing Patches**: Count of the patches that are missing in the system. Click this link to view the details of the patches.
- **Informational Patches**: Total count of informational patches. Click this link to view the details of the patches.
- **Obsolete Patches**: Total count of obsolete patches. Click this link to view the details of the patches.
- **Health**: The health of the system.

Application and Patch Summary Report

Clicking the system count from the Vulnerable Systems Report, provides you the application-wise patch details for that system with their state like installed, missing, informational, obsolete, etc.

See Also: Viewing Vulnerable Patches Report, Viewing Supported Patches Report, Viewing Task Status Report

Viewing Vulnerable Patches Report

The Vulnerable Patches Report provides you the details of the patches that are applicable to your network and the affected systems. By default, it lists the details of the patches released in the current month. You have an option to select a different period or to specify a custom period and generate the report.

To view the report, click the **Vulnerable Patches Report** link available under the **Reports** tab. The following details are shown here:

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**: The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Affected Systems**: Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed. Click this link to view the details.
- **Installed Systems**: Refers to the count of the systems where the patch has been installed. Click this link to view the details.
- **Missing Systems**: Refers to the count of the systems that do not have the patches installed yet. Click this link to view the details.

See Also: Viewing Vulnerable Systems Report, Viewing Supported Patches Report, Viewing Task Status Report

Viewing Supported Patches Report

The Supported Patches Report provides the details of all the patches released by Microsoft Corporation irrespective of whether it is related to your network or not. When you plan to upgrade the systems in your network by installing the latest applications, you can sneak through this report to check whether any updates are available for the application.

By default, it lists the details of the patches released in the current month. You have an option to select a different period or to specify a custom period and generate the report.

To view the report, click the **Supported Patches Report** link available under the **Reports** tab. The following details of the patches are shown here:

- **Patch ID**: A unique reference ID in Desktop Central for every patch.
- **Bulletin ID**: The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- **Patch Name**:The name of the patch. Clicking this link, will lead you to the **Patch Details** view, which provides more details about the patch.
- **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Reboot**: Specifies whether the patch installation requires a system reboot or not.

See Also: Viewing Vulnerable Systems Report, Viewing Vulnerable Patches Report, Viewing Task Status Report

Hardware and Software Inventory

Hardware / Software Inventory and Asset Management

The Inventory module provides comprehensive details about the hardware and software details of the Windows systems in the network that helps in Asset Management.

Desktop Central periodically scans the network to collect the hardware and software asset details from each Windows desktop. The Hardware inventory details include information like, memory, operating system, manufacturer, device types, peripherals, etc. The Software inventory provides details of the software detected in the network grouped by volume and software vendors. It also provides the license compliance details of the software and software metering.

Scanning the Windows systems for inventory assets can be scheduled to have an up-to-date information. Alerts are generated to notify any specific events like a new hardware/software detected, license not compliant, etc. The comprehensive reports helps you to view the details in few clicks.

Inventory Management Features

- Complete Hardware and Software Inventory.
- Scan the systems periodically to collect the hardware and software details.
- Manage Software Licenses.
- Detect Prohibited Software in the network.
- Provides software usage statistics.
- Alert on specific events.
- Comprehensive reports on hardware, software inventory and license compliance.

Follow the links to learn more,

- Software Metering
- Viewing Computer Details
- Viewing Hardware Details
- Viewing Software Details
- Viewing Inventory Alerts
- Viewing Inventory Reports

Software Metering

Software metering allows you to monitor software usage in your enterprise. The Software Metering feature in Desktop Central, enables you to get the following information:

- Statistics of software applications used in computers in your network
- List of prohibited software applications in your network
- Details of usage of software applications that help you plan your software application-related purchases
- Status of the license compliance of software that helps you to plan for additional license purchases or cancel unused licenses

Features

The features include the following:

Software Metering Reports

There are two types of software metering reports that help you make an informed decision about buying software applications and renewing licenses for existing software applications. The reports are as follows:

- Software Inventory reports
- Software Compliance reports

Software Metering Rules

Software metering rules are rules that you can define to enable easy collection of software usage data for the computers in your network.

Prerequisites

You must know the following information before you add rules:

1. File name
2. Original file name
3. Product name
4. File version

To find out the information mentioned above, follow the steps given below:

	Assume that you have to find the file name, original file name, product name and version of Adobe Media Player.

1. Click **start**
2. Point to **Programs>Adobe**
3. Right-click **Adobe Device Central CS5** and click **Properties**
4. In the **Shortcut** tab, click **Find Target**

	The name of the target is the file name. Refer to Figure 1: Target .exe file for Adobe Device Central CS5. If the Find Target option is not available, locate where the .exe file of the application is stored and follow the steps given below.

Figure 1: File Name

5. Right-click on the target .exe file and click **Properties**
6. Click the **Version** tab
7. In the **Item** name list, click each of the following names to get information about them:

- Original file name
- Product name
- File version

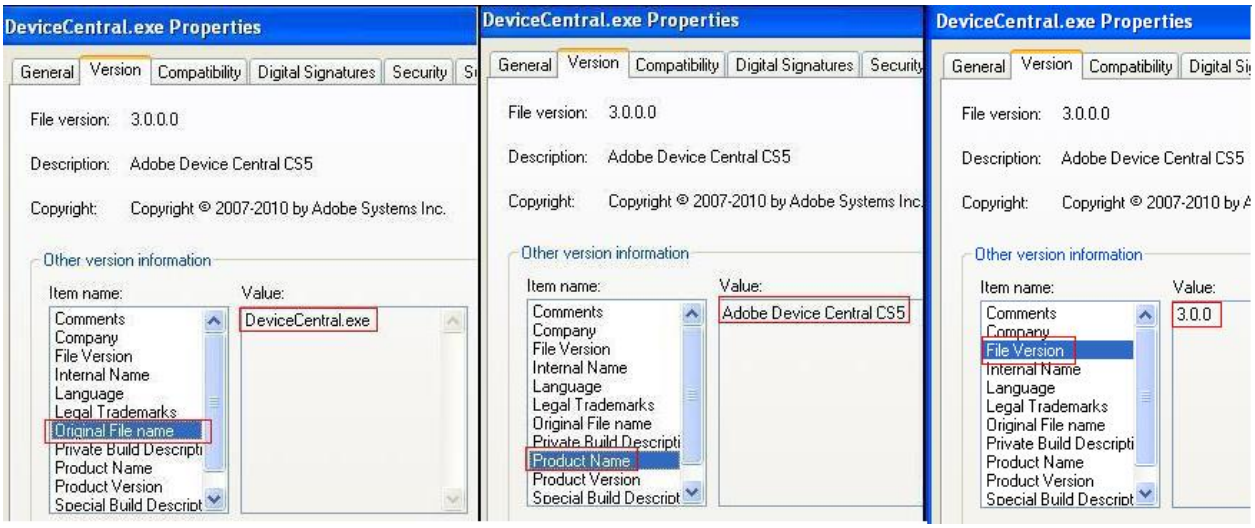


Figure 2: Original file name, Product name and Version

8. Click **OK**

You now have the required information to add rules.

Adding Rules

You are required to add rules to monitor the usage details of specific software applications. To add rules, follow the steps given below:

1. Click **Inventory**
2. In the **Actions/Settings** section, click **Software Metering**
3. Click **Add Rules**
4. Click **Select Software**
5. Select the required software application
6. Click **Select**
7. Enter a name for the rule

	The name you enter for the rule should be unique and descriptive. For example, if you have selected Adobe Flash Player, you can enter Monitoring Adobe Flash Player Usage as the name of the rule. Once you have used this name, you cannot use it as a name for any other rule.

9. Enter the following:
10. File name
11. Original file name
12. Product name
13. Version

	Refer to the section about prerequisites for more information.

10. Enter comments (if required)
11. Click **Save**

You have added a rule for a software application.

By default, the software metering rule is enabled. You can disable, edit or delete the rule by using the icons in the Action column. You can also disable, edit or delete more than one software metering rule simultaneously by using the respective buttons provided.

	You cannot add software metering rules for groups of software.

Predefined Rules

In Software Metering there are certain predefined rules available. These rules are used to automatically assign rules to software applications that are commonly monitored. For example, if you monitor the Microsoft Office Suite in all the computers in your network to keep a track of license information, it will be added automatically to the list of software metering rules. Rules will be created for all the software applications that comprise the Microsoft Office Suite.

Software Usage Statistics

It is important to monitor software usage statistics and record them. This information will help you make an informed decision when you want to buy new software applications or renew licenses for existing software applications. Desktop Central provides information about all the software applications installed in your network.

The software usage information is gathered from the metering rules that you create for software applications.

Viewing software usage information

To view software usage information gathered from software metering rules, follow the steps given below:

1. Click the **Reports** tab
2. In the **Reports Category**, click **Inventory Reports**
3. In the **Software Reports** section, click **Application Metering Rules Summary**
4. You can see the following information:
5. Name of the software metering rule
6. Name of the file
7. Discovered count: This refers to the number of computers that the agent finds the software application installed in. For example, if you have installed Adobe Dreamweaver on 500 computers, but 300 computers are not available (because they are shut down) when the agent is scanning the network. The agent will detect the Adobe Dreamweaver software application only in 200 computers. Hence, the discovered count is 200. This information gets updated everyday at 12:00 a.m.
8. Usage count: This refers to the number of times a software application is used (opened and closed) in all the computers that are being monitored for software usage in your network. For example, if Mozilla Firefox is installed in 300 computers and each of the 300 users uses Mozilla Firefox 10 times a day for 5 working days, the usage count of Mozilla Firefox, for all the computers, will be 15000.

	You can view the usage details for individual computers and individual software applications which belong to a group, in the Software Details page. To view the details, click on either the name of the software or the discovered count.

- Duration of usage: This refers to information about how long a software application has been used. This is measured in hours.

5. Click on the discovered count number to view the details of a software metering rule for specific computers.

	Use this report instead of the report Software Usage by Computer for detailed information about software usage in the computers in your network.

You can now view software usage information gathered from software metering rules.

Viewing Computer Details

The Computers view provides the details of the computers and their operating systems.

To view the computers, select the **Inventory** tab and click the **Computers** link. It also provides a graphical representation of the computers by their operating systems. The table below provides the following details of the computers:

- **Computer Name**: The DNS name of the computer
- **Operating system**: The operating system of the computer
- **Service Pack**: The service pack version of the operating system
- **Version**: The operating system version.
- **Virtual Memory**: Total virtual memory in kilobytes.
- **Free Virtual Memory**:Total virtual memory in kilobytes that is currently unused and available.
- **Visible Virtual Memory**:Total physical memory that is available to the operating system.
- **Free Visible Memory**: Total physical memory that is currently unused and available.

You can use the **Column Chooser** to select the columns to view.

Viewing Hardware Details

The Hardware view provides the details of the hardware detected in the scanned systems.

To view the hardware details, select the **Inventory** tab and click the **Hardware** link. It provides the following details:

- **Hardware Name**: Name of the hardware device.
- **Hardware Type**: Type of the hardware like processor, keyboard, port, etc.
- **Manufacturer**: Name of the manufacturer of that hardware device.
- **Number of Items**: Total number of items available in the scanned system. To get the details of number of copies available in each system, click the number of items.

You can use the **Column Chooser** to select the columns to view.

Viewing Software Details

The Software Inventory view provides the details of the software detected in the scanned systems.

To view the software inventory details, select the **Inventory** tab and click the **Software** link. You can filter the view by Software Type, Access Type, or License Compliance status using the **Filter** option. It provides the following details:

- **Software Name**: Name of the software.
- Version: The version of the software.
- **Software Type**: Can be either commercial or non-commercial. Use the **Move To** option to specify the software type.
- **Purchased**: Number of copies purchased. This information has to be provided by clicking the **Add / Modify License** button or from Manage Software Licenses.
- **Installed**: Number of copies installed.
- **Remaining**: Number of licenses remaining.
- **Compliant Status**: The license compliance status of the software. The status is arrived based on the license count specified using the **Add / Modify License** button or from Manage Software Licenses and is not applicable for non-commercial software.
- **Access Type**: Can be either Allowed or Prohibited. To add/remove software to the prohibited links, use the **Move To** option or from Configure Prohibited Software.
- Vendor: The software vendor.
- **Licensed To**: Refers to the person or the company to whom the software is licensed.
- **Purchased Date**: Date of purchase of license.
- **License Expiry Date**: Date of license expiry.
- **Remarks**: Remarks, if any.

You can use the **Column Chooser** to select the columns to view.

To Add License Details

1. Select the software from the table and click **Add / Modify License**. This opens the Add / Modify License view.
2. The manufacturer and the software version details are pre-filled and cannot be modified.
3. Specify the number of licenses purchased.
4. Specify the purchase and expiry date in the respective fields (optional).
5. Click **Add License**.

To Specify Software and Access Type

1. Select the software from the table and choose the access or the software type from the Move To combo box. You can select multiple software and choose the required option.
2. Click **OK** to confirm.

To Assign Software to a specific Category

1. Select the software from the table and choose a category from the Assign To Category combo box. You can select multiple software and assign them to a category.
2. Click **OK** to confirm.

Note: When you assign a software that was earlier assigned to a different category to a new category, it gets automatically disassociated from the previous category. This means that you cannot have the same software in two different categories simultaneously.

Viewing Inventory Alerts

Desktop Central generates Email Alerts to notify the following:

1. When a new hardware is detected in the network
2. When a new software is detected in the network
3. Non Compliance of software licensing policy, i.e., the license is inadequate and have to purchase more licenses to be compliant
4. When a prohibited software is detected in the network.

Based on the alert configuration, alerts are generated. You can view the alerts selecting the **Inventory** tab and clicking the **Alerts** link from the left pane.

You can filter the view based on the Alert Type, which can be any of the following:

- Hardware Added
- Hardware Removed
- Allowed Software Installed
- Allowed Software Uninstalled
- Prohibited Software Installed
- Prohibited Software uninstalled
- Software Under-Licensed
- License Expired
- Prohibited Software Identified
- New Computer Identified

Viewing Inventory Reports

Desktop Central provides various out-of-the-box inventory reports to view the software and hardware inventory details of the systems in the network. It also provides reports for verifying the license compliance and software metering.

1. Hardware Inventory Reports
2. Software Inventory Reports
3. Software Compliance Reports
4. System Details Reports
5. Warranty Reports

Hardware Inventory Reports

Computers by OS

Provides the details of the computers by their operating system. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by OS** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Manufacturer

Provides the details of the computers by their manufacturer. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Manufacturer** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Memory

Provides the details of the computers by their RAM size. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Memory** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Age

Provides the details of the computers by their year of manufacturing. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Age** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Device Type

Provides the details of the computers based on their type like, Laptop, Portable, Desktop etc. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Device Type** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computer by Disk Usage

Provides the details of the computers along with their total and free hard disk space. You can filter the view by domain ot by specifying the disk usage criteria. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a remote connection to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computer by Disk Usage** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Software Inventory Reports

Software by Manufacturer

Provides the details of the software installed in the scanned systems based on their vendors along with the total number of copies installed. Clicking the copies count will show the computers that have the software installed. You can filter the view by selecting a vendor from the combo box.

To view the report, select the **Inventory** tab and choose the **Software by Manufacturer** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Recently Installed Software

Provides the list of software installed recently. You can choose to select a pre defined period or provide a custom period to get the software list.

To view the report, select the **Inventory** tab and choose the **Recently Installed Software** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Prohibited Software

Provides the list of prohibited software detected in the network.

To view the report, select the **Inventory** tab and choose the **Prohibited Software** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software Usage by Computer

Provides the list of software and their usage statistics in individual computers.

To view the report, select the **Inventory** tab and choose the **Software Usage by Computer** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software Product Keys

Provides the list of Product Keys that were used for installing the software. The Product Keys can be identified for the following software:

1. Adobe Photoshop
2. Macromedia Dreamweaver
3. Macromedia Flash
4. Microsoft Office
5. Microsoft SQL Server
6. Microsoft Visual Studio

To view the report, select the **Inventory** tab and choose the **Software Product Keys** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Computers with / without a specific Software

Displays the list of Computers that have/do not have a particular software installed on them. You have the flexibility to extract the list based on inputs like, Exact Match of the Software Name specified (or) just a part of the Software Name, etc. Say for example: For an exact match, you specify MS Word and select "Equal" in the Software Name filter. And if you want to identify all the computers that have any of the Microsoft Products, you can simply select the "Like" filter and specify Microsoft in the Software Name field.

To view the report, select the **Inventory** tab and choose the **Computers with / without a specific Software** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software Metering

For every Software Metering Rule that you have defined, the Software Metering report will provide the summary of the usage statistics like the number of computers which have this software installed, the usage count of this software and the total usage in hours. You can click on the computers count to get the usage statistics on the individual computers where this software is installed.

To view the report, select **Inventory --> Inventory Reports --> Software Metering**

License Compliance Reports

License Compliance Report

Provides the details of the commercial software with their license compliance status. The license compliance status id determined based on the input provided in the Manage Software Licenses.

To view the report, select the **Inventory** tab and choose the **License Compliance Report** link by hovering the mouse over the **Inventory Reports**

Licenses to be Renewed

Provides the list of software whose licenses have to be renewed shortly. You can choose the time period from the combo box. You can also view the licenses that has already expired by selecting the appropriate option.

To view the report, select the **Inventory** tab and choose the **Licenses to be Renewed** link by hovering the mouse over the **Inventory Reports**

Viewing System Details Reports

1. Local Group Members
2. Computers by Services

Local Group Members

This reports will give you the list of local user accounts available in the computers of the selected domain. By default, this will list the all the computers with group name as Administrator. You can filter the view by selecting the domain or a custom group and choose the group to view their details.

To view the report, select the **Inventory** tab and choose the **Local Group Members** link available under System Details category by hovering the mouse over the **Inventory Reports**

Computers by Services

This report provides you with the list of computers that has a particular Windows Service running. You can choose the service, its start mode and state and click Generate Report to get the list of computers running that particular service.

To view the report, select **Inventory tab --> Inventory Reports --> Computers by Services**.

Viewing Warranty Reports

Desktop Central automatically retrieves the warranty information of Dell, HP, Toshiba and Lenova computers and provides you the details of the computers whose warranty is about to expire or whose warranty has already expired, etc. While Dell, Toshiba and Lenova computers require no additional information other than their service tag, HP computers require the Product Number to retrieve the warranty information from the vendor. To specify the Product Number of HP computers, follow the steps below:

1. Select Admin --> Feed Custom Data for Computers
2. Choose the HP computers from this list and click the edit link available beside it.
3. Specify the Product Number of the computer in the respective field and save.

1. Do not specify the Shipping and Expiry date yourself. Specifying this will stop automatic warranty check and all the warranty reports will be based on this expiry date you specify here.
2. You can also import the product numbers in bulk using the Import from CSV option

For computers other than HP, Toshiba, Dell and Lenova, you can specify the shipping and expiry information manually here to get warranty information in reports.

Soon-to-expire Warranty

Provides you the details of the computers whose warranty is about to expire soon. You can filter the view to choose the Domain, Custom Group and expiry period.

Expired Warranty

Provides the list of computers whose warranty has already expired

Unidentified Computers

Computers whose warranty information could not be retrieved or for those whose expiry information has not been specified manually will be listed here.

Windows Tools

Desktop Central provides various windows tools that can be run on the network system simultaneously. This section guides you through the purpose and the process of accessing these tools. The Windows Tools include the following:

- System Tools
- Remote Desktop Sharing
- Wake on LAN Tool
- Remote Shutdown Tool

To access these tools, select the Tools tab from the Desktop Central Client and click on the respective tool.

System Tools

Windows System Tools

Desktop Central provides various system tools, such as Disk Cleaner, Disk Checker, and Disk Defragmenter, that can be run on the multiple computers simultaneously. This section guides you through the process of creating and scheduling tasks to run these tools and to view the status history of the tasks that are executed. Follow the links to learn more:

- Creating and Scheduling Tasks
- Viewing and Modifying the Tasks
- Viewing the Task History

Creating and Scheduling Tasks

To create and schedule a task to run the Windows system tools in multiple computers, follow the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the network machines.
2. Click on any of the tools under the System Tools category to open the Task Details page. This lists all the tasks that are already created and scheduled. Click the Add Task button to create a new task. This opens the Add Task Wizard and follow the instructions as explained below:

Step 1: Define Task

1. Provide a name and description for the task.
2. Select the tools that you wish to run and click Next.
3. Based on the tool selection, specify the options for executing the task as below:
    1. Check Disk: Select the drive that has to be checked and the required options and click Next. You can select from any of the following options:
    - *Verbose* - Displays the name of each file in every directory as the disk is checked.
    - *Quick Check* - This option is only available for NTFS file system. This skips the checking of cycles within the folder structure and performs a less vigorous check of index entries to reduce the time.
    2. Disk Cleanup: Select the files and folders to be cleaned and click Next. The following actions can be performed **
    - *Compress old files* - Windows can compress files that you have not used in a while. Compressing the files saves disk space while still enabling you to use them. No files are deleted. Because files are compressed at different rates, the displayed amount of disk space you will gain is approximate.
    - *Remove content indexer* - The Indexing service speeds up and improves file searches by maintaining an index of the files on the disk. These files are left over from a previous indexing operation and can be deleted safely.
    - *Remove downloaded Program Files* - Downloaded program files are ActiveX controls and Java programs that are downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.
    - *Remove internet cache files* - The Temporary Internet Files folder contains Web pages that are stored on your hard disk for quick viewing. Your personalized settings for Web pages are left intact.
    - *Remove Office setup files* - Installation files used by office. If these files are removed from your computer, you may be prompted for original installation media or source during Reinstall, Repair, or Patch operation. It is recommended that you not remove these files unless you always have ready access to your installation media

- *Remove offline files* - Temporary files are local copies of network files that you specifically made available offline so that you can use them when you are disconnected from the network.
- *Remove old check disk files* - When Chkdsk checks your disk for errors, it might save lost file fragments as files in your disk's root folder. These files are unnecessary and can be removed.
- *Empty recycle bin* - The Recycle Bin contains files you have deleted from your computer. These files are not permanently removed until you empty the Recycle Bin.
- *Remove Temporary files* - Programs sometimes store temporary information in a Temp folder. Before a program quits, it usually deletes this information. You can safely delete temporary files that have not been modified in over a week.
- *Remove temporary offline files* - Temporary offline files are local copies of recently used network files that are automatically cached for you so that you can use them when you are disconnected from the network.
- *Remove Active Setup Temp Folders*
- *Remove memory dump files*
- *Remove remote desktop cache files*
- *Remove setup log files*
- *Remove old system restore positions.*
- *Remove web pages*
- *Remove uninstall backup images*
- *Remove webclient and web publisher cache files*

3. Disk Defragmenter: Select the drive that has to be defragmented and the required options and click Next. Seelct from the following options:

- *Verbose*: Displays the complete analysis and defragmentation reports
- *Analyze*: Analyzes the volume and displays a summary of the analysis report.
- *Force Defragmentation*: Forces defragmentation of the drive regardless of whether it needs to be defragmented.

Step 2: Define Target

Using the Defining Targets procedure, define the targets for deploying the tasks.

Step 3: Define Scheduler

Specify the following scheduling options:

Parameter	Description
Run As*	The name of the user as whom the task will be run. Click the ☆ icon to select and assign a dynamic variable to this parameter, for example, $DomainName\$DomainUserName or $ComputerName\$DomainUserName.
Password	The password of the user.
Confirm Password	Confirm the password again.

Parameter	Description
Perform this task*	Specify the time to perform the task. You can select from the following options: *Daily:* To run the task daily. Specify the time and duration to run the task. *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run. *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months. *Once:* To run the task only once. You need to specify the date and time. *At System Startup:* To run the task when the system is started. *At Logon:* To run the task during the user logon. *When Idle:* To run the task when the system is idle for the specified time.
Advanced Settings	
General	*Enabled*: Select this option to run the task at the specified time. *Run only when logged on:* Select this option to run the task only when the user has logged on.
Scheduled Task Completed	*Delete the task if it is not scheduled to run again:* Select this option to delete the task when it is no longer scheduled. *Stop Task:* Select this option and specify the duration after which the task will be stopped.
Idle Time	Select the required options: Specify the duration,the system has to be idle before starting a task. Stop the task if the computer ceases to be idle
Power Management	Select the required options: Don't start the task if the computer is running on batteries Stop the task if battery mode begins Wake the computer to run this task

Step 4: Deploy the Task

Click the **Deploy** button to deploy the task in the defined targets. The tasks will be run at the scheduled time and interval. The status of the tasks and its execution history can be verified from the Task Details page. Refer to the Viewing the Task History topic for details.

See Also: Viewing and Modifying the Tasks, Viewing Task History, Disk Defragmenter, Check Disk, Disk Cleanup

**The descriptions of various file types in Disk Cleanup are taken from Microsoft Help Documentation

Viewing and Modifying the Tasks

Desktop Central allows creating multiple tasks that can be created to run various actions on different target computers at different intervals. You can view the tasks that are created by following the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the computers.
2. Click on any of the tools under the System Tools category to open the Task Details page. This lists all the tasks that are already created and scheduled.
3. To modify a task,
    1. Click the  icon from the Actions column of the corresponding task.
    2. This opens the Modify Configuration Wizard. You can add/remove tools, change the tool options, the target systems, and the scheduled time as required.
    3. Click **Deploy** to effect the changes.
4. To Delete a task, click the  icon from the Actions column of the corresponding task.

See Also: Creating and Scheduling Tasks, Viewing Task History, Disk Defragmenter, Check Disk, Disk Cleanup

Viewing Task History

Desktop Central provides the details of the tasks executed on the target devices and the access logs of the tool execution.

Viewing Last Execution Status

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the network machines.
2. Click on any of the tools under the System Tools category to open the Task Details page. This lists all the tasks that are already created and scheduled.
3. Click on a task to view the details, such as the systems in which the task is executed, the last execution time, and the status of the task execution. Clicking the status will provide the access log of the performed task.

Viewing Task Execution History

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the network machines.
2. Click on any of the tools under the System Tools category to open the Task Details page. This lists all the tasks that are already created and scheduled.
3. To view the history of the task executed on a specific system, click the computer name. This will provide the history of the task execution on that computer along with the status on each execution. Clicking the status will provide the access log pertaining to that execution.

See Also: Creating and Scheduling Tasks, Viewing and Modifying the Tasks, Disk Defragmenter, Check Disk, Disk Cleanup

Remote Desktop Sharing

The Remote Desktop Sharing feature in Desktop Central enables administrators to access remote computers in a network. This Web-based feature enables you to access computers in both Local Area Networks (LAN) and Wide Area Networks (WAN).

Read the following sections to learn more about the Remote Desktop Sharing feature:

- Prerequisites
- Making required settings
- Connecting to remote computers
- Transferring files
- Troubleshooting tips

Advantages

The advantages of using the Remote Desktop Sharing feature are as follows:

- Does not require authentication to gain access to a remote computer
- Supports viewing and accessing remote computers using Active X and Java Plug-ins
- Enables administrators to prompt users for confirmation before providing access to a remote desktop

Prerequisites for Sharing Computers Remotely

You can access computers of remote computers, in a Local Area Network (LAN) or in a Wide Area Network (WAN), to complete various tasks. For example, you can remotely access a computer to

Ensure that the following prerequisites are met before you access computers remotely. You must do the following:

- Configure controls in the browser you are using
- Open the required ports
- Configure settings to share computers remotely

Configuring Controls in Your Browser

You are required to configure certain controls in your browser before connecting remotely to a computer. For example, if you are using an ActiveX viewer, in Mozilla Firefox, to view the remote computer, you must install Java Plug-ins in the browser you are using.

Ensure that you configure controls only in the browser from where a remote connection is being established.

Configuring ActiveX Controls in Internet Explorer

You must configure ActiveX controls when using Internet Explorer to connect to computers remotely.

To configure ActiveX controls in Internet Explorer, you must make the following settings for your Web content zone:

- Specify custom security settings
- Set the security level

Specifying Custom Security Settings

To specify custom security settings for your local intranet, follow the steps given below:

1. Open Internet Explorer
2. On the **Tools** menu, click **Internet Options**
3. Click the **Security** tab
4. In the required Web content zone icon

	For example, if the remote computer and the Desktop Central server are both in the local intranet, you must configure the following settings for the local intranet.

5. Click **Custom Level**
6. In the **Settings** section, under **ActiveX controls and plug-ins**, click **Enable** or **Prompt** in the following sections:
   - Download signed ActiveX controls
   - Download unsigned ActiveX controls
   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked safe for scripting
7. Click **OK** to save the security settings you made
8. Click **OK** to close the Internet Options property sheet

You have enabled ActiveX controls in Internet Explorer

Setting Security Levels

To set the security level, follow the steps given below:

1. Open Internet Explorer
2. On the **Tools** menu, click **Internet Options**
3. Click the **Security** tab
4. Select **Local intranet**
5. Click **Default Level**
6. Set the security level to either one of the following:
   - Medium
   - Medium-Low
   - Low
7. Click **Apply** to apply the option you have set the security level to
8. Click **OK** to close the Internet Options property sheet

You have set the security level for your local intranet.

Configuring Mozilla Firefox or Flock to Install Desktop Central Add-ons

Before you use either Mozilla Firefox or Flock to establish a connection with a computer remotely, you must configure the browser settings to allow you to install Desktop Central add-ons in it.

To configure Mozilla Firefox or Flock to enable you to install Desktop Central add-ons in it, follow the steps given below:

1. On the **Tools** menu, click **Options**
2. Click the **Security** tab
3. Enable the **Warn me when sites try to install add-ons** option
4. Click **Exceptions**

5. In the **Allowed Sites** section, add the name or the IP Address of the machine where the Desktop Central server is installed
6. Click **Allow**
7. Click **Close**
8. Click **OK** to close the Options property sheet

You have configured Mozilla Firefox or Flock to enable installation of Desktop Central add-ons. Now you can install the required Desktop Central add-on. When you've installed the required add-ons, you can connect remotely to computers.

Installing Java Plug-ins in Browsers

You must install Java plug-ins when you want to:

- Use the Java viewer to connect remotely to a computer from a browser
- Use the ActiveX viewer in Mozilla Firefox or Flock to connect to a remote computer

If Java plug-ins are already installed, the connection is automatically established. However, if the required Java plug-ins are not installed, you will be prompted to download and install them to connect to a remote computer.

	You can download and install Java plug-ins from http://java.sun.com/products/plugin. You may have to restart the browser after installing the plug-ins.

Opening Required Ports

You must open relevant ports in the firewall in the Desktop Central server, when you want to do the following remotely:

- Control computers
- Transfer files

	If there is a third-party firewall between the Desktop Central server and the remote computer, you must open port number 8443.

Opening Ports to Control Computers Remotely

You must open the Transmission Control Protocol (TCP) port 8443 in the computer where the Desktop Central server is installed. If you are using the Windows firewall, follow the steps below to add this port to the exception list:

1. Click **start>Settings>Control Panel**
2. Double-click **Windows Firewall**
3. Click the **Exceptions** tab

4. Click **Add Port**
5. Enter a name for the port
6. Enter 8443 in the Port number box
7. Click **TCP**
8. Click **OK**

You have opened the port required to control computers remotely.

Opening Ports to Transfer Files Remotely

The following list gives you the port numbers that you must open to transfer riles remotely. These are categorized as follows:

For a secure mode of transfer

When you want to transfer files using a secure mode of transfer you must open the following ports:

- Gateway Port:8443
- File Transfer Port: 8031

For a non-secure mode of transfer

When you do not want to transfer files using a secure mode of transfer you must open the following ports:

- Gateway Port: 8444
- File Transfer Port: 8032

Changing the mode of transfer

The default mode of transfer is the secure mode. However, to change the mode of transfer to the non-secure mode, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Control**
3. Click the **Settings** tab
4. In the **Port Settings** section, uncheck the **Use Secure Connection** checkbox

You have changed the mode of transfer from a secure connection to a non-secure connection.

Configuring Remote Desktop Settings

You can configure the following settings in Desktop Central before you connect and control a remote computer:

- Port-related settings
- Compression settings
- Prompt settings
- General settings

Features of the Remote Desktop Settings

The table given below enables you to understand when to use each of the settings given in the Settings tab for Remote Desktop Sharing:

S.No.	Section	Option	Description
1	General Settings		
		Viewer Type	This enables you to choose the viewer you want to use to view the computer that you access remotely. You can choose either an ActiveX viewer or a Java viewer.
		Notify users upon sharing	Use this option when you want to notify your users that the administrator has connected remotely to their computer.
		Disable Wallpaper during Remote Connection	Use this option to disable the wallpaper (set by the user) during a remote connection.
		Disable Aero Theme during Remote Connection	Use this option to disable the Aero theme during a remote connection. This is only applicable for computers that have the Microsoft Windows Vista operating system (and later versions) installed in them.
		Log the reason for remote connection	Use this option to ensure that the administrator enters a reason while connecting remotely to a computer.
		Blacken the monitor of the client	Use this option to blacken the monitor of the user during a remote connection. This ensures that the

S.No.	Section	Option	Description
		computer during remote connection	user does not see the changes that are made by the administrator.
		Lock the keyboard and the mouse of the client computer during remote administration	Use this option when you want to take full control of the user's computer to complete a task.
2	Port Settings	Use secure connection	This ensures that you use a secure connection when connecting to a user's computer remotely
3	Compression Settings	Fast	Use this option, when you want the rendering to be faster. The compression ratio will be lower and will consume higher bandwidth comparatively.
		Best	Use this option, when you want to optimize bandwidth utilization. The compression ratio will be higher and the User Interface (UI) rendering will be comparatively slower.
4	Prompt Settings	Enable Prompt	This option allows you to get confirmation from a user before connecting to their computer. Only Desktop Central users with administrative privileges can configure this option. If a user is logged in, Desktop Central sends a remote-connection confirmation request for the user's approval. Remote connection is established only if the user approves the request within 30 seconds. If the user does not approve the request within 30 seconds, the remote connection is not established automatically. If a user is not logged in, the remote connection is established without waiting for a confirmation from the

S.No.	Section	Option	Description
			user.
		Time out (in seconds)	Use this option to set the amount of time you want to give the user to approve the request to allow a remote connection.
		Prompt Message	Enter the text that you want the user to see when prompted for confirmation to allow remote control.

To configure remote computer settings, follow the steps given below:

You must have administrator privileges to make the settings given below.

1. Click the **Tools** tab
2. Click **Remote Control**
3. Click the **Settings** tab
4. In the **General Settings** section, make the following settings:
5. Select the type of viewer

The viewer you choose will be the default option for all the users and they can change it if required.

6. Check the required checkboxes
7. In the **Port Settings** section, check the **Use Secure Connection** checkbox
8. Enter 8444 and 8021 in the **Gateway Port** and **File Transfer Port** boxes, respectively

The port numbers that you specify should be opened in the firewall of the computer where the Desktop Central server is installed.

9. In the **Compression settings** section, check the required options
10. Click **Save Changes**

You have configured the remote computer settings as required.

Remote Desktop Sharing: Configuring Settings

You are required to configure the following settings before you connect to a remote computer:

1. General settings
2. User-confirmation settings
3. Screen Recording Settings
4. Performance settings

General Settings

You can make general settings using the Settings tab to enable the option to:

1. Select the type of viewer you want to use to view the computer that you will access remotely. You can choose either an ActiveX viewer or a Java viewer.
2. Notify users that you have connected remotely to their computer.
3. Disable the wallpaper set by the user during a remote connection.
4. Disable the Aero theme during a remote connection. This is only applicable for computers that have the Microsoft Windows Vista operating system, and later versions, installed in them.
5. Ensure that a reason is entered while connecting remotely to a computer.
6. Blacken the user's monitor during a remote connection. This ensures that the user does not see the changes that are made by the administrator.
7. Lock the keyboard and the mouse of the client computer during remote administration. You can use this option when you want to take full control of the user's computer to complete a task.
8. Capture alpha-blending. This enables you to capture transparent windows.
9. View-only mode. You can only view remote computers using this mode. You cannot give any inputs or make changes in the computer that you are viewing. You are required to disable the following options to use the view-only mode:
    1. Notify users upon sharing
    2. Blacken the monitor of the client computer during a remote connection
    3. Lock the keyboard and mouse of the client computer during a remote connection
    4. Capture alpha-blending
    5. User confirmation

    Using Other Settings While Using the View-only Mode

    This section comprises information about how other settings will work when the view-only mode has been enabled:

1. If you want to view a computer silently, ensure that all the other options like locking a keyboard, capture alpha-blending, notifying a user and user confirmation are disabled.
2. If the **Make User Confirmation Permanent** option is enabled, the view-only mode option will be disabled automatically.

Configuring General Settings

To configure remote computer settings, follow the steps given below:

You must have administrator privileges to make the settings given below.

1. Click the **Tools** tab
2. Click **Remote Control**
3. Click the **Settings** tab
4. In the **General Settings** section, make the following settings:
5. Select the type of viewer

The viewer you choose will be the default option for all the users and they can change it if required.

6. Check the required checkboxes
7. Click **Save Changes**

You have configured the general settings.

User-confirmation Settings

You can send users a message asking for permission to connect remotely to their computers. This option allows you to get confirmation from a user before connecting to their computer. Only Desktop Central users with administrative privileges can configure this option.

If a user is logged in, Desktop Central sends a remote-connection confirmation request for the user's approval. Remote connection is established only if the user approves the request within 30 seconds. If the user does not approve the request within 30 seconds, the remote connection is not established automatically.

If a user is not logged in, the remote connection is established without waiting for a confirmation from the user.

You can also do the following:

1. Set the amount of time you want to give the user to approve the request to allow a remote connection
2. Enter the text that you want the user to see when prompted for confirmation to allow remote control
3. Check the **Always Prompt** checkbox to send a user-confirmation message to users even if they have logged off or in locked state
4. Exclude computers from receiving a user-confirmation message

Making User Confirmation Permanent

One of the prerequisites required to comply with HIPAA is to protect user privacy. Therefore, it is mandatory to get the approval of users before connecting remotely to their computers. Making user confirmation permanent will ensure that you always get the user's consent before establishing a remote connection.

If you choose to make user confirmation permanent you cannot revert the settings.

Using Other Settings After Making User Confirmation Permanent

This section comprises information about how other settings like Always Prompt and Exclude Computers will work when user confirmation has been made permanent.

1. If you enable the **Make User Confirmation Permanent** option. All the computers in your network will receive a user-confirmation message before a remote connection is established.
2. If you check the **Exclude Computers** checkbox after you have enabled the **Make User Confirmation Permanent** option, the following actions will take place:
    1. All computers in your network will receive a user-confirmation message
    2. Computers in the **Exclude Computers** list will not receive a user-confirmation message
3. If you check the **Always Prompt** checkbox after you have enabled the **Make User Confirmation Permanent** option, the following actions will take place:
    1. All computers in your network will receive a user-confirmation message
    2. Computers that are locked and users that have logged off will receive a user-confirmation message
4. If you check both the **Always Prompt** and **Exclude Computers** checkbox after you have enabled the **Make User Confirmation Permanent** option, the following actions will take place:
    1. All computers in your network will receive a user-confirmation message
    2. Computers in the **Exclude Computers** list will not receive a user-confirmation message
    3. Computers that are locked and users that have logged off will receive a user-confirmation message

Steps

This section comprises steps required to do the following:

1. Configure user-confirmation settings
2. Exclude computers from receiving a user-confirmation message before a remote connection is established

Configuring User-confirmation Settings

To configure user confirmation settings, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Control**
3. Click the **User Confirmation** tab
4. Check the **User Confirmation** checkbox

You can check the **Always Prompt** checkbox to send a user-confirmation message to users even if they have logged off or in locked state.

5. Enter the amount of time you want to give the user, to approve the request to allow a remote connection, in the **Time-out** box
6. Enter a customized message to display on the user's screen asking for approval for a remote connection, in the **Confirmation Message** box
7. Click **Save Changes**

You have configured the user confirmation settings.

Excluding Computers

You can also exclude computers from receiving a user-confirmation message. When you exclude computers from receiving user-confirmation messages, you can connect to them immediately, without an approval from the user.

If you have made the user-confirmation option permanent, check the **Exclude Computers** checkbox to ensure that the computers in the Exclude Computers list do not receive a user-confirmation message before a connection is established.

To exclude computers from receiving a user confirmation message requesting users to allow a remote connection, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Control**
3. Click the **User Confirmation** tab
4. In the **Exclude Computers** section, click **Add Computers**

5. Filter computers as required. For example, you can filter the computers by domain
6. Select the computers that should not receive a confirmation message before you connect remotely to them
7. Click **OK**

These settings will be effective only when you check the User Confirmation checkbox.

Screen Recording Settings

Screen recording enables you to record the entire remote control session that can be used for auditing purposes. Given below are the operation performed when you have enabled screen recording:

1. When you connect to a computer, the Desktop Central Agent on the computer to which you connect will check for the available hard disk space for saving the video.
2. If sufficient space is available, the session and recording will start and a notification will be displayed on the client computer that this session is being recorded (configurable)
3. After the session is completed, the recorded video is uploaded to the Desktop Central Server. The recorded video is available under the History tab available within the Remote Control tool.

To enable and configure Screen Recording, follow the steps below:

1. Click the **Tools** tab
2. Click **Remote Control**
3. Select the **Screen Recording** tab
4. Select the "Enable Screen Recording" check box and specify the following
    1. Select the required Codec that have to be used for compression and decompression of the video. If the selected Codec is not available on the remote computer, the default codec will be used.
    2. Chose the Frames per Second. The higher the frames per second will give you a smooth mouse movements, while it also increases the size of the video. If it is just for auditing purposes, it is better to leave it with the default value.
    3. Choose the required color quality. Higher the color quality will gives broader range of color depth, but also increases the size of the video.
    4. Specify the maximum storage size for the recorded videos. When the storage limit exceeds, the previously recorded files are automatically deleted to free the space.
    5. Specify what should be done when there is no enough space on the remote computer when the session is in progress. You can either choose to stop the recording and continue with the session or disconnect the session.
    6. If you wish to notify the users that the remote control session is being recorded, select the "Enable User Notification" checkbox and specify the message and notification duration. If you want the notification be permanently displayed throughout the session, select "Always show a notification when recording is in progress" option.

Performance Settings

You can configure the following performance settings to increase the performance of remote connectivity:

1. **Compression Settings**

   Compression settings include the following options:

   1. Fast: Use this option, when you want the rendering to be faster. The compression ratio will be lower and will consume higher bandwidth comparatively.
   2. Best: Use this option, when you want to optimize bandwidth utilization. The compression ratio will be higher and the User Interface (UI) rendering will be comparatively slower.

1. **Color-quality Settings**

   Selecting an appropriate color-quality level enables you to use your bandwidth effectively during a remote session. Lowering the level of the color quality will decrease the consumption of your bandwidth. This will ensure effective bandwidth consumption.

Default Settings

The default settings for performance settings are as follows:

1. Compression Settings
   1. For LAN (local offices): Fast
   2. For WAN (remote offices):Best
2. Color Quality
   1. For LAN (local offices): High (16 bit)
   2. For WAN (remote offices):High (16 bit)

Configuring Performance Settings

To configure performance settings, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Control**
3. Click the **Performance** tab
4. Click  in the **Action** column against the name of the required computer
5. Select the required settings for the following from the dropdown boxes:

   1. Compression
   2. Color Quality

6. Click **Save**

You have configured the performance settings as required.

Connecting to Remote Desktop

Desktop Central's Remote Control feature enables administrators to access any computer in a Local Area Network (LAN) or a Wide Area Network.

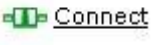
Ensure that you have completed these prerequisites and made the required settings before you connect remotely to a computer.

Using this feature you can do the following:

1. Connect remotely to computers
2. Transfer files between computers
3. Switch between multiple monitors during a remote session

Connecting Remotely to Computers

To connect remotely to computers, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Control**
3. Click 

You have connected remotely to a computer. You can use the **View Desktop** link to control the user's computer.

	When you are connecting to a remote desktop for the first time from a specific system, you must log in to the system with local administrative privileges. Subsequent connections from the same machine do not require this, as the necessary ActiveX controls and plug-ins would have got downloaded.

Transferring Files Between Computers

To transfer files to remote computers, follow the steps given below:

1. Click the **Tools** tab
2. In the **Windows Tools** section, click **Remote Control**
3. Click **Connect** against the name of a computer to connect remotely to it
4. On the top of the remote-connection screen, click **File Transfer**
5. Select the required file from a folder from your computer
6. Click  to transfer it to a folder in the remote computer

You have transferred files to a remote computer.

Switching Between Multiple Monitors

When you establish a remote connection, Desktop Central automatically detects the monitors are available and displays this information on the ActiveX tool bar. You can choose the monitor that you want to view and can switch between the available monitors whenever you want, during the session.

To switch between multiple monitors during a remote session, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Control**
3. On the **Computers** tab, in the **Viewer** section, select Active X.

	Only the Active X viewer supports viewing multiple monitors during a remote session.

4. In the **Action** column, against the computer that you want to connect to, click Connect
5. Click **View Desktop**

	When Desktop Central detects multiple monitors, it automatically adds an icon on the toolbar, which enables you to switch between multiple monitors. It is known as the Multi Monitor icon. The primary monitor gets displayed by default.

6. Click the Multi Monitor icon to switch between monitors

You can now switch between multiple monitors during a remote session.

Controlling a Remote Computer

After establishing connection with a remote desktop, you can complete the same tasks that you do from any computer. For example, you can create and deploy a configuration. You can use the toolbar to complete the following tasks:

Toolbar Icon	Action
	Send a Ctrl+Alt+Delete message to a remote computer
	Refresh the current view. If the computer is locked or no user has logged on, you are required to login
	Switch between different applications in the remote computer
	Black out a user's monitor so that the user cannot view the tasks that you

Toolbar Icon	Action
	are completing on the the remote computer
	Lock a user's keyboard and mouse
	Unlock a user's keyboard and mouse
	Gain control to access a user's computer
	Give the control back to the user
	Zoom in
	Zoom out
	Reset a view to its original size
	Reset the size of the view so that it fits onto the screen
	View a remote desktop in full screen mode

Read about known issues and limitations related to sharing desktops remotely,here.

Auditing Remote Access Details

Whenever a user establishes a remote connection using Desktop Central, all the events performed on the remote computer are logged. Clicking the  icon available beside the computer name will list all the remote access made to that computer with the details of the user and the start/end time.

You can also view the history of all the remote connections that have been established, using Desktop Central, in the History tab. The details that you can view are as follows:

1. Date on which the connection was made
2. User name of the user who made the connection
3. Name of the computer which was accessed
4. Time at which the connection was made
5. Duration for which the connection lasted
6. IP address of the viewer
7. Name of the domain from which the viewer logged on

File Transfer

Desktop Central allows you to remotely access desktops and transfer files between them.The Remote Desktop Sharing mechanism supports remote login to any desktop in your network by any user account that has Remote Control privileges. Files can be transffered between computers via the Active-X Viewer only. Java viewer is not supported at the moment.

File Transfer - Advantages

1. Files can be transferred between both the machines viz.,the one initiating the Remote Control Session and that which is getting connected with.
2. Ability to transfer files across domains and workgroup machines.
3. The entire process is Fast, Reliable, and Secure.

File Transfer Ports

The following are the list of ports that need to opened in the Desktop Central Server to enable File Transfer:

For Secure Mode:

- Gateway Port : 8047
- File Transfer Port : 8053

For Non Secure Mode

- Gateway Port: 8048
- File Transfer Port: 8054

Note: The default mode is Secure mode. However to select non-secure mode, click on the *Edit Settings* link in the *Remote Control* page and simply uncheck the "Use Secure Connection" checkbox under the *Port Settings* of *Remote Control Settings* page.

Follow the links to learn more:

- Pre-requisites
- Connecting to Remote Desktop
- Troubleshooting Tips

Troubleshooting Tips

1. I was able to connect to a desktop from remote, but nothing is visible?

Please check the following:

- Whether you have enabled ActiveX controls in the browser from where a connection is established. Refer to the Pre-requisites topic for details on configuration.
- If you are connecting to a desktop for the first time, log in to the system as a local administrator and connect. Subsequent connections from the same machine do not require administrative privileges as the necessary ActiveX controls and plug-ins would have got downloaded.

2. I am getting an "Access Denied" error when I try to connect to a remote desktop.

This error message is shown when the supplied credentials while defining the Scope of Management (SoM) is invalid or changed.

3. On connecting to a remote desktop, "The specified service does not exist as an installed service" error is shown.

This error message is shown when the Desktop Central Agent is not installed properly in the client machine. To reinstall the agent, follow the steps below:

1. Click the SoM link from the Quick Links.
2. Select the machines in which the agent needs to be re-installed and click **Install Agent**.

4. When I select a desktop from the list, the status is always shown as not available, though the system is up.

This happens when the client machine has firewall enabled with the "Don't Allow Exceptions" option selected. Disable the firewall to connect to that machine from remote.

5. I am getting an "The system cannot find the file specified" error when I try to connect to a remote desktop.

This error message is shown when one of the required files has been deleted from the client machine. Reinstall the agent as given below:

1. Click the SoM link from the Quick Links.
2. Select the machines in which the agent needs to be re-installed and click **Install Agent**.

6.I was able to connect to a remote Desktop. But, the display is not proper.

Try by changing the screen resolution using the Zoom in / Zoom Out icons.

Wake on LAN

The Wake on LAN Tool of Desktop Central helps to schedule booting of systems in the Windows Network remotely. It allows you to create different task to group the computers and specify a time to boot the machines in that task.

Creating and Scheduling Wake on LAN Tasks

To create a Wake on LAN task, follow the steps below:

Step 1: Define Task

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the network machines.
2. Click the Wake on LAN tool listed under the Windows Tools category to open the task details page. This will list all the Wake on LAN tasks that have been created.
3. Click the Schedule Wake Up button to create a new task and specify the following:
    1. Provide a name of the task
    2. Choose the speed for the Wake on LAN task. Depending upon the selected speed, Desktop Central allocates more threads to complete the task.
    3. Waiting time after wake up: Specify the time in minutes after which the status gets updated in the Desktop Central client.
    4. Verify the computers already powered up before waking up: Select this option, if you wish to check the status before attempting to boot the machine.
    5. Use broadcast to wake up computers: Desktop Central supports sending both unicast and broadcast packets to boot the machines. When this option is not selected, Desktop Central first sends an unicast WOL packet to the machine to boot and check whether the machine is booted. If this fails, it broadcasts the WOL packet in the whole subnet.
    6. Resolve IP Address on each schedule: Select this option to resolve the IP Addresses of the machines during every schedule.

Step 2: Select Computers

1. Click Add Computers button to choose the computers for this task. The selected computers gets added to the table below.
2. Broadcasting of the WOL packtes is based on the subnet address of the computers. If the subnet address is blank of if it is incorrect, the task may fail. You can either click the icon and update the subnet address and MAC Address manually for individual computers ate select the computers in the same subnet and use the Set Subnet Address button to update the Subnet Address of multiple computers.

Step 3: Define Scheduler

1. *Once:* To run the task only once. You need to specify the date and time.
2. *Daily:* To run the task daily. Specify the time and duration to run the task.
3. *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run.
4. *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months.

Step 4: Deploy Task

Click the **Submit** button to deploy this task. The tasks will be run at the scheduled time and interval. The status of the tasks and its execution history can be verified from the Task Details page.

Viewing and Modifying Wake on LAN Tasks

To view the Wake on LAN tasks that have been created, follow the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the computers.
2. Click the Wake on LAN tool listed under the Windows Tools category to open the task details page. This lists all the tasks that are already created and scheduled.
3. To modify a task,
    1. Click the icon from the Actions column of the corresponding task.
    2. This opens the Modify task page. You can add/remove computers, change the task options, and the scheduled time as required.
    3. Click **Submit** to effect the changes.
4. To Delete a task, click the icon from the Actions column of the corresponding task.

Viewing Wake on LAN Task Status

To View the status of the Wake on LAN tasks that have ben created, follow the steps below:

1. Select the Tools tab from the Desktop Central client. This opens the list of tools that can be run on the computers.
2. Click the Wake on LAN tool listed under the Windows Tools category to open the task details page. This lists all the tasks that are already created and scheduled.
3. Click the Task name to view the status of the computers in that task.
4. You can filter to view the details of the computers by status like Scheduled, Processing, Success, and Failed.

Configuring Wake on LAN

BIOS Settings

The Wake-On-LAN functionality is generally disabled by default. The option to enable Wake-On-LAN is different with each computer manufacturer. The most common method adopted across different PC's are as follows:

1. During the computer's power-on self-test enter the BIOS setting screen by pressing the F1, INS, or DEL keys.
2. Select **Power** settings. Check for **Power Up Control**.
3. Enable settings related to Power Up on PCI card, LAN, or Network.
4. Click **Save** and exit the BIOS settings.

Operating System (OS) Settings

In some Windows OS, the drivers can enable the Wake ON LAN features of network adapters. For example in Windows 2000, click Power Management tab and under the **Adapters** properties, select the option **Allow this device to bring the computer out of standby**.

Alternatively, you can also check the **Advanced** setting table for parameters related to Wake on LAN and Waking on "Magic Packets" and enable them.

Wake-On-LAN (WOL) Cable

For Wake On LAN to work on computers with older PCI busses, a WOL cable must be installed between the Network Card and the Motherboard. Because this requires opening the computer case, we advice you to contact your PC manufacturer for specific instructions.

Enabling Directed Broadcasts on your Network

To send WOL packets from remote networks, the routers must be configured to allow directed broadcasts. To know if the IP broadcast packets have been disabled, check for the line "no ip directed-broadcast" in the interface configuration. If IP broadcasts are enabled, the line "no ip directed-broadcast" will not be present.

Remote Shutdown Tool

The Remote Shutdown tool of Desktop Central provides options to shutdown, restart, lock and hibernate systems remotely. You can complete the following tasks, manually, using this tool:

- Add computers to shutdown or restart
- Understand and use various shutdown options
- Complete the following supported operations
- View the status of operations

You can also schedule the automatic completion of the tasks mentioned above.

Completing Tasks Manually

You can complete the following tasks manually using Desktop Central. You can do this by using the **Shutdown Now** tab.

Adding Computers to Shutdown or Restart

You are required to add computers on the Remote Shutdown page to shutdown or restart remotely. Before adding systems to shutdown or restart, ensure that you have specified common credentials, in all systems, to complete these tasks. To specify credentials, visit the Add Computers page.

To add computers to shutdown or restart, follow the steps below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Click **Add Computers**
4. Against **Select Type**, choose **Computer**
5. Select a domain or workgroup to view the computers in it
6. Select the required computers to add
7. Click **OK**

Note: Repeat steps 5 and 6 to add computers from other domains or workgroups.

The selected computers are listed under **Computer Name** in the **Shutdown Now** tab.

To remove computers from the Shutdown Now tab, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. Click **Remove Computers**

The selected computers are removed from the **Shutdown Now** tab.

Shutdown Options

When you want to shutdown a computer, you are required to specify the following options for shutting down:

- **Shutdown Mode**

Choose one of the following options:

- Normal: Use this option to close all the applications, as they would close normally, before shutting down computers
- Forced: Use this option to close all the applications forcibly, before shutting down the computers. You can also use this option when applications are running in the background and you want to shutdown the computer immediately.
- **Timeout**

Use this option to specify the time in seconds to display a warning message in all the client computers before shutting down. Specify zero to skip the message and shutdown immediately

- **Shutdown Message**

Enter a message in the field provided. This message will be displayed in all the computers before they are shutdown.

Supported Operations

You can complete the following tasks on a remote computer:

Shutting down a computer

To shut down a computer, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. Click **Shutdown Now**
5. Specify the required settings
6. Click **Shutdown**

You've successfully shut down the selected computers.

Restarting a computer

To restart a computer, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. Click **Restart Now**
5. Specify the required settings
6. Click **Restart**

You've successfully restarted the selected computers.

Setting a computer in Hibernate mode

To set a remote computer in Hibernate mode, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. From the **More Actions** list, select **Hibernate**
5. Click **Yes**

You have successfully set the selected computers in Hibernate mode.

Setting a computer to Stand by mode

To set a remote computer to Stand by mode, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. From the **More Actions** list, select **Stand by**
5. Click **Yes**

You have successfully set the selected computers to Stand by mode.

Locking a computer

To lock a computer, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. From the **More Actions** list, select **Lock Computers**
5. Click **Yes**

You have successfully locked the selected computers.

Scheduling Automatic Tasks

You can complete the following tasks automatically using Desktop Central. You can do this by using the **Schedule Shutdown** tab.

Creating and Scheduling Tasks

You can create and schedule various tasks. To create and schedule a shutdown task, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Click the **Schedule Shutdown** tab
4. Click **Add Shutdown Task**
5. Enter a name for the task
6. From the **Operation** section, select the required type of task
7. Select the **Shutdown/Restart Options**, if applicable

Note: These options are available only if you select Shutdown or Restart.

8. Select the required computers
9. Schedule when you want the task to take place:

- **Once**: Use this option if you want the task to take place only once. Specify a start time and start date.
- **Daily**: Use this option if you want the task to take place everyday. Specify whether the task should take place on all days or only on weekdays.
- **Weekly**: Use this option if you want the task to take place on a weekly basis. Specify a start time and the required days of the week.
- **Monthly**: Use this option if you want the task to take place on a monthly basis. Specify the start time, when you want this task to take place (for example, first Sunday or the day), and months in which you want this task to take place.

10. Click **Save Task**
11. Select the required task
12. In the **Action** column, select **Execute Now**

You have created and deployed a task using the **Schedule Shutdown** tab

Windows Configurations

Desktop Central enable remote configurations that can be applied to users and computers of the Windows domain-based network. The following sections guides you in configuring various Windows applications, security settings, display settings, firewall settings, and so on, to the Windows users and computers:

- User Configurations: Explains the various configurations that can be deployed to users using Desktop Central and the steps to define them.
- Computer Configurations: Explains the various configurations that can be deployed to computers using Desktop Central and the steps to define them.
- Configuring Collections: Helps you to define a collection configurations that can be deployed simultaneously for several users or computers.
- Defining Targets: Provides you the details of defining target computers and users for deploying the configuration.
- Managing Configurations and Collections: Helps you to manage the defined configurations, such as viewing the status of the defined configurations or collections, suspending the deployment, resuming the suspended deployments, and so on.
- Viewing Configuration Reports: Detailed report on the defined and deployed configurations using Desktop Central along with its status.
- Viewing System Uptime Reports: Provides the details of uptime and downtime of computers in the specified period.

How the Configurations gets Applied

Whenever a configuration is deployed using Desktop Central, it will be made available to the Desktop Central agents to apply the configurations in the client computers. The Desktop Central Agents residing at the client computers will pull the configuration details from the Server and process them. The Desktop Central agents will contact the Server at the following intervals to pull the details:

1. For user-specific configurations - during user logon and every 90 minutes thereafter till the user logs out of the domain.
2. For computer-specific configurations - during system startup and every 90 minutes thereafter till the system is shutdown.

User Configurations

This section details the configurations that can be applied to the users of the Windows Domain. These configurations are applied to the users during user logon or logoff.

Note: Ensure that you have defined the scope of management before defining the configurations. For details, refer to Defining the Scope of Management.

To reach the configuration screen, follow the steps below:

1. Click **Add Configuration** link from the Quick Links. This will list all the supported configurations for users and computers.
2. Click the required configuration listed under the User Configurations.

Desktop Central supports the following configurations that can be applied on users:

- Configuring Alerts
- Executing Custom Scrips
- Configuring Display Settings
- Mapping Network Drives
- Setting Environment Variables
- Managing Files and Folders
- Redirecting User-Specific Folders
- Configuring Internet Explorer Settings
- Configuring IP Printer
- Launching Applications
- Displaying Message Box
- Configuring MS Office Settings
- Configuring Outlook Settings
- Setting Path
- Managing Permissions
- Configuring Power Options
- Configuring Registry Settings
- Securing USB Devices
- Configuring Security Policies
- Configuring Shared Network Printer
- Managing Shortcuts
- Installing Software - MSI/EXE Format

Configuring Alerts

Alert Configuration enables you to warn the users about the password expiration, lower hard disk space, and larger temp file size. The alert configuration are user-specific and requires the user to be logged on to view the alerts.

Step 1: Name the Configuration

Provide a name and description for the Alert Configuration.

Step 2: Define Configuration

The table given below lists the parameters for which alerts can be configured:

Parameter	Description
Password Expiration	The number of days before which the user has to be informed about the password expiration. The default value is 14 days.
Disk Space	The disk space in MB. When the disk space goes below the specified value the user will be warned.
Purge Temp Files	Specify whether to delete the temp files when exceeding the specified limit. You also have an option to specify the file types, size of the files, and whether to prompt the user before deleting the temp files or not.

Note: The alerts will be displayed during every logon of the user as long as the alert condition is met. For example, the user will be warned about the lower disk space during every logon until the free disk space exceeds the specified value.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Alert Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Alert Configuration in the targets defined. The alerts will be displayed when the defined conditions are met.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Executing Custom Scripts

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

Desktop Central provides options for configuring almost all the user configurations from remote. In addition to the configurations that are supported by Desktop Central, administrators can also write their own scripts that could be run on the user machines for accomplishing specific configurations. The scripts could be any of the following:

- Batch file (.bat or .cmd)
- In any other language hosted by Windows Script Host (WSH), such as VB Script, JScript, Perl, REXX, and Python.

Note: The script engines for languages like Perl, REXX, and Python, must be registered with Windows.

Step 1: Name the Configuration

Provide a name and description for the custom script configuration.

Step 2: Define Configuration

The table given below lists the parameters that have to be provided for defining the configuration.

Parameter	Description
Script Name*	The script that has to be executed in the user machines. You have an option to select the script from any of the following: **Local**: The machine from where the configuration is being defined. **Inventory**: Refers to the Desktop Central inventory. All the scripts that have been added using Managing Scripts procedure will be available here. **Network Share**: Refers to the network share.

Parameter	Description
Script Arguments	The arguments that have to be provided while executing the scripts.
Execute During*	Refers to the script execution time. This can be either during the user **logon** or **logoff**.

* - Refers to the mandatory fields.

Note: The scripts specified from the **local** or **share**, will automatically be added to the Desktop Central inventory after successful deployment.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Custom Script Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Custom Script Configuration in the targets defined.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Managing Custom Scripts, Viewing Configuration Reports, Defining Targets

Configuring Display Settings

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Display Configuration is for configuring the settings of Microsoft Windows Desktop such as welcome message, IntelliMouse tips, icons, folders and shortcuts, wallpaper, etc.

Step 1: Name the Configuration

Provide a name and description for the configuration.

Step 2: Define Configuration

The table below lists the display settings that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
Wall Paper File	The wallpaper file (image file) that has to set as the desktop background. The wallpaper can be set from either local computer or from a network share by selecting the appropriate option. For wall papers that are set locally all the target computers should have the file in the same location. When choosing a file from network share, you can click the ☆ icon to select and assign a dynamic variable to this parameter.
Rename "My Computer" Icon	The name you wish to configure in place of "My Computer". Click the ☆ icon to select and assign a dynamic variable to this parameter.
Rename "My Network Places" Icon	The name you wish to have in place of "My Network Places". Click the ☆ icon to select and assign a dynamic variable to this parameter.
Remove "Windows Welcome Screen"	Select this option if you wish to remove the welcome message displayed by Windows.
Remove "Intellimouse	Select this option to remove the intellimouse tips.

Parameter	Description
Tips Screen"	
Remove "My Documents" Desktop Icon	Select this option to remove the "My Documents" icon from the desktop.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Display Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Display Configuration in the targets defined.

The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Mapping Network Drives

The Drive Mapping configuration enables you to map a remote network resource to the user machines. The mapped resource can then be accessed from the local machine using the drive name.

Step 1: Name the Configuration

Provide a name and description for the Drive Mapping configuration.

Step 2: Define Configuration

The table given below list the parameters that have to be specified for mapping a network drive:

Parameter	Description
Drive Name	The drive letter that has to be mapped with the resource.
Resource to be Shared	The shared resource in the network that has to be mapped.
Hide from Windows Explorer	To specify whether the mapping has to be hidden in the Windows Explorer. Select this option, if you want to hide.
Drive Label	The label name for the mapped drive that has to displayed in Windows Explorer.
Disconnect all existing network drives before mapping new	Specify whether to disconnect all the existing mappings or not.

Note:

1. To map more network drives, click **Add More Drives** and repeat Step 2. The mapped drive gets added to the **List of Drives to be Mapped** table.
2. To modify a mapping from this table, select the appropriate row, click icon and change the required values.
3. To delete a mapping from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Drive Mapping Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Drive Mapping Configuration in the targets defined. The configurations will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Setting Environment Variables

Environment variables are strings that contain information about the environment for the system, and the currently logged on user. Some software programs use the information to determine where to place files (such as temp, tmp, path etc). Environment variables control the behavior of various programs. Any user can add, modify, or remove a user environment variable. However, only an administrator can add, modify, or remove a system environment variable. Using Desktop Central, the environment variables can be defined and added.

Step 1: Name the Configuration

Provide a name and description for the Environment Variable configuration.

Step 2: Define Configuration

The following table lists the parameters that have to be specified**:**

Parameter	Description
Variable*	The environment variable name that has to be modified or added.
Value*	The value that has to be stored in the environment variable. Click the icon to select and assign a dynamic variable to this parameter.

* - denotes mandatory fields

Note:

1. To add more environment variables, click **Add More Variable** and repeat Step 2. The defined environment variable gets added to the **List of Environment Variable** table.
2. To modify a environment variable from this table, select the appropriate row, click icon and change the required values.
3. To delete a environment variable from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Environment Variable Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Environment Variable Configuration in the targets defined. The configurations will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Setting Path

Managing Files and Folders

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The File and Folder Operation allows you to copy, move, rename, delete files and folders of the users. Desktop Central File and Folder Operation Configuration enables you to copy/move/delete files for several users from central location.

Step 1: Name the Configuration

Provide a name and description for the File and Folder Operation configuration.

Step 2: Define Configuration

You can perform the following actions:

- Copy Files and Folders
- Rename/Move Files and Folders
- Delete Files and Folders

Copy Files and Folder

To copy files and folders, select the *Copy* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: *Copy a File* - To copy a file from one location to another *Copy a File to a Folder* - To copy a file from one location to a specified folder *Copy Multiple Files* - To copy multiple files to a specified folder *Copy a Folder* - To copy a folder from one location to another

Parameter	Description
Source File	Specify the file that has to be copied. The file can either be in a shared location or in the specified location in the client machines.
Destination File	Specify the destination location with the file name.
Destination Folder	Specify the destination folder to copy the files/folders.
Include Read Only Files	Select this option, if you wish to copy the files even if it has only read-only permissions
Include System Files	Select this option if you wish to copy the system files.
Include Hidden Files	Select this option if you wish to copy the hidden files.
Overwrite Existing Files	Select this option to overwrite the existing files.
Create Destination Directory if doesn't Exist	Select this option to create the destination directory, if it does not exist.
Include Sub Folders	Select this option, if you wish to copy sub folders or the files within the sub folders.
Continue on Error	While copying multiple files or folders, specify whether to continue, if any error is encountered while copying.
Choose file modification time	Specify the file or folder modification time. Files that meet the specified criteria will only be copied.
Connect using Credentials	To copy Files/Folders across Domains or amongst Workgroup computers, you need to specify a credential that has access to the source Files/Folders.

Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Rename / Move Files and Folders

To rename or move the files and folders, select the *Rename/Move* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: Rename/Move a file Rename/Move a folder
Source File/Folder	Specify the file or the folder that has to be copied
Destination File/Folder	Specify the destination file or the folder.

Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Delete Files and Folders

To delete the files and folders, select the *Delete* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: Delete a File Delete Multiple Files Delete a Folder
Source File	Specify the files/folders that has to be deleted
Include Read Only Files	Select this option, if you wish to delete the read-only files
Include System Files	Select this option, if you wish to delete the system files
Include Hidden Files	Select this option, if you wish to delete the hidden files.
Include Sub Folders	Select this option, if you wish to delete the sub folders or the files within the sub folders.
Continue on Error	While deleting multiple files or folders, specify whether to continue, if any error is encountered while deleting.

	**Note**: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

To modify a file action from the **List of File Actions** table, select the appropriate row and click icon and change the required values.

To delete a file action from the **List of File Actions** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the File and Folder Operation Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined File and Folder Operation Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Redirecting User-Specific Folders

The Folder Redirection configuration helps you to change the location of the standard user profile directories to a different location in the network. So, when the user login from a different machine in the same domain, he/she will have access to his/her profiles.

Step 1: Name the Configuration

Provide a name and description for the Folder Redirection configuration.

Step 2: Define Configuration

You can perform the following actions:

- **Redirect the folders and copy the existing contents** - This redirects the user-specific folders from the local machine to a network share and copy the existing contents to the new location. You also have an option to exclude specific folders from being copied.
- **Redirect the folders without copying the contents** - This redirects the user-specific folders from the local machine to a network share without copying the existing contents.
- **Restore to default** - Will restore the settings to default (All folders will be pointed to the local machine).

Select the required options and specify the values for the following fields that require change in settings. For each of the fields in the following table, click the **Browse** button next to the corresponding field to launch **Network Browser** window. Select the folder location and click **OK** button. If this field is left blank, the corresponding folder settings is left unchanged.

The following table provides a brief description about the user-specific folders that can be redirected using Desktop Central.

User-specific Folder	Description
Start Menu*	Contains the shortcuts that appear in the start menu.
Programs Menu*	Contains the shortcuts that appear in the Programs group of the start menu.

User-specific Folder	Description
Startup Group*	Contains the shortcuts that appear in Start --> Programs --> Startup menu. This specifies the applications that should be started during the user logon.
Desktop*	Contains the shortcuts and files that appear in the user's desktop.
Favorites [IE Bookmarks]*	Contains the Internet Explorer bookmarks.
Personal [My Documents]*	Contains the personal documents of that user.
My Pictures*	Contains the personal pictures and images of that user.
Cookies*	Contains the cookies used by the Web sites/applications.
History*	Contains the bookmarks of the previously accessed sites.
Recent*	Contains the shortcuts of the recently accessed documents.
Temporary Internet Files*	The temporary Internet files are cached by Internet Explorer in this folder.
Send To*	Contains the shortcuts listed in the **Send To** sub-menu. The **Send To** sub-menu is displayed in the right-click menu of a file.
Exclude Folders	This option is available only when you choose to copy the existing contents. Specify the folders as comma separated that should not be copied.
Don't copy temporary internet files	This option is available only when you choose to copy the existing contents. Select this option if you do not wish to copy the temporary internet files.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Folder Redirection configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Folder Redirection Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.
See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Redirecting Common Folders

Installing Software - MSI & EXE Packages

The Software Installation configuration helps you to install MSI and EXE packages remotely to specific users of several computers of the Windows network from a central location.

Step 1: Name the Configuration

Provide a name and description for the Software Installation Configuration.

Step 2: Define Configuration

You have an option to install either an EXE or an MSI package

- Install MSI Package
- Install EXE Package

Install MSI Package

Select the Installer type as **MSI** and specify the following values:

Parameter	Description
MSI Package Name	This will list all the MSI packages that are available in the Software Repository. Select the MSI that has to be installed.
Operation Type	To specify how the installation should happen. Select any of the following options: *Install Completely:* Selecting this option will install the application automatically. *Advertise*: Selecting this option will notify the user about the availability of the software. Thy can choose whether to install the software or not. *Remove*: Selecting this option remove (uninstall) the

Parameter	Description
	application from the system
Run As	The user as whom the MSI has to be installed.
Password	Password for the user as whom the MSI has to be installed.
Copy	You have an option to copy the installables to the client machines before installing them. Select the required option: *None:* Selecting this option will not copy the installation files. *Copy file to client machines:* Will copy the exe or the msi file alone as specified in the software package to the client machines. *Copy folder to client machines:* Will copy the entire directory that has the installation file to the client machines. Copy option will be mandatory, when the network share requires a user credential to access and when you opt to install the software as a different user using the Run As option.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	Description
Schedule Time to Perform the Operation	Select his option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type & Installation / Uninstallation Option selected, but this will begin after the time specified here.

Specify the Deployment Settings for the software:

If you have defined Deployment Templates, you can load the Deployment Settings directly from a template by selecting the required template from the list.

Parameter	Description
Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after system startup: *During startup*: Select this option if the software has to be installed/uninstalled during computer startup. *After startup*: Select this option if the software has to be installed/uninstalled after the computer startup when the next GP update happens (within 90 minutes) *During or After Startup*: Either of the above, whichever is earlier
Install Between	If you want the installation to happen only between a specified time of a day, you can specify the Start and End time within which the deployment should begin. The Start Time can also be greater than the End time - in such cases the End time is assumed to be on the following day. For example, if you wish the deployment should happen between 10.00 PM and 4.00 AM, you can specify the Start Time as 22:00:00 and End Time as 04:00:00
Allow Users to Skip Deployment	Specify whether the use can skip the deployment at a later time by selecting the "Allow Users to Skip Deployment". When you do not select this option, the deployment will be forced and the user will not have any control on the deployment. When you allow users to skip deployment, you can also specify whether they can skip it as long as they wish or force deployment after a specific date.
Reboot Policy	*Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines.

Parameter	Description
	Force Shutdown when the user has logged in: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Install EXE Packages

Select the Installer type as **EXE** and specify the following values:

Parameter	Description
EXE Package Name	This will list all the EXE packages that are available in the Software Repository. Select the EXE that has to be installed.
Operation Type	To specify how the installation should happen. Select any of the following options: *Install Completely:* Selecting this option will install the application automatically. *Advertise*: Selecting this option will notify the user about the availability of the software. Thy can choose whether to install the software or not. *Remove*: Selecting this option remove (uninstall) the application from the system
Run As	The user as whom the EXE has to be installed.
Password	Password for the user as whom the EXE has to be installed.
Copy	You have an option to copy the installables to the client machines before installing them. Select the required option: *None:* Selecting this option will not copy the installation files. *Copy file to client machines:* Will copy the exe or the

Parameter	Description
	msi file alone as specified in the software package to the client machines. *Copy folder to client machines:* Will copy the entire directory that has the installation file to the client machines. Copy option will be mandatory, when the network share requires a user credential to access and when you opt to install the software as a different user using the Run As option.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	Description
Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after user login: *During Login*: Select this option if the software has to be installed/uninstalled during the user login. *After Login*: Select this option if the software has to be installed/uninstalled after the user login but within 90 minutes. *During or After Login*: Either of the above, whichever is earlier
Schedule Time to Perform the Operation	Select his option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type selected, but this will begin after the time specified here.
Reboot Policy	*Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. *Force Reboot when the user has logged in*: Select this

	option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Windows Installer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Windows Installer Configuration in the defined targets. The software installation for the selected targets will happen as scheduled.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Internet Explorer Settings

The Internet Explorer settings such as Home page, Search page, Download directory, and Proxy Server settings can be configured using Desktop Central Internet Explorer Configuration.

Step 1: Name the Configuration

Provide a name and description for the Internet Explorer configuration.

Step 2 Define Configuration

The following table provides the Internet Explorer parameters that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
Home Page	Refers to the page that opens when the Internet Explorer is started.
Search Page	Refers to the search engine that Internet Explorer uses when clicked on the Search button from the toolbar.
Download Directory	Refers to the location where the file downloads are redirected. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Automatic Configuration Script	Refers to the URL of the script that is used to configure the proxy settings of Internet Explorer.
Internet Connection Wizard	The Internet Connection Wizard is invoked when a user tries to launch the Internet Explorer for the first time. Specify whether to remove or retain this.
Proxy Server	A proxy server is a server that acts as an intermediate between the computer in the network and the Internet, and that ensures security, administrative control, and caching. Select the appropriate proxy setting.

Parameter	Description
Address**	The IP address or host name of the Proxy Server.
Port**	The port number of the Proxy Server
Bypass for local addresses**	Specifies how the request has to be routed when a local address is accessed using the Internet Explorer. Select any of the following options: **Bypass proxy server:** Select this option if the request should not be routed through the proxy server for local addresses. **Dont Bypass proxy server:** Select this option if the request should be routed through the proxy server even for local addresses. **Preserve Client Settings:** To preserve the settings of the client untouched.
Do not use proxy server for addresses beginning with**	The list of addresses that begins with the text specified in this field will not use the Proxy Server. You can specify multiple values as semi-colon separated. Example: `adventnet.com;desktopcentral.com` This field is enabled only when Bypass Proxy server option is selected.

** - required only if **Use Proxy Server** option is selected.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Internet Explorer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Internet Explorer Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring IP Printer

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The IP Printer Configuration is for adding or deleting the IP Printer connection in the user computers. For configuring a shared printer in the computer for specific users, refer to the Configuring Shared Printer topic.

Step 1: Name the Configuration

Provide a name and description for the IP Printer configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add an IP Printer
- Delete an IP Printer

Add an IP Printer

To add an IP Printer, select the **Action** as *Add* and specify the following values:

Parameter	Description
DNS Name/IP	The host name or IP address defined for the printer. *Example*: `192.111.2.32`
Printer Name	The display name for the printer.
Protocol	The printing protocol supported by the printer. Select the printing protocol from the Protocol list box. The default option is "RAW".
Port Number	The port number/queue name in which printing protocol is communicating between the computer and printer. Enter the port number in the Port Number field

Parameter	Description
	if the "RAW" Protocol is selected or enter the queue name if the "LPR" Protocol is selected. The default value is 9100.
Port Name	This is an optional field. By default, the port name is IP_<IP_Address/DNS_Name>. You can change the port name if required.
Shared Printer for Driver Installation	Browse to select a shared printer for installing the driver. If the drivers are already installed in the target computers, this field can be left blank.
Set as default printer	Browse to select a shared printer for installing the driver. If the drivers are already installed in the target computers, the Desktop Central will skip the driver installation.
Connect Shared Printer using Credentials	To copy Driver Files across Domains or amongst Workgroup computers, you need to specify a credential that access domain/workgroup machine where the Shared Printer Driver Files are present.

Delete an IP Printer

To delete an IP Printer, select the **Action** as *Delete* and specify the following values:

Parameter	Description
Printer Name	The display name of the printer.
Delete all existing IP printer connections	To delete all the existing IP printer connections in the computer for the specified user, select this option.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the IP Printer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined IP Printer Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Configuring Shared Printer

Launching Applications

Launch Application configuration enables you to launch an application during user logon.

Step 1: Name the Configuration

Provide a name and description for the Launch Application configuration.

Step 2: Define Configuration

Select whether the application has to be launched from the local computer or from the network share. If you select the Local option, all the selected target computers should have the application in the same location. Specify the following:

Parameter	Description
Application Name	Browse and select the application that has to be launched. The applications that are available in the local machine from where the application has to be launched can also be specified. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Arguments	Specify the arguments for the application, if any. Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note:

1. To launch more applications, click **Add More Application** and repeat Step 2. The added application gets added to the **Launch Application** table.
2. To modify an application from this table, select the appropriate row, click icon and change the required values.
3. To delete an application from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Launch Application Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Launch Application Configuration in the targets defined. The applications configured will be launched during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Displaying Message Box

For the users in the network, the pop-up messages with the warning or error can be displayed during the user logon. If the user has already logged on while deploying this configuration, the message will be displayed during the next logon.

Step 1: Name the Configuration

Provide a name and description for the Message Box configuration.

Step 2: Define Configuration

You have an option to create a new message box or delete the existing message box. Select the required option and specify the following:

Parameter	Description
Message Type	The message type as Information, Warning, or error.
Window Title	The title of the message box.
Message	The message that has to be displayed.
Timeout in Seconds	The duration, in seconds, for the message display.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Message Boxes Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Message Boxes Configuration in the targets defined. The message will be displayed during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Displaying Legal Notices

Configuring MS Office Settings

The MS Office related settings such as Open or Save, Clip Art, User Options, Command Bars, Shared Template, etc can be configured for all the users using Desktop Central MS Office Configuration.

Step 1: Name the Configuration

Provide a name and description for the MS Office configuration.

Step 2: Define Configuration

The MS Office applications that can be configured using Desktop Central are listed in the Choose Application/Suite combo box. Select the application version and specify the values that have to be changed. Leave it blank, if no change is required.

The following table lists the parameters that can be configured for each MS Office applications:

Parameter	Description
Word	
Open/Save Folder*	Refers to the default working folder for Microsoft Word. Clicking Open or Save menu will open this folder location.
Clip Art Folder*	Refers to the default Clip Art folder. This opens when you insert an image from the clip art.
User Options Folder*	Refers to the folder where the user options are stored.
Tools Folder*	Refers to the folder where the office tools are stored.
Auto Recover Folder*	Refers to the folder where the recovered files are stored due to the system crash.
Startup Folder*	Refers to the location where the templates and add-ins are loaded during the startup of Microsoft Word.

Parameter	Description
Excel	
Open/Save Folder*	Refers to the default working folder for Microsoft Excel. Clicking Open or Save menu will open this folder location.
At startup, open all files in*	Refers to the folder containing the files that have to be opened during startup.
Access	
Open/Save Folder*	Refers to the default working folder for Microsoft Access. Clicking Open or Save menu will open this folder location.
Command Bars Folder*	Refers to the location where the command bar buttons of Microsoft Access are stored.
PowerPoint	
Open/Save Folder*	Refers to the default working folder for Microsoft Powerpoint. Clicking Open or Save menu will open this folder location.
Command Bars Folder*	Refers to the location where the command bar buttons of Microsoft Powerpoint are stored.
Office	
Template Folder*	Refers to the location where the Microsoft Office templates are stored.
Shared Template Folder*	Refers to the location where the shared Microsoft Office templates are stored.
Outlook	
Journal Item Log File*	Refers to the location where the old journal item file is stored.
Journal Outlook Item Log File*	Refers to the location where the old journal item file that is referred by the journal entry is stored.
Office Explorer Favorites Folder*	Refers to the default location for storing the favorites. Clicking the Add Favorites menu item will store the URLs in this location.
Office Explorer Views Folder*	Refers to the location where the user views are stored.
Print Settings File*	Refers to the file which stores the print styles of the user views.

* - Click the icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the MS Office Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined MS Office Configuration for the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Outlook Settings

Microsoft Outlook settings such as general settings, new mail arrival, automatic archive, sending a message, message format and handling, and spell check can be configured. The Outlook Configuration is used to configure these settings for the users of the network from a central location.

Step 1: Name the Configuration

Provide a name and description for the Outlook configuration.

Step 2: Define Configuration

The table given below lists the Outlook parameters that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
General Settings	
View Outlook Bar	To show or hide the Outlook shortcut bar when Outlook is opened.
View Folder List	To show or hide the folders listed when Outlook is opened.
Warn before deleting items	To enable or disable the warning message when deleting entries from the *Deleted Items* folder.
Startup in this Folder	The folder which must be opened after the Outlook is invoked. Select from the following options: *Outlook Today*, *Inbox*, *Calendar*, *Contacts*, *Tasks*, *Journal*, *Notes*, and *User-defined*. Select *User-defined* option to make the user configure this option.
Empty the Deleted Items folder upon exit	Select the frequency at which the contents of the *Deleted Items* folder should be cleared when exiting the Outlook. Select *User-defined* option to make the user configure this option.

Parameter	Description
New mail arrival	
Display a New mail Desktop Alert	To enable or disable the notification message when a new mail arrives.
Play a sound	To enable or disable playing sound when a new mail arrives.
AutoArchive	
Run AutoArchive	To enable or disable the automatic archiving of folder. Specify the required option and choose the frequency at which archiving should be done.
Prompt to AutoArchive	To specify whether to prompt before archiving or not.
Move old items to	The location where the archived files must be stored. Click the ☆ icon to select and assign a dynamic variable to this parameter.
File name	The name of the archived file.
Delete expired items (e-mail folders only)	To specify whether the expired items should be deleted or not.
When sending a message	
Allow comma as address separator	To specify whether comma should be used as a address separator or not.
Automatic name checking	To enable or disable automatic checking for the validity of names in the recipient list.
Message format & handling	
Compose in this Message Format	Select the message format as *HTML*, *Rich Text*, or *Plain Text*. Select User-defined to leave it to the user to configure.
Use Microsoft Word to edit email messages	Specify whether Word should be used as a default editor.
Send a copy of the pictures instead of the reference to their location (only for HTML format)	To specify whether to send pictures along with the mail or not.
Save copies in Sent items folder	To specify whether to save copies in the sent folder or not.
Autosave unsent	To specify whether to save the unsent messages or not. Select the frequency if you are enabling this option.
Spelling	

Parameter	Description
Always check spelling before sending	To specify whether to check spelling before sending the message or not.
Always suggest replacements for misspelled words	To specify whether to suggest replacement for misspelt words or not.
Ignore words in UPPERCASE	To enable or disable checking words in upper case letters.
Ignore words with numbers	To enable or disable checking words containing numbers.
Ignore original message in replies	To enable or disable checking the spelling of original mails in replies.

Step 3: Define Target

Using the Defining targets procedure, define the targets for deploying the Outlook Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Outlook Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Setting Path

For the users in the network, the paths which are configured and stored in the **Path** variable in the **Environment Variables** window (invoked by Right-click the **My Computer** icon, choose **Properties** > **Advanced** tab, click the **Environment Variables** button). The search paths including local paths, network paths or UNCs (Universal Naming Conventions). Using the Path Configuration, the path entries are added in the **Environment Variables** window for the users in the network.

Step 1: Name the Configuration

Provide a name and description for the Path configuration.

Step 2: Define Configuration

Specify the path to be added to the environment variables. Multiple paths can be specified separated by a semi-colon (**;**). Click the  icon to select and assign a dynamic variable to the Path variable.

Step 3: Define Target

Using the Defining targets procedure, define the targets for deploying the Path Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Path Configuration in the defined targets. The configurations will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Setting Environment Variables

Managing Permissions

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Permission Management allows you to grant revoke permission on the files, folders and registry for the users. Desktop Central Permission Management Configuration enables you to grant/revoke permissions to multiple users from a central point.

Step 1: Name the Configuration

Provide a name and description for the Permission Management configuration.

Step 2: Define Configuration

You can grant or revoke permissions for the following objects:

- Files
- Folders
- Registry

Files

To grant or revoke permissions for files, select the *File* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: Append - To append to the existing file permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object.

Parameter	Description
	Overwrite - To overwrite the existing file permissions Revoke - To revoke the existing file permissions of the specified user/group. All the permissions to the specified user/group on that file will be removed. However, the inherited permissions will not be removed.
Path	Specify the path of the file for which you need to specify permissions
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Folders

To grant or revoke permissions for folders, select the *Folder* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: Append - To append to the existing folder permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. Overwrite - To overwrite the existing folder permissions Revoke - To revoke the existing folder permissions. All the permissions to the specified user/group on that folder will be removed. However, the inherited permissions will not be removed.

Parameter	Description
Path	Specify the path of the folder for which you need to specify permissions
Inheritance	Select the required option to specify how the permission should effect its subfolders and files
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Registry

To grant or revoke permissions for registry, select the *Registry* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: Append - To append to the existing registry permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. Overwrite - To overwrite the existing registry permissions Revoke - To revoke the existing registry permissions. All the permissions to the specified user/group on that registry key will be removed. However, the inherited permissions will not be removed.
Hive	Select the registry hive from the given options
Key	Specify the key within that hive for which you need to set the permissions
Inheritance	Select the required options to specify how the permission should effect its subkeys.
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

To modify a permission from the **List of Permission Actions** table, select the appropriate row and click icon and change the required values.

To delete a permission from the **List of Permission Actions** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Permission Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Permission Management Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Power Options

The Power Management Configuration enables you to adjust your power settings to save energy. You can add, modify, and delete power schemes for users from a central point.

Step 1: Name the Configuration

Provide a name and description for the Power Management Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create/Modify a Power Scheme
- Delete a Power Scheme

Create / Modify a Power Scheme

To create a new scheme, select the **Create Scheme** tab of the Power Management Configuration. Select the **Modify Scheme** tab to modify an existing scheme. Specify the following values:

Parameter	Description
Power Scheme*	The name of the power scheme that has to be created/modified. If you are modifying a default scheme, select the Default Scheme option and select the scheme.
Overwrite if scheme already exits	Select this option to overwrite the scheme, if one with the same name exists. This option is only available for create scheme.
Set as active power scheme	Select this option if you wish to make this scheme active. Clearing this option will only create or modify the scheme and the system will continue to use the previously applied

Parameter	Description
	scheme.
Turn Off Monitor	Turns off the monitor after the specified period of inactivity. Select the period from the combo box.
Turn Off Hard Disk	Turns off the hard disk after the specified period of inactivity. Select the period from the combo box.
System StandBy	The system goes to the standby mode after the specified period of inactivity. Select the period from the combo box.
System Hibernate	Turns off the computer after saving everything in memory to the hard disk after the specified period of inactivity. When the system is turned on again, it is restored to the same position. Select the period from the combo box.
Advanced Options	
Enable Hibernate support	Select this option to enable hibernation of the computer.
Always show icon on the taskbar	Select this option to display the power icon in the system tray.
Prompt for password when computer goes off StandBy	Select this option, if you wish the user to authenticate himself/herself when the computer is resumed from standby mode.
When I close lid	Select the action to be performed on closing the lid. It can be either left as such or made to go to the standby mode.
When I press the power button on my computer	Select the action to be performed when the power button is pressed from the following options: Do nothing - to leave it as such Ask me what to do - to prompt the user Standby - to go to the standby mode Shutdown to shutdown the computer
When I press the sleep button on my computer	Select the action to be performed when the sleep button is pressed from the following options:

Parameter	Description
	Do nothing - to leave it as such Ask me what to do - to prompt the user Standby - to go to the standby mode Shutdown to shutdown the computer

* - denotes mandatory parameters

	**Note**: While creating new schemes, you can select any of the default schemes from the list to load its values and then modify it to suit your need.

If you wish to create/modify more schemes, click **Add More Scheme** button and repeat step 2. The defined scheme gets added to the **List of Power Schemes added** table.

Delete a Power Scheme

To delete an existing power scheme, select the Delete Scheme tab of the Power Management Configuration and specify the name of the scheme that has to be deleted.

If you wish to create/modify/delete more schemes, click **Add More Scheme** button and repeat step 2. The defined task gets added to the **List of Power Schemes added** table.

To modify a scheme from **List of Power Schemes added** table, select the appropriate row and click icon and change the required values.

To delete scheme from **List of Power Schemes added** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Power Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Power Management Configuration in the defined targets. The Power Management configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Registry Settings

The Registry Settings allows you to add, modify, and delete the values in the registry of the users. Desktop Central Registry Settings Configuration enables you to modify the values in the registry centrally and for several users.

Step 1: Name the Configuration

Provide a name and description for the Registry Settings configuration.

Step 2: Define Configuration

You can perform the following actions:

- Write Value
- Delete Value
- Add Key
- Delete Key

Write Value

To write a value in the registry, select the **Action** as *Write Value* and specify the following values:

Parameter	Description
Header Key	Select the header key from the following options: *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. *HKEY_USERS/.Default*: It has the default profile

Parameter	Description
	preferences.
Key	Keys are sub-components of the hives. Specify the key value.
Type	The type of the value. This varies with respect to the Header Key selected. Select the appropriate type from the combo box.
Value	Specify the value to be added. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Data / Expression	Specify the data or expression. If the new value has to be created without data, enter the word clear inside the parentheses as (clear). Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note: If you wish to write more values, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Value

To delete a value from the registry, select the **Action** as *Delete Value* and specify the following values:

Parameter	Description
Header Key	Select the header key from the following options: *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value.
Value	Specify the value to be deleted.

	**Note**: If you wish to delete more values, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Add Key

To add a registry key, select the **Action** as *Add Key* and specify the following:

Parameter	Description
Header Key	Select the header key from the following options: *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value to be added.

	**Note**: If you wish to add more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Key

To delete a registry key, select the **Action** as *Delete Key* and specify the following values:

Parameter	Description
Header Key	Select the header key from the following options: *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. *HKEY_CURRENT_USER*: It has the preferences for

Parameter	Description
	the user currently logged in. *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value that has to be deleted.

	**Note**: If you wish to delete more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

To modify a registry setting from the **Registry Settings** table, select the appropriate row and click icon and change the required values.

To delete a registry setting from the **Registry Settings** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Registry Settings Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Registry Settings Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Securing USB Devices

The Secure USB configuration is used for both users and computers to block or unblock the use of the USB devices. This configuration is applicable to users irrespective of the computers they use.

Using this configuration, you can block or unblock the following devices:

- Mouse devices
- Disk drives (for example, USB drives and external hard-disk drives)
- CD ROMs
- Portable devices (for example, mobile phones, digital cameras and portable media players)
- Floppy disks
- Bluetooth devices
- Images (for example, USB cameras and scanners)
- Printers
- Modems

You can also exclude devices using the Device Instance ID assigned to each device.

Making Secure USB Settings for Users

When you create the Secure USB configuration to block or unblock devices for users, you can set actions to take place once the user logs off. These actions enable you to retain or remove the settings that you make, using the Secure USB configuration, once the user logs off. The actions that you can set include the following:

- Don't alter device status: Use this option to retain the settings you have made, even after the user has logged off.

  For example, if you use this option, the settings that you have made to block or unblock the usage of USB devices will apply to all users who log on.

- Disable all devices excluding mouse: Use this option to remove the settings you have made, even after the user has logged off.

Applying Secure USB Settings to Computers and Users

When you apply the Secure USB configuration to both computers and users, the settings made for computers will be applied before the settings made for users. For example, assume that you have made the following settings:

- Settings for users

- Administrator: You have unblocked the usage of the disk drive
- Other users (excluding the administrator): You have not deployed any configurations

- Settings for a computer: You have blocked the usage of portable devices and disk drives

The following actions will take place:

- Computer startup: The Secure USB configuration settings made for the computer are applied when the computer is started. This means that no portable devices and disk drives can be used.
- Administrator logon: The Secure USB configuration for the computer is applied. However, it is over written by the settings made for the administrator. This means that the administrator can use disk drives.
- Other users (excluding the administrator) log on: The Secure USB configuration made for the computer is applied.
- Other users (excluding the administrator)log off: The log off-action settings made for users are applied when a user logs off. If the log off-action setting is set to Don't alter device status, then the settings made will apply to the next user who logs on, provided that the user does not have any settings that apply to them.

Creating Configurations to Secure USB Devices

As an administrator, you can create a configuration block or unblock specific USB devices. You can also exclude specific devices, if required.

To create a configuration to secure USB devices for users, follow the steps given below:

1. Click the **Configurations** tab
2. Click **Configuration**
3. In the **User Configurations** section click **Secure USB**
4. Enter a name and description for the configuration
5. Select the devices to block or unblock
6. Select the required log-off action
7. Define the target
8. Make the required execution settings
9. Click **Deploy**

You have created configurations to secure USB devices. These configurations will be applied when the user logs in to the computer.

Excluding Devices

When you block a device you can exclude certain devices from being blocked by using the Device Instance ID assigned to each device. You can exclude devices only when you are creating configurations for users.

Every USB device has a unique ID. This ID is assigned to devices by the system to identify them easily.

Identifying the Device Instance ID of a Device

To identify the Device Instance ID of a device, follow the steps given below:

1. Right-click **My Computer**
2. Click **Properties**
3. Click the **Hardware** tab
4. Click **Device Manager** (Refer to the figure below)

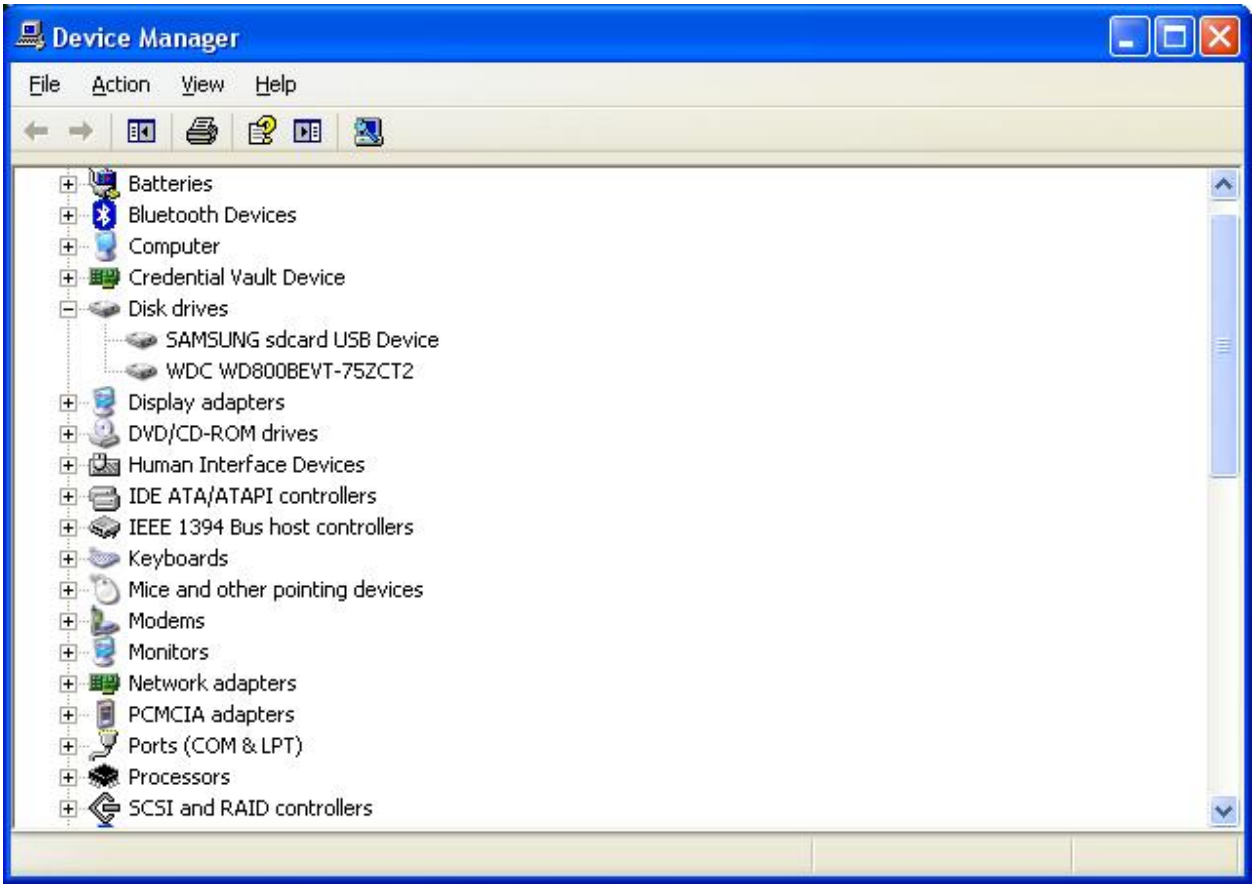


Figure 1: Device Manager

From the list of devices, expand the list of devices for which you want the Device Instance ID.

For example, if you want to identify the Device Instance ID of a mobile phone that you have connected to the computer, expand portable devices and follow the next step.

5. Right-click on the name of a specific device and click **Properties** (Refer to the figure below)

Figure 2: Properties

6. Click the **Details** tab
7. In the drop-down box, select **Device Instance ID** or Device Instance Path (Refer to the figure below)

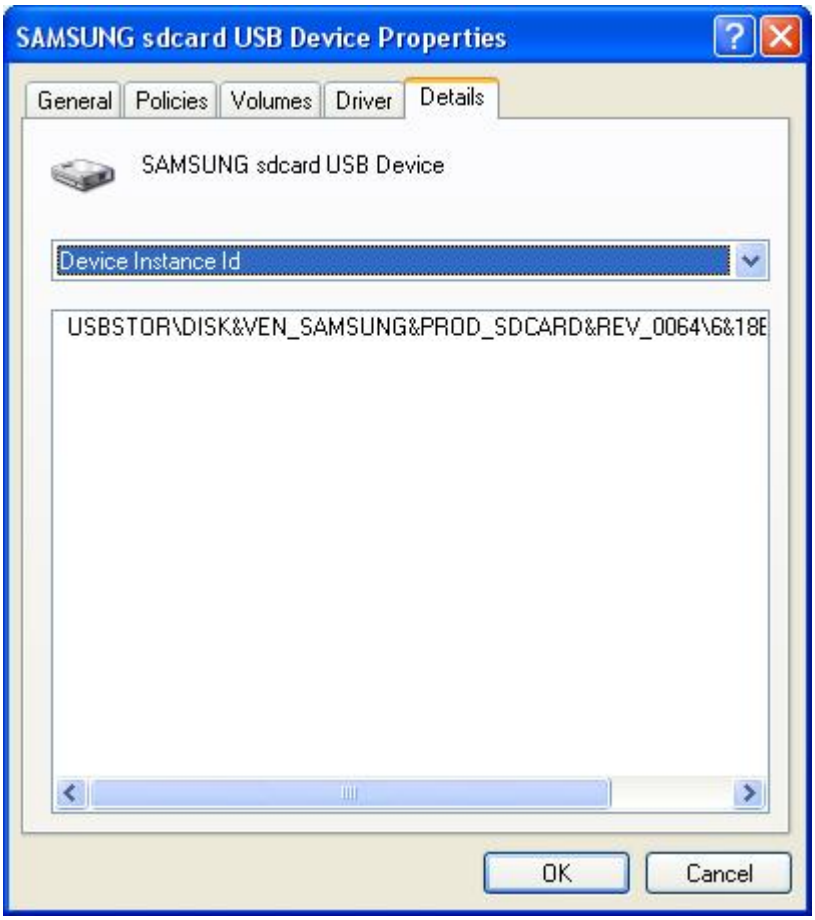


Figure 3: Device Instance ID

	In computers which have the operating system Windows Vista (and later versions), the Device Instance ID is called the **Device Instance Path**. You can copy the Device Instance Path from the Properties property sheet of the Device Manager. In computers that have older versions of the Windows operating system installed in them, you cannot copy the Device Instance ID directly from the Properties property sheet of the Device Manager. To copy the Device Instance ID you must open the dcusbaccess log file. This file is located in <Drive>\<Desktopcentral_Agent Folder>\logs\dcusbaccess.log. It contains information about the following: Action Time (inserted\removed time)

	Action (inserted\removed) Friendly name Device Instance ID

You can now view and copy the Device Instance ID for a specific device.

You can exclude devices only when you have blocked a device. To exclude devices, follow the steps given below:

1. Click the **Exclude Devices** link against a device
2. Enter the **Device Instance ID** for the device
3. Click **Close**

You have excluded a device from being blocked.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Securing USB for Computers

Scheduling Tasks

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

The Windows Scheduler Configuration enables you to schedule any program, task, or a script to run at a specified time. You can also schedule a task to run daily, weekly, monthly , etc. The Scheduler Configuration enables you to add, modify tasks from a central point.

Step 1: Name the Configuration

Provide a name and description for the Scheduler Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create/Modify a Task
- Delete a Task

Create / Modify a Task

To create a new task, select the **Create Task** tab of the Scheduler Configuration. Select the **Modify Task** tab to modify an existing task. Specify the following values:

Parameter	Description
Name of the task*	The name of the task that has to be created/ modified.
Overwrite if task already exits	Select this option to overwrite the task, if one with the same name exists. This option is only available for create task.
Application Name*	The application or the program that has to be run. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Arguments	The arguments to run the program, if any. Click the ☆ icon to select and assign a dynamic variable to this parameter.

Parameter	Description
User Name*	The name of the user as whom the task will be run. Click the ☆ icon to select and assign a dynamic variable to this parameter, for example, $DomainName\$DomainUserName or $ComputerName\$DomainUserName.
Password	The password of the user.
Confirm Password	Confirm the password again.
Perform this task*	Specify the time to perform the task. You can select from the following options: *Daily:* To run the task daily. Specify the time and duration to run the task. *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run. *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months. *Once:* To run the task only once. You need to specify the date and time. *At System Startup:* To run the task when the system is started. *At Logon:* To run the task during the user logon. *When Idle:* To run the task when the system is idle for the specified time.
Advanced Settings	
General	*Enabled*: Select this option to run the task at the specified time. *Run only when logged on:* Select this option to run the task only when the user has logged on.
Scheduled Task Completed	*Delete the task if it is not scheduled to run again:* Select this option to delete the task when it is no longer scheduled. *Stop Task:* Select this option and specify the duration after which the task will be stopped.

Parameter	Description
Idle Time	Select the required options: Specify the duration,the system has to be idle before starting a task. Stop the task if the computer ceases to be idle
Power Management	Select the required options: Don't start the task if the computer is running on batteries Stop the task if battery mode begins Wake the computer to run this task

* - denotes mandatory parameters

If you wish to create/modify more tasks, click **Add More Task** button and repeat step 2. The defined task gets added to the **Task** table.

When a wrong password is provided for tasks scheduled in Win2k / WinXP SP1 machines, the tasks will be successfully created, but, fails to execute.

Delete a Task

To delete a task, select the Create Task tab of the Scheduler Configuration and specify the name of the task that has to be deleted.

If you wish to create/modify/delete more tasks, click **Add More Task** button and repeat step 2. The defined task gets added to the **Task** table.

To modify a task from the **Task** table, select the appropriate row and click  icon and change the required values.

To delete a task from the **Task** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Scheduler Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Scheduler Configuration in the defined targets. The scheduler configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See also : Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Security Policies

Security policies determine the various security restrictions that can be imposed on the users in a network. The security settings for Active Desktop, Computer, Control Panel, Explorer, Internet Explorer, Network, and System categories can be defined using **Security Policies Configuration**.

Step 1: Name the Configuration

Provide a name and description for the Security Policies Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Choose Policy Category	The specific policy area in which the security policy will be applied. Select the desired category from left. This displays the relevant security polices. For details on the each category, refer to Windows Help documentation. For details on the each policy in the **Select the Policy** list, refer to Security Policies topic.
Policy Value	To enable, disable, or to leave it unconfigured, select the appropriate option.

Note:

1. To modify a security policy from this table, select the appropriate row, click icon and change the required values.
2. To delete a security policy from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Security Policies Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Security Policies Configuration in the defined targets. The security policies will be applied during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Security Policies

Configuring Shared Network Printer

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

When a printer is installed in a machine in the network and is shared, other machines in the network can use this printer for their printing needs. Desktop Central enables you to configure the Shared Network Printer in the user machines.

For configuring an IP printer connection to the computer, refer to the Configuring IP Printer topic.

Note: To add the Shared Network Printer Configuration, a computer must be installed with printer connection and must be shared.

Step 1: Name the Configuration

Provide a name and description for the Shared Network Printer Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add a Shared Network Printer
- Delete a Shared Network Printer

Add a Shared Network Printer

To add a Shared Network Printer, select the **Action** as *Add* and specify the following values:

Parameter	Description
Shared Network Printer Path*	Browse and select the path of the shared network printer location in the network.
Set as default printer	Select this check box, if you want to make this as the default printer for the user. By default, this option is cleared.

* - denotes mandatory field

Delete a Shared Network Printer

To delete a Shared Network Printer, select the **Action** as *Delete* and specify the following values:

Parameter	Description
Shared Network Printer Path*	Browse and select the path of the Shared Network Printer location in the network.
Delete all existing Shared Network Printer connections	Select this check box, if you want to delete all the existing Shared Network Printer connections. By default, this option is disabled.

* - denotes mandatory field

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Shared Network Printer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Shared Network Printer Configuration in the defined targets. The printer configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Managing Shortcuts

The shortcut is an icon that points to a file, folder or an Internet URL. The Shortcut Configuration enables you to add shortcuts to the users from a central point.

Step 1: Name the Configuration

Provide a name and description for the Shortcut Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create a Shortcut
- Create an Internet Shortcut
- Delete a Shortcut / Internet Shortcut

Create a Shortcut

To create a shortcut, select the **Action** as *Create Shortcut* and specify the following values:

Parameter	Description
Overwrite	To modify the existing shortcut select this option.
Shortcut Name*	Specify the name of the shortcut.
Target Application*	Browse and select the target application from the network for which a shortcut has to be created. The target application can also be in the local machine where the configuration is being deployed.
Arguments*	If the application requires any arguments, specify the arguments. Leave it blank if it does not require any arguments.

Parameter	Description
Shortcut Location	Select the location to create the shortcut. The shortcut location can be any of the following: *User Desktop*: Refers to the desktop of that user. *User Favorites*: Refers to the favorites folder of that user. *User Start Menu*: Refers to the start menu of that user. *User Programs Group*: Refers to the Start --> Programs group of that user. *User Startup Group*: Refers to the Start --> Programs --> Startup group of that user. *User Quick Launch Bar*: Refers to the quick launch bar of that user. *All Users Desktop*: Refers to the desktop common for all the users. *All Users Start Menu*: Refers to the start menu common for all users. *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.
Start In Folder*	Some applications may have some references to additional files during execution. In such cases, browse and select the location from where the application has to be started.
Shortcut Comments	Specify the comments for this shortcut.
Icon File*	Browse and select the icon for the shortcut.
Run Window	Select how the application has be started - *Normal*, *Maximized*, or *Minimized*.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note: If you wish to create more shortcuts, click **Add Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

Create an Internet Shortcut

To create an Internet shortcut, select the **Action** as *Create Internet Shortcut* and specify the following values:

Parameter	Description
Shortcut Name*	Specify the name of the Internet shortcut.
Target URL*	Specify the URL for which the shortcut needs to be created.
Shortcut Location	Select the location to create the shortcut. The shortcut location can be any of the following: *User Desktop*: Refers to the desktop of that user. *User Favorites*: Refers to the favorites folder of that user. *User Start Menu*: Refers to the start menu of that user. *User Programs Group*: Refers to the Start --> Programs group of that user. *User Startup Group*: Refers to the Start --> Programs --> Startup group of that user. *User Quick Launch Bar*: Refers to the quick launch bar of that user. *All Users Desktop*: Refers to the desktop common for all the users. *All Users Start Menu*: Refers to the start menu common for all users. *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.
Icon File*	Browse and select the icon for the shortcut.

Delete a Shortcut / Internet Shortcut

To delete a shortcut, select the **Action** as *Delete Shortcut / Internet Shortcut* respectively and specify the following values:

Parameter	Description
Shortcut Name	Specify the name of the shortcut. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Shortcut Location	Select the location from where the shourcuts needs to be deleted. The shortcut location can be any of the following: *User Desktop*: Refers to the desktop of that user. *User Favorites*: Refers to the favorites folder of that user. *User Start Menu*: Refers to the start menu of that user. *User Programs Group*: Refers to the Start --> Programs group of that user. *User Startup Group*: Refers to the Start --> Programs --> Startup group of that user. *User Quick Launch Bar*: Refers to the quick launch bar of that user. *All Users Desktop*: Refers to the desktop common for all the users. *All Users Start Menu*: Refers to the start menu common for all users. *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.

Note: If you wish to delete more shortcuts, click **Add More Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

To modify a shortcut from the **Shortcut** table, select the appropriate row and click icon and change the required values.

To delete a shortcut from the **Shortcut** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Shortcut Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Shortcut Configuration in the defined targets. The shortcut configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Computer Configurations

This section details the configurations that can be applied to the computers of the Windows Domain. Configurations applied to computers are available for all the users of the computers. These configurations are applied to the computers during startup or shutdown.

Note: Ensure that you have defined the scope of management before defining the configurations. For details, refer to Defining the Scope of Management.

To reach the configuration screen, follow the steps below:

1. Click **Add Configuration** link from the Quick Links. This will list all the supported configurations for users and computers.
2. Click the required configuration listed under the Computer Configurations.

Desktop Central supports the following configurations that can be applied on computers:

- Redirecting Common Folders
- Executing Custom Scripts
- Setting Environment Variables
- Managing Files and Folders
- Configuring Windows XP Firewall
- Configuring General Computer Settings
- Managing Windows Local Groups
- Installing Patches
- Installing Software - MSI/EXE Format
- Installing Windows Service Packs
- Configuring IP Printers
- Launching Applications
- Displaying Legal Notices
- Displaying Message Box
- Setting Path
- Managing Permissions
- Configuring Registry Settings
- Securing USB Devices

- Scheduling Tasks
- Configuring Security Policies
- Managing Shortcuts
- Configuring Windows Services
- Managing Windows Local Users

Redirecting Common Folders

The Common Folder Redirection Configuration helps to change the location of the All User Shell folders that are shared by all the users. The All User Shell folders which contains common Start Menu, Programs Group, Startup Group, Desktop, and application data shared by all the users. For the redirection of the user-specific folders in the computer, refer to the Redirecting User-Specific Folders topic.

Step 1: Name the Configuration

Provide a name and description for the Common Folder Redirection Configuration.

Step 2: Define Configuration

Select the values for the following fields that require change in settings. For each of the fields in the following table, click the **Browse** button next to the corresponding field to launch **Network Browser** window. Select the folder location and click **OK** button. If this field is left blank, the corresponding folder settings is left unchanged.

The following table provides a brief description about the common folders that can be redirected using Desktop Central.

Field	Description
Common Start Menu*	Contains the shortcuts that appear in the start menu that are common for all the users of the computer.
Common Programs Group*	Contains the shortcuts that appear in the Programs group of the start menu that are common for all the users of the computer.
Common Startup Group*	Contains the shortcuts that appear in Start --> Programs --> Startup menu. This specifies the applications that should be started during the startup of the system.
Common Desktop*	Contains the shortcuts and files that appear in the desktop that are common for all the users of the computer.
Common Application Data*	Contains the application data that are shared by all the users (C:/Documents and Settings/All Users/Application Data).

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Common Folder Redirection Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Common Folder Redirection Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Redirecting User-Specific Folders

Executing Custom Scripts

Desktop Central provides options for configuring almost all the computer configurations from remote. In addition to the configurations that are supported by Desktop Central, administrators can also write their own scripts that could be run on the machines for accomplishing specific configurations. The scripts could be any of the following:

- Batch file (.bat or .cmd)
- In any other language hosted by Windows Script Host (WSH), such as VB Script, JScript, Perl, REXX, and Python.

Note: The script engines for languages like Perl, REXX, and Python, must be registered with Windows.

Step 1: Name the Configuration

Provide a name and description for the Custom Script Configuration.

Step 2: Define Configuration

The table given below lists the parameters that have to be provided for defining the configuration.

Parameter	Description
Script Name*	The script that has to be executed in the machines. You have an option to select the script from any of the following: **Local**: The machine from where the configuration is being defined. **Inventory**: Refers to the Desktop Central inventory. All the scripts that have been added using Managing Scripts procedure will be available here. **Network Share**: Refers to the network share.

Parameter	Description
Script Arguments	The arguments that have to be provided while executing the scripts.
Execute During*	Refers to the script execution time. This can be either during the system **startup** or **shutdown**.

* - Refers to the mandatory fields.

Note: The scripts specified from the **local** or **share**, will automatically be added to the Desktop Central inventory after successful deployment.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Custom Script Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Custom Script Configuration in the targets.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Managing Custom Scripts

Setting Environment Variables

Environment variables are strings that contain information about the environment for the system, and the currently logged on user. Some software programs use the information to determine where to place files (such as temp, tmp, path etc). Environment variables control the behavior of various programs. Any user can add, modify, or remove a user environment variable. However, only an administrator can add, modify, or remove a system environment variable. Using Desktop Central, the environment variables can be defined and added.

Step 1: Name the Configuration

Provide a name and description for the Environment Variable Configuration.

Step 2: Define Configuration

The following table lists the parameters that have to be specified**:**

Parameter	Description
Variable*	The environment variable name that has to be modified or added.
Value*	The value that has to be stored in the environment variable. Click the ☆ icon to select and assign a dynamic variable to this parameter.

* - denotes mandatory fields

Note:

1. To add more environment variables, click **Add More Variables** and repeat Step 2. The defined environment variable gets added to the **List of Environment Variable** table.
2. To modify a environment variable from this table, select the appropriate row, click icon and change the required values.
3. To delete a environment variable from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Environment Variable Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Environment Variable Configuration in the targets defined. The configurations will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Setting Path

Managing Files and Folders

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The File and Folder Operation allows you to copy, move, rename, delete files and folders in computers. Desktop Central File and Folder Operation Configuration enables you to copy/move/delete files for several computers from central location.

Step 1: Name the Configuration

Provide a name and description for the File and Folder Operation configuration.

Step 2: Define Configuration

You can perform the following actions:

- Copy Files and Folders
- Rename/Move Files and Folders
- Delete Files and Folders

Copy Files and Folder

To copy files and folders, select the *Copy* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: *Copy a File* - To copy a file from one location to another. *Copy a File to a Folder* - To copy a file from one location to a specified folder. *Copy Multiple Files* - To copy multiple files to a specified folder. *Copy a Folder* - To copy a folder from one location to another.

Parameter	Description
Source File	Specify the file that has to be copied. The file can either be in a shared location or in the specified location in the client machines.
Destination File	Specify the destination location with the file name.
Destination Folder	Specify the destination folder to copy the files/folders.
Include Read Only Files	Select this option, if you wish to copy the files even if it has only read-only permissions.
Include System Files	Select this option if you wish to copy the system files.
Include Hidden Files	Select this option if you wish to copy the hidden files.
Overwrite Existing Files	Select this option to overwrite the existing files.
Create Destination Directory if doesn't Exist	Select this option to create the destination directory, if it does not exist.
Include Sub Folders	Select this option, if you wish to copy sub folders or the files within the sub folders.
Continue on Error	While copying multiple files or folders, specify whether to continue, if any error is encountered while copying.
Choose file modification time	Specify the file or folder modification time. Files that meet the specified criteria will only be copied.
Connect using Credentials	To copy Files/Folders across Domains or amongst Workgroup computers, you need to specify a credential that has access to the source Files/Folders.

Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Rename / Move Files and Folders

To rename or move the files and folders, select the *Rename/Move* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: Rename/Move a file Rename/Move a folder
Source File/Folder	Specify the file or the folder that has to be copied
Destination File/Folder	Specify the destination file or the folder.

Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Delete Files and Folders

To delete the files and folders, select the *Delete* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: Delete a File Delete Multiple Files Delete a Folder
Source File	Specify the files/folders that has to be deleted
Include Read Only Files	Select this option, if you wish to delete the read-only files
Include System Files	Select this option, if you wish to delete the system files
Include Hidden Files	Select this option, if you wish to delete the hidden files.
Include Sub Folders	Select this option, if you wish to delete the sub folders or the files within the sub folders.

Parameter	Description
Continue on Error	While deleting multiple files or folders, specify whether to continue, if any error is encountered while deleting.

Note: If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

To modify a file action from the **List of File Actions** table, select the appropriate row and click icon and change the required values.

To delete a file action from the **List of File Actions** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the File and Folder Operation Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined File and Folder Operation Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Windows XP Firewall

The Firewall configuration in the Windows XP Operating System can be modified using Desktop Central. The Windows XP Firewall blocks or permits access to the computer for specific TCP or UDP ports.

	**Note:** The Firewall Configuration can be deployed only on the computers with the Windows XP (with Service Pack 2) Operating System.

Step 1: Name the Configuration

Provide a name and description for the Firewall Configuration.

Step 2: Define Configuration

Select the Firewall Action from the combo box. The action could be any of the following:

- **ON**: To turn on the Windows XP Firewall.
- **OFF**: To turn off the Windows XP Firewall.
- **DONT MODIFY**: To preserve the client settings. This option is selected by default.

	**Note:** The Firewall configurations defined using Desktop Central can be deployed successfully to the client computers. However, it will take effect only when you turn on the Windows XP Firewall.

Specify the following parameters to block/unblock a port:

Parameter	Description
Port Action	Select whether to block, unblock, or to retain client settings using the Windows XP Firewall. The default option is Block.
Choose Port [Number -	Specify the port in the form of Port Number - Port Name -

Parameter	Description
Name - Protocol]	Protocol. The standard ports and services are listed in the combo box. If the required port is not listed, select the **Customize** link to either choose the port from the Additional ports list or to add your own by providing the required details.
Dependent Services	On selecting the port the dependent services are shown in this field. This cannot be modified from here.

Note:

1. To block/unblock more ports, click **Add More Ports** and repeat Step 2. The port gets added to the **Firewall** table.
2. To modify a setting from this table, select the appropriate row, click icon and change the required values.
3. To delete a setting from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets deploying the Firewall Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Firewall Configuration in the defined targets. The configurations will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring General Computer Settings

The General Configuration is for configuring the general settings for the computers, such as configuring display the last user name, synchronize the system time with Time Server, and so on.

Step 1: Name the Configuration

Provide a name and description for the General Configuration.

Step 2: Define Configuration

The table below lists the general settings that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
Display last User Name	To specify whether to display the previously logged user name or not. This is displayed when a user logs on to the system. To leave it unchanged, select *Preserve client settings* option.
Registered Owner*	The name of the registered owner of the system. This is displayed in the General tab of the My Computer properties window.
Registered Company*	The name of the company. This is displayed in the General tab of the My Computer properties window.
Time Server	Browse and select a time server to synchronize the time of the computer with of the time server. Time synchronization happens when the computer is started.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the General Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined General Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Managing Windows Local Groups

The Group Management allows you to add, modify, or delete local groups from the computers.

Step 1: Name the Configuration

Provide a name and description for the Group Management Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add Group
- Delete Group
- Modify Group

Add Group

To add a group to the computer, select the **Add Group** link from the Choose Group Action table and specify the following:

Parameter	Description
Group Name	The name of the group that has to be created.
Description	The description of the group.
Add Member	Select the Member Type as Local, Domain User, or Domain Group and specify/select the users or global groups that have to be added to the local group.
Overwrite if group already exist	Select this option, if you wish to overwrite the group definition, if one with the same name exists.

	**Note**: If you wish to add more groups or to perform another action, click **Add More Actions** button and continue. The values gets added to the **List of Settings** table.

Delete Group

To delete a group from the computer, select the **Delete Group** link from the Choose Group Action table and specify the group name that has to be deleted.

	**Note**: If you wish to delete more groups or to perform another action, click **Add More Actions** button and continue. The values gets added to the **List of Settings** table.

Modify Group

To modify a group of the computer, select the **Modify Group** link from the Choose Group Action table and specify the group name that has to be deleted.

Parameter	Description
Group Name	The name of the group that has to be modified.
Description	The description of the group.
Add Member	Select the Member Type as Local, Domain User, or Domain Group and specify/select the users or global groups that have to be added to the local group.
Remove Member	Select the Member Type as Local, Domain User, or Domain Group and specify/select the users to be removed from this group.

	**Note**: If you wish to modify more groups or to perform another action, click **Add More Actions** button and continue. The values gets added to the **List of Settings** table.

To modify a setting from the **List of Settings** table, select the appropriate row and click  icon and change the required values.

To delete a setting from the **List of Settings** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Group Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Group Management Configuration in the targets defined. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Installing Patches

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Install Patches configuration enables you to install patches to fix the application vulnerabilities from a central location.

Step 1: Name the Configuration

Provide a name and description for the Install Patches Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Add the Patches	Click the Add More Patches button to invoke the Patch Browser. From the patch browser select the patches that have to be applied. The patch browser has an option to view the missing patches or all patches, which can then be filtered based on the application and service pack.
Scheduler Settings	Install After Select this option and specify the date and time after which the patches have to be installed. The patches will be installed based on the Install Options selected after the scheduled time.
Deployment Settings	If you have defined Deployment Templates, you can load the Deployment Settings directly from a template by selecting the required template from the list. Install Options Install during computer startup: Select this option if the patches have to be deployed during computer startup. Install during 90 minutes refresh interval: Select this option

Parameter	Description
	if the patches have to be installed after the computer startup when the next update happens (within 90 minutes) Either of the above, whichever is earlier Install Between If you want the installation to happen only between a specified time of a day, you can specify the Start and End time within which the deployment should begin. The Start Time can also be greater than the End time - in such cases the End time is assumed to be on the following day. For example, if you wish the deployment should happen between 10.00 PM and 4.00 AM, you can specify the Start Time as 22:00:00 and End Time as 04:00:00 Allow Users to Skip Deployment Specify whether the use can skip the deployment at a later time by selecting the "Allow Users to Skip Deployment". When you do not select this option, the deployment will be forced and the user will not have any control on the deployment. When you allow users to skip deployment, you can also specify whether they can skip it as long as they wish or force deployment after a specific date. Reboot Policy Do not reboot: Select this option if the client computers should not be rebooted after installing the patches. Force Reboot when the user has logged in: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. Force Shutdown when the user has logged in: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. Allow user to skip Reboot: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. Allow user to skip Shutdown:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

	**Note**: If you have reached this configuration page from the Patch Management tab by selecting the patches, the selected patches automatically gets added to the List of Patches.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Install Patches Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Install Patches Configuration in the defined targets. The software installation for the selected targets will happen during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Installing Software - MSI & EXE Packages

The Software Installation configuration helps you to install MSI and EXE packages remotely to several computers of the Windows network from a central location.

Step 1: Name the Configuration

Provide a name and description for the Software Installation Configuration.

Step 2: Define Configuration

You have an option to install either an EXE or an MSI package

- Install MSI Package
- Install EXE Package

Install MSI Package

Select the Installer type as **MSI** and specify the following values:

Parameter	Description
MSI Package Name	This will list all the MSI packages that are available in the Software Repository. Select the MSI that has to be installed.
Operation Type	To specify how the installation should happen. Select any of the following options: *Install Completely:* Selecting this option will install the application automatically. *Advertise*: Selecting this option will notify the user about the availability of the software. Thy can choose whether to install the software or not. *Remove*: Selecting this option remove (uninstall) the application from the system

Parameter	Description
Run As	The user as whom the MSI has to be installed.
Password	Password for the user as whom the MSI has to be installed.
Copy	You have an option to copy the installables to the client machines before installing them. Select the required option: *None:* Selecting this option will not copy the installation files. *Copy file to client machines:* Will copy the exe or the msi file alone as specified in the software package to the client machines. *Copy folder to client machines:* Will copy the entire directory that has the installation file to the client machines. Copy option will be mandatory, when the network share requires a user credential to access and when you opt to install the software as a different user using the Run As option.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	Description
Schedule Time to Perform the Operation	Select his option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type & Installation / Uninstallation Option selected, but this will begin after the time specified here.

Specify the Deployment Settings for the software:

If you have defined Deployment Templates, you can load the Deployment Settings directly from a template by selecting the required template from the list.

Parameter	Description
Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after system startup: *During startup*: Select this option if the software has to be installed/uninstalled during computer startup. *After startup*: Select this option if the software has to be installed/uninstalled after the computer startup when the next GP update happens (within 90 minutes) *During or After Startup*: Either of the above, whichever is earlier
Install Between	If you want the installation to happen only between a specified time of a day, you can specify the Start and End time within which the deployment should begin. The Start Time can also be greater than the End time - in such cases the End time is assumed to be on the following day. For example, if you wish the deployment should happen between 10.00 PM and 4.00 AM, you can specify the Start Time as 22:00:00 and End Time as 04:00:00
Allow Users to Skip Deployment	Specify whether the use can skip the deployment at a later time by selecting the "Allow Users to Skip Deployment". When you do not select this option, the deployment will be forced and the user will not have any control on the deployment. When you allow users to skip deployment, you can also specify whether they can skip it as long as they wish or force deployment after a specific date.
Reboot Policy	*Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. *Force Shutdown when the user has logged in*: Select

Parameter	Description
	this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Install EXE Packages

Select the Installer type as **EXE** and specify the following values:

Parameter	Description
EXE Package Name	This will list all the EXE packages that are available in the Software Repository. Select the EXE that has to be installed.
Operation Type	Select the operation type as Install or Uninstall.
Run As	The user as whom the EXE has to be installed.
Password	Password for the user as whom the EXE has to be installed.
Copy	You have an option to copy the installables to the client machines before installing them. Select the required option: *None:* Selecting this option will not copy the installation files. *Copy file to client machines:* Will copy the exe or the msi file alone as specified in the software package to the client machines. *Copy folder to client machines:* Will copy the entire directory that has the installation file to the client machines. Copy option will be mandatory, when the network share requires a user credential to access and when you opt to install the software as a different user using the Run As option.

Click **Add More Packages** to install/uninstall additional software.

	**Note**:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	Description
Installation / Uninstallation Option	Specify whether the installation should happen during or after system startup.
Schedule Time to Perform the Operation	Select this option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type & Installation / Uninstallation Option selected, but this will begin after the time specified here.
Reboot Policy	*Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Windows Installer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Windows Installer Configuration in the defined targets. The software installation for the selected targets will happen as scheduled.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Installing Windows Service Packs

The Install Service Pack configuration enables you to install windows service packs to operating system and other windows applications from a central location.

Step 1: Name the Configuration

Provide a name and description for the Install Service Pack Configuration.

Step 2: Define Configuration

Specify the following:

Parameter	Description
Select the Service Pack	All the available Service packs are listed here. You can filter the view based on the OS or the application by selecting the appropriate option from the Select Application combo box. Select the service pack from the list and specify whether to reboot the system after applying the service pack.
Deployment Settings	Install After Select this option and specify the date and time after which the service pack has to be installed. The service pack will be installed based on the Install Options selected after the scheduled time. Install Options *Install during computer startup*: Select this option if the service pack has to be deployed during computer startup. *Install during 90 minutes refresh interval*: Select this option if the service pack has to be installed after the computer startup when the next update happens (within 90 minutes)

Parameter	Description
	Either of the above, whichever is earlier Reboot Policy *Do not reboot*: Select this option if the client computers should not be rebooted after installing the service pack. *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to displayed in the client machines. *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Note: If no service pack details are listed here, check whether you can configured the Proxy Settings.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Install Service Pack Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Install Service Pack Configuration in the defined targets. The software installation for the selected targets will happen during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring IP Printer

The IP Printer Configuration is for adding or deleting the IP Printer connection in the computers. For configuring a shared or IP printers in the computer for specific users, refer to the Configuring Shared Printer / Configuring IP Printer topics under User Configurations.

Step 1: Name the Configuration

Provide a name and description for the IP Printer configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add an IP Printer
- Delete an IP Printer

Add an IP Printer

To add an IP Printer, select the **Action** as *Add* and specify the following values:

Parameter	Description
DNS Name/IP	The host name or IP address defined for the printer. *Example*: `192.111.2.32`
Printer Name	The display name for the printer.
Protocol	The printing protocol supported by the printer. Select the printing protocol from the Protocol list box. The default option is "RAW".
Port Number	The port number/queue name in which printing protocol is communicating between the computer and printer. Enter the port number in the Port Number field if the "RAW" Protocol is selected or enter the queue name if the "LPR" Protocol is selected. The default value is 9100.

Parameter	Description
Port Name	This is an optional field. By default, the port name is IP_<IP_Address/DNS_Name>. You can change the port name if required.
Shared Printer for Driver Installation	Browse to select a shared printer for installing the driver. If the drivers are already installed in the target computers, the Desktop Central will skip the driver installation.
Connect Shared Network Printer using Credentials	To copy Driver Files across Domains or amongst Workgroup computers, you need to specify a credential that access domain/workgroup machine where the Shared Printer Driver Files are present.

Delete an IP Printer

To delete an IP Printer, select the **Action** as *Delete* and specify the following values:

Parameter	Description
Printer Name	The display name of the printer.
Delete all existing IP printer connections	To delete all the existing IP printer connections in the computer for the specified user, select this option.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the IP Printer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined IP Printer Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Configuring Shared Printer

Launching Applications

Launch Application configuration enables you to launch an application during startup or shutdown of the computer.

Step 1: Name the Configuration

Provide a name and description for the Launch Application Configuration.

Step 2: Define Configuration

Select whether the application has to be launched from the local computer or from the network share. If you select the Local option, all the selected target computers should have the application in the same location. Specify the following:

Parameter	Description
Application Name*	Browse and select the application that has to be launched. The applications that are available in the local machine from where the application has to be launched can also be specified.
Arguments*	Specify the arguments for the application, if any.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note:

1. To launch more applications, click **Add More Application** and repeat Step 2. The added application gets added to the **Launch Application** table.
2. To modify an application from this table, select the appropriate row, click icon and change the required values.
3. To delete an application from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Launch Application Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Launch Application Configuration in the targets defined. The applications configured will be launched during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Displaying Legal Notices

The important enterprise wide announcements, legal notice, etc., can be configured using the Legal Notice configuration. The configured message will be displayed whenever the user presses ctrl+alt+del to login.

Step 1: Name the Configuration

Provide a name and description for the Legal Notice Configuration.

Step 2: Define Configuration

Specify the following:

Parameter	Description
Remove Already Defined Legal Notice	Select this option to clear the previous configurations, if any.
Window Title*	Specify the window title of the legal notice.
Message*	Specify the message that has to be displayed.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Legal Notice Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Legal Notice Configuration in the defined targets. The configured legal notice will be displayed during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Displaying Message Box

Displaying Message Box

For the computers in the network, the pop-up messages with the warning or error can be displayed during the system startup. If the system is already running while deploying this configuration, the message will be displayed during the system restart.

Step 1: Name the Configuration

Provide a name and description for the Message Boxes Configuration.

Step 2: Define Configuration

You have an option to create a new message box or delete the existing message box. Select the required option and specify the following:

Parameter	Description
Message Type	The message type as Information, Warning, or Error.
Window Title	The title of the message box.
Message	The message that has to be displayed.
Timeout in Seconds	The duration, in seconds, for the message display.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Message Boxes Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Message Boxes Configuration in the targets defined. The message will be displayed during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Displaying Legal Notices

Setting Path

Path is an environment variable that contains the path prefixes that certain applications, utilities, and functions uses to search for an executable file. The Path Configuration enables you to add path prefixes to this variable.

Step 1: Name the Configuration

Provide a name and description for the Path Configuration

Step 2: Define Configuration

Specify the path to be added to the environment variables. Multiple paths can be specified separated by a semi-colon (**;**). Click the ☆ icon to select and assign a dynamic variable to the Path variable.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Path Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Path Configuration in the targets defined. The configurations will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Setting Environment Variables

Managing Permissions

The Permission Management allows you to grant revoke permission on the files, folders and registry. Desktop Central Permission Management Configuration enables you to grant/revoke permissions to multiple computers from a central point.

Step 1: Name the Configuration

Provide a name and description for the Permission Management configuration.

Step 2: Define **Configuration**

You can grant or revoke permissions for the following objects:

- Files
- Folders
- Registry

Files

To grant or revoke permissions for files, select the *File* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: Append - To append to the existing file permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while

	the user/group can still modify the object. Overwrite - To overwrite the existing file permissions Revoke - To revoke the existing file permissions of the specified user/group. All the permissions to the specified user/group on that file will be removed. However, the inherited permissions will not be removed.
Path	Specify the path of the file for which you need to specify permissions
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Folders

To grant or revoke permissions for folders, select the *Folder* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: Append - To append to the existing folder permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. Overwrite - To overwrite the existing folder permissions Revoke - To revoke the existing folder permissions. All the permissions to the specified user/group on that folder will be removed. However, the inherited permissions will not be removed.
Path	Specify the path of the folder for which you need to specify permissions

Parameter	Description
Inheritance	Select the required option to specify how the permission should effect its subfolders and files
Settings	Select the required options.

Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Registry

To grant or revoke permissions for registry, select the *Registry* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: Append - To append to the existing registry permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. Overwrite - To overwrite the existing registry permissions Revoke - To revoke the existing registry permissions. All the permissions to the specified user/group on that registry key will be removed. However, the inherited permissions will not be removed.
Hive	Select the registry hive from the given options
Key	Specify the key within that hive for which you need to set the permissions
Inheritance	Select the required options to specify how the permission should effect its subkeys.
Settings	Select the required options.

	Note: If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

To modify a permission from the **List of Permission Actions** table, select the appropriate row and click icon and change the required values.

To delete a permission from the **List of Permission Actions** table, select the appropriate row and click icon.

Step 3: **Define** Target

Using the Defining Targets procedure, define the targets for deploying the Permission Management Configuration.

Step 4: **Deploy** Configuration

Click the **Deploy** button to deploy the defined Permission Management Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Registry Settings

The Registry Settings allows you to change the values in the registry in the workstations. Desktop Central Registry Settings Configuration enables you to modify the registry values from a central location.

Step 1: Name the Configuration

Provide a name and description for the Registry Settings Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Write Value
- Delete Value
- Add Key
- Delete Key

Write Value

To write a value to the registry, select the **Action** as *Write Value* and specify the following:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value.
Type	The type of the value. This varies with respect to the Header Key selected. Select the appropriate type from the combo box.
Value*	Specify the value to be added.

Parameter	Description
Data / Expression*	Specify the data or expression. If the new value has to be created without data, enter the word clear inside the parentheses as (clear).

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note: If you wish to write more values, click **Add More Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Value

To delete a value from the registry, select the **Action** as *Delete Value* and specify the following values:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value.
Value	Specify the value to be deleted.

Note: If you wish to delete more values, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Add Key

To add a registry key, select the **Action** as *Add Key* and specify the following:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value to be added.

	Note: If you wish to add more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Key

To delete a registry key, select the **Action** as *Delete Key* and specify the following values:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value that has to be deleted.

	Note: If you wish to delete more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

To modify a registry setting from the **Registry Settings** table, select the appropriate row and click icon and change the required values.

To delete a registry setting from the **Registry Settings** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Registry Settings Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Registry Settings Configuration in the targets defined. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Securing USB Devices

The Secure USB configuration is used for both users and computers to block or unblock the use of the USB devices.

Using this configuration, you can block or unblock the following devices:

- Mouse devices
- Disk drives (for example, USB drives and external hard-disk drives)
- CD ROMs
- Portable devices (for example, mobile phones, digital cameras and portable media players)
- Floppy disks
- Bluetooth devices
- Images (for example, USB cameras and scanners)
- Printers
- Modems

You can also exclude devices using the Device Instance ID assigned to each device.

Applying Secure USB Settings to Computers and Users

When you apply the Secure USB configuration to both computers and users, the settings made for computers will be applied before the settings made for users. For example, assume that you have made the following settings:

- Settings for users

- Administrator: You have unblocked the usage of the disk drive
- Other users (excluding the administrator): You have not deployed any configurations

- Settings for a computer: You have blocked the usage of portable devices and disk drives

The following actions will take place:

- Computer startup: The Secure USB configuration settings made for the computer are applied when the computer is started. This means that no portable devices and disk drives can be used.
- Administrator logon: The Secure USB configuration for the computer is applied. However, it is over written by the settings made for the administrator. This means that the administrator can use disk drives.

- Other users (excluding the administrator) log on: The Secure USB configuration made for the computer is applied.
- Other users (excluding the administrator)log off: The log off-action settings made for users are applied when a user logs off. If the log off-action setting is set to Don't alter device status, then the settings made will apply to the next user who logs on, provided that the user does not have any settings that apply to them.

Creating Configurations to Secure USB Devices

As an administrator, you can create a configuration block or unblock specific USB devices. You can also exclude specific devices, if required.

To create a configuration to secure USB devices for users, follow the steps given below:

1. Click the **Configurations** tab
2. Click **Configuration**
3. In the **Computer Configurations** section click **Secure USB**
4. Enter a name and description for the configuration
5. Select the devices to block or unblock
6. Define the target
7. Make the required execution settings
8. Click **Deploy**

You have created configurations to secure USB devices. These configurations will be applied during the system startup.

Excluding Devices

When you block a device you can exclude certain devices from being blocked by using the Device Instance ID assigned to each device.

Every USB device has a unique ID. This ID is assigned to devices by the system to identify them easily.

Identifying the Device Instance ID of a Device

To identify the Device Instance ID of a device, follow the steps given below:

1. Right-click **My Computer**
2. Click **Properties**
3. Click the **Hardware** tab
4. Click **Device Manager** (Refer to the figure below)

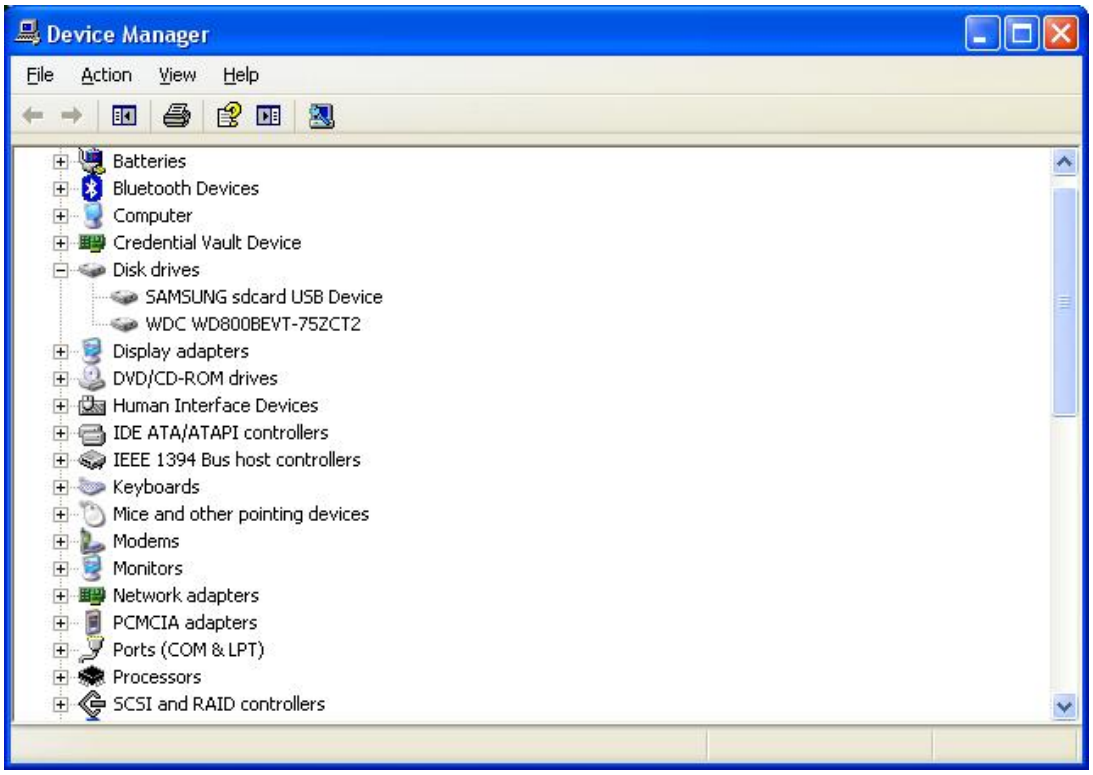


Figure 1: Device Manager

From the list of devices, expand the list of devices for which you want the Device Instance ID.

For example, if you want to identify the Device Instance ID of a mobile phone that you have connected to the computer, expand portable devices and follow the next step.

5. Right-click on the name of a specific device and click **Properties** (Refer to the figure below)

Figure 2: Properties

6. Click the **Details** tab

7. In the drop-down box, select **Device Instance ID** or Device Instance Path (Refer to the figure below)

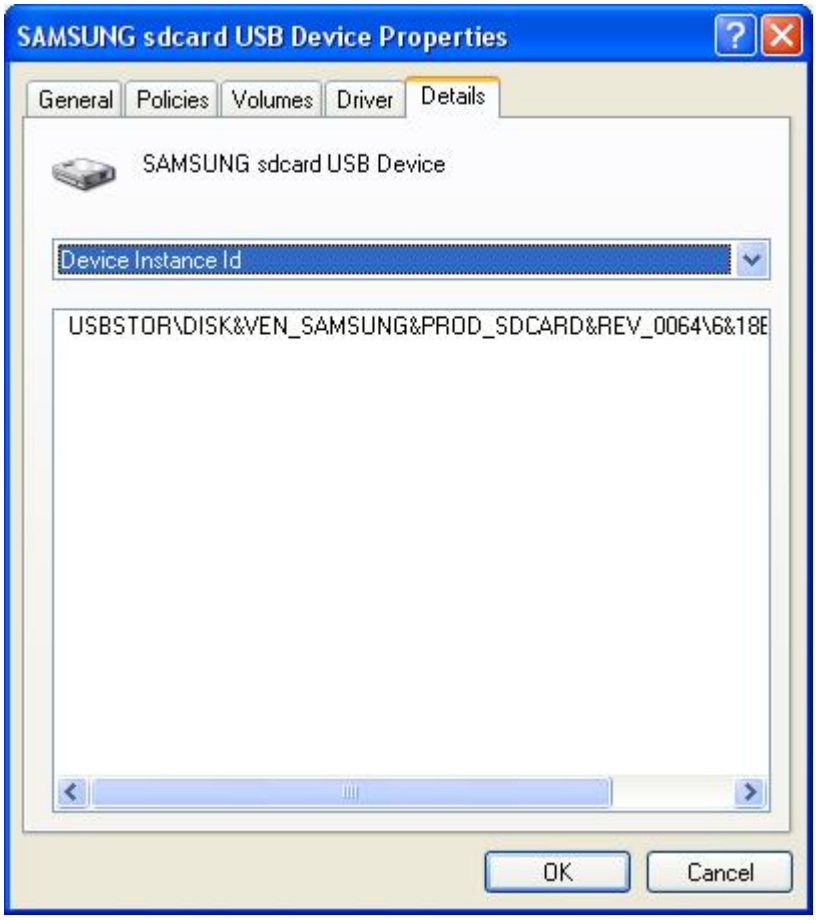


Figure 3: Device Instance ID

	In computers which have the operating system Windows Vista (and later versions), the Device Instance ID is called the **Device Instance Path**. You can copy the Device Instance Path from the Properties property sheet of the Device Manager. In computers that have older versions of the Windows operating system installed in them, you cannot copy the Device Instance ID directly from the Properties property sheet of the Device Manager. To copy the Device Instance ID you must open the dcusbaccess log

	file. This file is located in <Drive>\<Desktopcentral_Agent Folder>\logs\dcusbaccess.log. It contains information about the following: Action Time (inserted\removed time) Action (inserted\removed) Friendly name Device Instance ID

You can now view and copy the Device Instance ID for a specific device.

You can exclude devices only when you have blocked a device. To exclude devices, follow the steps given below:

1. Click the **Exclude Devices** link against a device
2. Enter the **Device Instance ID** for the device
3. Click **Close**

You have excluded a device from being blocked.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Securing USB for Users

Scheduling Tasks

The Windows Scheduler Configuration enables you to schedule any program, task, or a script to run at a specified time. You can also schedule a task to run daily, weekly, monthly , etc. The Scheduler Configuration enables you to add, modify tasks from a central point.

Step 1: Name the Configuration

Provide a name and description for the Scheduler Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create/Modify a Task
- Delete a Task

Create / Modify a Task

To create a new task, select the **Create Task** tab of the Scheduler Configuration. Select the **Modify Task** tab to modify an existing task. Specify the following values:

Parameter	Description
Name of the task*	The name of the task that has to be created/modified.
Overwrite if task already exits	Select this option to overwrite the task, if one with the same name exists. This option is only available for create task.
Application Name*	The application or the program that has to be run. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Arguments	The arguments to run the program, if any. Click

Parameter	Description
	the ☆ icon to select and assign a dynamic variable to this parameter.
User Name*	The name of the user as whom the task will be run. Click the ☆ icon to select and assign a dynamic variable to this parameter, for example, $DomainName\$DomainUserName or $ComputerName\$DomainUserName.
Password	The password of the user.
Confirm Password	Confirm the password again.
Perform this task*	Specify the time to perform the task. You can select from the following options: *Daily:* To run the task daily. Specify the time and duration to run the task. *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run. *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months. *Once:* To run the task only once. You need to specify the date and time. *At System Startup:* To run the task when the system is started. *At Logon:* To run the task during the user logon. *When Idle:* To run the task when the system is idle for the specified time.
Advanced Settings	
General	*Enabled*: Select this option to run the task at the specified time. *Run only when logged on:* Select this option to run the task only when the user has logged on.
Scheduled Task Completed	*Delete the task if it is not scheduled to run again:* Select this option to delete the task when it is no longer scheduled. *Stop Task:* Select this option and specify the duration after which the task will be stopped.

Parameter	Description
Idle Time	Select the required options: Specify the duration,the system has to be idle before starting a task. Stop the task if the computer ceases to be idle
Power Management	Select the required options: Don't start the task if the computer is running on batteries Stop the task if battery mode begins Wake the computer to run this task

* - denotes mandatory parameters

If you wish to create/modify more tasks, click **Add More Task** button and repeat step 2. The defined task gets added to the **Task** table.

Note: When a wrong password is provided for tasks scheduled in Win2k / WinXP SP1 machines, the tasks will be successfully created, but, fails to execute.

Delete a Task

To delete a task, select the Create Task tab of the Scheduler Configuration and specify the name of the task that has to be deleted.

If you wish to create/modify/delete more tasks, click **Add More Task** button and repeat step 2. The defined task gets added to the **Task** table.

To modify a task from the **Task** table, select the appropriate row and click icon and change the required values.

To delete a task from the **Task** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Scheduler Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Scheduler Configuration in the defined targets. The scheduler configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Security Policies

For the computers in the network, the Security Policies are security settings to specify the security and restrictions. The security settings for preventing users to change file type association can be defined using **Security Policies Configuration**.

Step 1: Name the Configuration

Provide a name and description for the Security Policies Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Choose Policy Category	The specific policy area in which the security policy will be applied. Select the desired category from left. This displays the relevant security polices. For details on the each category, refer to Windows Help documentation. For details on the each policy in the **Select the Policy** list, refer to Security Policies topic.
Policy Value	To enable, disable, or to leave it unconfigured, select the appropriate option.

Note:

1. To modify a security policy from this table, select the appropriate row, click icon and change the required values.
2. To delete a security policy from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Security Policies Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Security Policies Configuration in the targets defined. The security policies will be applied during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets, Security Policies

Managing Shortcuts

The shortcut is an icon that points to a file, folder or an Internet URL. The Shortcut Configuration enables you to add shortcuts to the computers from a central point.

Step 1: Name the Configuration

Provide a name and description for the Shortcut Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create a Shortcut
- Create an Internet Shortcut
- Delete a Shortcut / Internet Shortcut

Create a Shortcut

To create a shortcut, select the **Action** as *Create Shortcut* and specify the following values:

Parameter	Description
Overwrite	To modify the existing shortcut select this option.
Shortcut Name*	Specify the name of the shortcut.
Target Application*	Browse and select the target application from the network for which a shortcut has to be created. The target application can also be in the local machine where the configuration is being deployed.
Arguments*	If the application requires any arguments, specify the arguments. Leave it blank if it does not require any arguments.

Parameter	Description
Shortcut Location	Select the location to create the shortcut. The shortcut location can be any of the following: *All Users Desktop*: Refers to the desktop common for all the users. *All Users Start Menu*: Refers to the start menu common for all users. *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.
Start In Folder*	Some applications may have some references to additional files during execution. In such cases, browse and select the location from where the application has to be started.
Shortcut Comments	Specify the comments for this shortcut.
Icon File*	Browse and select the icon for the shortcut.
Run Window	Select how the application has be started - *Normal*, *Maximized*, or *Minimized*.

- Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note: If you wish to create more shortcuts, click **Add Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

Create an Internet Shortcut

To create an Internet shortcut, select the **Action** as *Create Internet Shortcut* and specify the following values:

Parameter	Description
Shortcut Name*	Specify the name of the Internet shortcut.
Target URL*	Specify the URL for which the shortcut needs to be created.
Shortcut Location	Select the location to create the shortcut. The

Parameter	Description
	shortcut location can be any of the following: *All Users Desktop*: Refers to the desktop common for all the users. *All Users Start Menu*: Refers to the start menu common for all users. *All Users Programs Group*: Refers to the Start -> Programs group common for all the users. *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.
Icon File*	Browse and select the icon for the shortcut.

Delete a Shortcut / Internet Shortcut

To delete a shortcut, select the **Action** as *Delete Shortcut / Delete Internet Shortcut* respectively and specify the following values:

Parameter	Description
Shortcut Name	Specify the name of the shortcut. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Shortcut Location	Select the location from where the shortcuts needs to be deleted. The shortcut location can be any of the following: *All Users Desktop*: Refers to the desktop common for all the users. *All Users Start Menu*: Refers to the start menu common for all users. *All Users Programs Group*: Refers to the Start -> Programs group common for all the users. *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.

	**Note**: If you wish to delete more shortcuts, click **Add More Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

To modify a shortcut from the **Shortcut** table, select the appropriate row and click icon and change the required values.

To delete a shortcut from the **Shortcut** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Shortcut Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Shortcut Configuration in the defined targets. The shortcut configuration will take effect during the next system start up.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Windows Services

Applications that have to be run automatically whenever the system is started can be configured to run as a Windows service. However in certain cases, after installing an application as a service, you may wish to change the startup type or delete the service. The Service Configuration enables you to change the settings for the services available in the **Control Panel >Administrative Tools >Services**.

Step 1: Name the Configuration

Provide a name and description for the Service Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Service Name	Select the name of the service from the combo box. The combo box contains the list of standard Windows services. If the required service is not listed, click **Customize** to either select the service from the Additional Services list or add you own by giving the required details.
Action	Specify the action to be performed from the following: *Don't Modify*: To preserve the client settings. This option is selected by default. *Start*: Select this option to start the service. *Stop*: Select this option to stop the service. *Restart*: Select this option to restart the service.
Service Startup Type	Select how the service should be started from the following options: *Don't Modify*: To preserve the client setting. *Manual*: Select this option if the service has to be manually

Parameter	Description
	started after the system startup. *Disabled*: Select this option to disable the service. *Automatic*: Select this option to automatically start the service along with the system.

Note:

1. To add more services, click **Add More Service** and repeat Step 2. The service gets added to the **Services** table.
2. To modify a service from this table, select the appropriate row, click icon and change the required values.
3. To delete a service from this table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Service Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Service Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Managing Windows Local Users

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The User Management allows you to add, modify, or delete local users from the computers.

Step 1: Name the Configuration

Provide a name and description for the User Management Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add User
- Change Password
- Remove User
- Modify User

Add User

To add an user to the computer, select the **Add User** link from the Choose User Action table and specify the following:

Parameter	Description
User Name	The user name for the user to be created.
Full Name	The full name of the user.
Description	The description for this user.
Password	The password for this user.
Confirm Password	Confirm the password again.
Overwrite if user already exist	Select this option to overwrite the user, if one with the same name exists.
Advanced Settings	
User Must change password	Specify whether the user has to change the

Parameter	Description
at next logon	password during the next logon or not.
User Cannot Change Password	Specify whether the user can change the password or not.
Password Never Expires	Specify whether the password should expire or not.
Account is Disabled	Specify whether the user account should be disabled or not.
User Profile	
Member of	Specify the groups in which this user account is a member.
Logon Script	Specify the logon script that has to be executed during the user logon.
Profile Path	Specify the path where the user profiles has to be stored.
Local Path	Specify a local path as the home folder. For example, c:\users\johnsmith.
Connect Map To	If the user's home folder has to be stored in a network directory, select the drive letter in the **Connect Map** and specify the network path in the **To** field.

Note: If you wish to add more users or to perform another action, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

Change Password

To change the user password, select the **Change Password** link from the Choose User Action table and specify the following:

Parameter	Description
User Name	The user name of the user whose password has to be changed.
Password	Type the new password.
Confirm Password	Re-type the password to confirm.

Note: If you wish to continue adding more actions, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

Remove User

To remove an user from the computer, select the **Remove User** link from the Choose User Action table and specify the user to be removed.

Note: If you wish to remove more users or to perform another action, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

Modify User

To modify an user, select the **Modify User** link from the Choose User Action table and specify the following:

Parameter	Description
User Name	The user name of the user to be modified.
Full Name	The full name of the user.
Description	The description for this user.
Advanced Settings	
User Must change password at next logon	Specify whether the user has to change the password during the next logon or not.
User Cannot Change Password	Specify whether the user can change the password or not.
Password Never Expires	Specify whether the password should expire or not.
Account is Disabled	Specify whether the user account should be disabled or not.
Account is Locked	Specify whether the user account should be locked or not.
User Profile	
Member of	Specify the groups in which this user account is a member.
Logon Script	Specify the logon script that has to be executed during the user logon.

Parameter	Description
Profile Path	Specify the path where the user profiles has to be stored.
Local Path	Specify a local path as the home folder. For example, c:\users\johnsmith.
Connect Map To	If the user's home folder has to be stored in a network directory, select the drive letter in the **Connect Map** and specify the network path in the **To** field.

Note: If you wish to modify more users or to perform another action, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

To modify a setting from the **List of Settings** table, select the appropriate row and click icon and change the required values.

To delete a setting from the **List of Settings** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the User Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined User Management Configuration in the targets defined. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

See Also: Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Configuring Collections

A collection of Configurations can be deployed in the target client workstation using Desktop Central. The advantages of Collection are

- The targets are defined once for multiple Configuration.
- When the configuration is deployed, it saves time to apply the configuration since collection of configuration is applied in each workstation.

Step 1: Define Collection

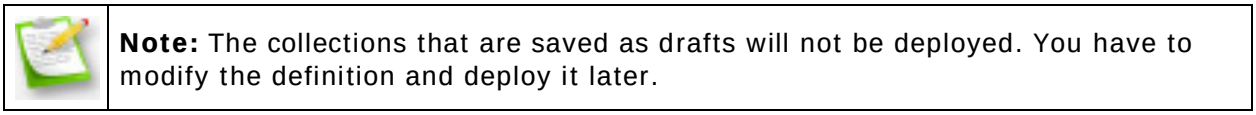
1. Click Add Collection link from the Quick Links.
2. Select the collection type as User Collection or Computer Collection. This opens the Add Collection Wizard.
3. Provide a name and description for the collection.
4. Choose the configurations that have to added to this collection and click Next. The configurations are specific to the collection type you have selected above.
5. Define the chosen configurations. Refer to User Configurations and Computer Configurations sections for details about the configurations.

Step 2: Define Target

Select the targets for which the configurations have to be applied. Refer to the Defining Targets topic for more details.

Step 3: Save or Deploy Collection

After defining the configurations and targets, click **Finish** to deploy the defined configurations to the selected targets. You also have an option to save the configurations as drafts for later modifications by clicking the **Save as Draft** button.



Note: The collections that are saved as drafts will not be deployed. You have to modify the definition and deploy it later.

Defining Targets

After defining the configuration, the configuration has to be deployed in the target client workstations. The target client workstations have to be defined for the configurations individually. Defining the targets involves selecting various types of targets given below:

The targets must be defined to deploy the Configuration in the machines of the network. When you add a configuration or collection of Configuration, you can find "Step 2" as **Define Target** in the GUI or in this documentation. This section explains the procedure to define the target for a configuration or collection of Configuration.

To define the targets for deploying the configuration or collection, the targets must be added to the **Target List**. A target can be added, removed or modified in the **Target List**.

Selecting Targets from a Domain

To add target computers and users from a Active Directory based domain, follow the steps below:

1. Select a domain from the list.
2. You can deploy the configuration to any of the following:
    1. **Site** - to deploy the configuration to all the users/computers of that site.
    2. **Domain** - to deploy the configuration to all the users/computers of that domain.
    3. **Organizational Unit** - to deploy the configuration to all the users/computers of that OU.
    4. **Group** - to deploy the configuration to all the users/computers of that Group.
    5. **User/Computer** - to deploy the configuration to the specified users/computers.
    6. **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
    7. **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.

3. After adding the target computers, you can specify the filtering criteria to exclude certain types of users/computers from applying the configuration. Specify the criteria as required.
4. Click **Add More Targets** and repeat steps 1 to 3 for adding more targets.

Note: If you wish to deploy the configuration for users/computers in different domains, use the **Add More Targets** button to add targets from multiple domains.

Selecting Targets from a Workgroup

To add target computers and users from a workgroup, follow the steps below:

1. Select a workgroup from the list.
2. You can deploy the configuration to any of the following:
    1. **Workgroup** - to deploy the configuration to all the users/computers of that workgroup.
    2. **User/Computer** - to deploy the configuration to the specified users/computers.
    3. **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
    4. **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.
3. After adding the target computers, you can specify the filtering criteria to exclude certain types of users/computers from applying the configuration. Specify the criteria as required.
4. Click **Add More Targets** and repeat steps 1 to 3 for adding more targets.

Note: If you wish to deploy the configuration for users/computers in different workgroups, use the **Add More Targets** button to add targets from multiple workgroups.

Selecting Targets in Remote Offices

To add target computers and users from remote offices, follow the steps below:

1. Select a remote office from the list. The remote office can either be a domain or a workgroup.
2. You can deploy the configuration to any of the following:
    1. **Site** - to deploy the configuration to all the users/computers of that site. This option is only available if the selected remote office is a domain.
    2. **Remote Office** - to deploy the configuration to all the users/computers of that remote office.
    3. **Organizational Unit** - to deploy the configuration to all the users/computers of that OU. This option is only available if the selected remote office is a domain.
    4. **Group** - to deploy the configuration to all the users/computers of that Group. This option is only available if the selected remote office is a domain.

5. **User/Computer** - to deploy the configuration to the specified users/computers.
6. **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
7. **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.

3. After adding the target computers, you can specify the filtering criteria to exclude certain types of users/computers from applying the configuration. Specify the criteria as required.
4. Click **Add More Targets** and repeat steps 1 to 3 for adding more targets.

Note: If you wish to deploy the configuration for users/computers in different remote offices, use the **Add More Targets** button to add targets from multiple domains.

Filter the selected target

You can exclude certain parts of the network which does not require the configuration to be deployed. This is optional when defining the targets. Desktop Central provides the option to exclude the parts of the Windows network. Select the Exclude Target check box to view the available options:

Exclude if Target Type is

The target types can be excluded which are in the lower hierarchy to the target selected in the **Select the target type and define** field. The target type can be excluded using the **Browse** button. Click the **Browse** button next to the required target types under the **Exclude if Target Type is** field to launch **Network Browser** window. Select the target type to be excluded for configuration deployment and click **Select** button. This field is mandatory. The target type can be any of the following (varies based on the target options selected):

- Branch - The branch offices to be excluded
- Domain - The domains to be excluded
- Organization Unit - The OUs to be excluded
- Group - The groups to be excluded
- Computer - The computers to be excluded
- IP Address - The IP Addresses to be excluded
- IP Range - The range of IP Addresses to be excluded
- Custom Group - The custom groups to be excluded

Exclude if Operating System is

The targets with specific Windows OS can be excluded for configuration deployment. Select the options under the **Exclude if Operating System is** field which has to excluded for configuration deployment.

Exclude if Machine Type is

The targets with specific machine type such as Notebook, Tablet PC, Desktop, Member Server, TermServClient, or Domain Controller can be excluded for configuration deployment. Select the options under the **Exclude if Machine Type is** field which has to excluded for configuration deployment.

Modifying a Target

To modify a target in the Target List, follow these steps:

1. Select the button under **Actions** column in the desired row that has to modified.
2. Change the targets as required and click the **Modify Target** button. The target details are updated in **Target List**.

Deleting a Target

To delete a row in the **Target List**, select the button under **Actions** column next to target that has to removed.

Managing Configurations and Collections

Clicking the **View Configuration** from the Quick Links will list the details of the configurations and collections that are defined using Desktop Central. You can view the details of the configurations by clicking the corresponding configuration name. Apart from viewing the configuration details, you can perform the following actions:

- Modify the Configuration/Collection
- Suspend a Configuration/Collection
- Resume a suspended Configuration/Collection

Viewing Status of Configuration/Collection

To view the status of the defined configuration/collection, follow the steps given below:

1. Click **View Configuration** from the Quick Links. This opens the All Configurations page.
2. All the configurations and collections that are defined are listed here. The status column provides the current status of the configuration/collection. The table given below lists the various states of the configuration/collection and its description:

Status	Description
Draft	Represents the configurations/collections that are saved as draft.
Ready To Execute	Represents the configurations/collections that are ready for execution. This will be the initial state of the deployed configurations/collections.
In Progress	Represents that the configuration is applied on one or more targets. Will continue to remain in this state until the configurations are applied to all the defined targets.
Suspended	Represents that the configuration/collection has been suspended.
Executed	Represents that the configuration/collection has been applied to all the defined targets.

3. To view the status of the configurations on individual targets, click the configuration name.

Modifying the Configuration/Collection

To modify a configuration/collection, follow the steps given below:

1. Click **View Configuration** from the Quick Links. This opens the All Configurations page.
2. All the configurations and collections that are defined are listed here. Click the icon from the Actions column of the corresponding configuration/collection.
3. Change the values as required.
4. Click **Deploy**.

Suspending the Configuration/Collection

To suspend a configuration/collection, follow the steps given below:

1. Click **View Configuration** from the Quick Links. This opens the All Configurations page.
2. All the configurations and collections that are defined are listed here. Click the icon from the Actions column of the corresponding configuration/collection that has to be suspended.

	Note: Configurations that have been applied to targets prior to suspension will not be reverted. Suspending a configuration will only stop further deployments.

Resuming the Suspended Configuration/Collection

To resume a suspended configuration/collection, follow the steps given below:

1. Click **View Configuration** from the Quick Links. This opens the All Configurations page.
2. All the configurations and collections that are defined are listed here. Click the icon from the Actions column of the corresponding configuration/collection that has to be resumed.

Viewing System Uptime Report

Provides the total uptime and downtime of the computers in the network for a given period. The report can be filtered to view computers in a specific domain and period. To view the report, select **Reports --> Power Management Reports --> System Uptime Report**

Configuring Data Storage Period

Desktop Central, by default, stored the uptime/downtime details of all the computers for a period of 30 days. This can be configured to suit your need. To specify the period,

1. Click Edit Settings link. This is open the Power Report Settings dialog.
2. Specify the number of days you wish to store the data and click Apply.

Viewing Report for a Specified Period

1. Select the Domain or select All Domains to view the uptime of all the computers.
2. Select a period from the list. To specify a custom period, click Select Custom Date and specify the start and end dates.
3. Specify the start and end time for which the report has to be displayed. If you wish to see the complete details, specify the start and end time as 00:00 and 23:59 respectively.
4. Selecting the "Consider hibernate/standby as shutdown" option will show the hibernate/standby periods as downtime.
5. Click Apply Fileter to view the report based on the specified criteria.

Viewing Detailed Uptime Report

Desktop Central will display the summary view of the total uptime and downtime of the computers based on the selected criteria. Selecting the Detail Report option will display the start and shutdowm times of the computers for the given period. You can also click the computer name to view its detailed and summary reports.

Exporting the Report

The System Uptime Report can be exported to a PDF or a CSV format by clicking the respective options from the top-right. The current report that is being displayed will be exported to the selected format.

Viewing Configuration Reports

The Configuration reports helps the administrators to view the details of the configurations that are applied on users, computers, and based on the configuration type. To view the reports, follow the steps given below:

1. Click the **Reports** tab to invoke the **Reports** page.
2. Click the desired report from the Configuration Reports.

The Configuration Reports includes the following reports:

- Configuration by User
- Configuration by Computer
- Configurations by Type

Configuration by User

This report provides a list of users for whom configurations were applied using Desktop Central. It also provides details about the total number of configurations applied for a particular user and the last configuration and time at which it was applied. Clicking the user name will list the details of the configurations applied for that user.

You also have an option to filter your view based on the time at which the configuration was applied or by the configuration type.

Configuration by Computer

This report provides a list of computers for which configurations were applied using Desktop Central. It also provides details about the total number of configurations applied for that computer and the last configuration and time at which it was applied. Clicking the computer name will list the details of the configurations applied for that machine.

You also have an option to filter your view based on the time at which the configuration was applied or by the configuration type.

Configurations by Type

This report provides you the list of configurations that have been applied on users and computers based on the configuration type. It also provides you the total number of configurations that have been applied for a particular type and the last configuration, and time at which it was applied.

Configuration Templates

Templates are predefined configurations that help in achieving a specific task. While you can perform any of these configurations by defining them on your own, templates helps to get things done faster. The following are advantages of Templates over the normal configurations:

1. Helps to complete the configurations quickly.
2. You do not need to know how to achieve a specific task; just need to select the target computers to apply the configuration.
3. You does not have to explore all the supported configurations and then select to define.

Using Templates

To view the available templates, select the Admin tab and click the Templates link from the left. This will list all the templates provided by Desktop Central. You can also filter the view by selecting an appropriate category from the combo box. The Type column indicates whether the configuration is applied to Users or Computers. The templates are tagged as below:

- Control Panel
- Hard Disk Maintenance
- Internet Explorer
- Network
- Power Management
- Proxy Configuration
- Restrict Media
- Security
- Service Management
- System Tools
- USB Security
- User Management
- XP Firewall Management

To use the template, follow the steps below:

1. Select Admin --> Templates to view the templates.
2. Click the Template that has to be applied to view its details; click the **Create from Template** button to create the configuration. Clicking **Create Configuration** link will also do the same action. This opens the configuration with all the properties defined.

3. Using the Defining Targets procedure, define the targets for deploying the configuration.
4. Click the **Deploy** button to deploy the defined Configuration in the targets defined. To save the configuration as draft, click **Save as Draft**.

Supported Templates

Desktop Central supports various templates that can be applied to Users/Computers. Follow the links below to view the details of the templates:

- Computer Configuration Templates
- User Configuration Templates

Computer Configuration Templates

Change local admin account password

To enhance the security, the administrators will prefer to change the password periodically. This template enables you to change the password of the local administrator account in the client machines.

Cleanup Recycle bin to free-up Hard Disk space

This helps in freeing up the hard disk space by removing the unwanted files/data from 18 different locations.

Create Alternate local Admin Account

To keep the computers secured, the administrators will prefer to change the local administrator account periodically. This template enables you to create an alternate local administrator account in the client computers.

Defrag Hard Disk for performance

A fragmented disk reduces the performance. It is recommended to defragment the disk periodically to improve the hard disk performance.

This template enables defragmentation of the hard disk at the scheduled time.

Delete local Administrator Account

This template enables you to delete the local administrator account in the client computers.

Disable the USB drives

To prevent data theft, the administrators prevent the users from using USB drives. This template, when applied to client computers, prevent them from using the USB drives.

Disable Unused local Guest account

Unused guest accounts are vulnerable points for the hackers. It is recommended to delete or disable any unused guest accounts from the client computers to avoid any misuse.

This template helps to disable the unused guest accounts from the client computers.

Open MEDC ports for communication

Desktop Central requires port 8021 for agent server communications and port 6100 for Remote Desktop Sharing. These port should not be blocked by the Windows Firewall for smooth functioning.

This template, when applied to client computers, will open up these ports to enable proper communication between the agent and server.

Restrict CD-ROM access

This template restrict the users form accessing the CD-ROM drives.

Restrict Floppy Access to locally logged on users

Allowing locally logged on users to access the floppy drives is a vulnerable point for hacking. Administrators prefer to disable access to the floppy drives when the users have not logged on to the domain.

This template helps in restricting the locally logged on uses to access the floppy drives.

Scan and Fix Hard disk Errors

The hard disks have to be periodically scanned for any errors and fix them. This will improve the life and performance of the disk.

This template enables scanning and fixing the hard disk errors in the client machines at the scheduled time.

Start MEDC Agent Service

When Scope of Management is defined, Desktop Central agent is installed in all the client computers that are within the scope. The Desktop Central agent has to be running as a service in the client computers to ensure proper communication with the Desktop Central Server.

This template helps you to start the Desktop Central Agent service in the client computers.

Write Protect the USB Storage Devices

To prevent data theft, the administrators prevent the users from writing data to USB storage devices. This template, when applied to client computers, prevent them from writing any data to the USB storage devices.

User Configuration Templates

Restrict Network Connections

Network properties when changed by the user result in bad network connectivity and unnecessary help desk calls in resolving the problem. This could be avoided by restricting the users from changing the network properties.

This template, when applied to users, will prevent them from changing the network properties.

Restrict Control Panel Applets

To enhance the security, the administrators can restrict the users from accessing specific Control Panel applets. This includes, Add/remove programs, Add/remove hardware, Internet options, Power options and System applet.

Proxy configuration for Internet Explorer

This template can be used to configure proxy server settings in the Internet Explorer browser of the client machines.

Laptop Power Saver Scheme

Establishing correct power settings helps in saving energy costs substantially. This template provides the recommended power settings for Laptops.

IE Browser restrictions for clients

This template restricts users from changing the Internet Explorer settings like Connections, Content, Favorites, Programs, Security, Advanced, History and Save As options

Disable Control Panel

You can use this template to disable the Control Panel completely. When applied to users, the users will not be able to access the Control Panel.

User Logon Reports

How are these reports generated?

These reports are generated with the help of the Desktop Central Agents installed in the client systems to track the user logon details

What way does it differ from Active Directory Reports?

In the case of Active Directory reports, if multiple domain controllers are used, the synchronization of data between the domain controllers happens at regular intervals and not very frequently. Hence the reports derived from the Active Directory may not be the latest or actual. To provide the current reports of the logon details, Desktop Central agent is used.

In addition to the current details, it also provides the logon history details, which is not available in the Active Directory reports.

Is there any limitation?

Yes, these reports are available only to the users and computers that fall within the defined scope of management. Also, when an user logs in and logs out immediately, this may not be tracked.

- Setting Up User Logon Reports
- Viewing User Logon Reports

Viewing User Logon Reports

To view the User Logon Reports, select the Reports tab and click the User Logon Reports link from the left pane. The User Logon Reports are classified under the following headings; click the links to learn more:

- General Reports
- Usage Reports
- History Reports

General Reports

Currently Logged on Users

Provides the list of users who are currently logged on to the domain.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Currently Logged on Users** link available under the General Reports category.

Currently Logged on Computers

Provides the list of computers from where users have logged on to the domain.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Currently Logged on Computers** link available under the General Reports category.

Usage Reports

Computers with No User Logon

Provides the list of computers where no user have logged on.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Computers with No User Logon** link available under the Usage Reports category.

History Reports

User Logon History

Provides the list of history of users who have logged on to the domain in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **User Logon History** link available under the History Reports category.

User Logon History by Computers

Provides the list of computers and their corresponding user logon history in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **User Logon History by Computers** link available under the History Reports category.

Domain Controllers with Reported Users

Provides the list of users and their corresponding Domain Controllers (logon servers) in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Domain Controllers with Reported Users** link available under the History Reports category.

User Logon History on Domain Controller

Provides the list of domain controllers and their corresponding user logon history in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **User Logon History by Domain Controllers** link available under the History Reports category.

Active Directory Reports

Desktop Central gives you an insight into the Active Directory by providing reports on various Active Directory components. The reports can be accessed by selecting the Reports tab from the client window. The following reports about the Active Directory are shown:

- Active Directory User Reports
- Active Directory Computer Reports
- Active Directory Group Reports
- Active Directory Organization Unit Reports
- Active Directory Domain Reports
- Active Directory GPO Reports

More granular reports are provided for each of the above components.

Active Directory Report Features

- Ability to generate reports for custom inputs for granularity.
- Customizable columns in all the reports.
- Columnar sorting of reports
- Export reports in PDF and CSV formats.
- Ability to synchronize report data with Active Directory at regular intervals.

Active Directory User Reports

To access the User Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page. The User Reports is selected by default.
2. Select the required link to view the reports.

Follow the links to learn more about the various User Reports provided by Desktop Central

- Active Directory General User Reports
- User Account Status Reports
- Password Based User Reports
- Privileged User Reports
- Logon Based User Reports

Active Directory General User Reports

All User Accounts

Provides the details of all the users of the domain that the system/user running the Desktop Central belongs to.

To view the report, click the **All User Accounts** link available under the General Reports category. Clicking a user from the report displays the complete user information of that user.

Recently Created User Accounts

Provides the details of the user accounts that are created recently. This is determined based on the value contained in the *createTimeStamp* attribute of the Active Directory.

To view the report, click the **Recently Created User Accounts** link available under the General Reports category.

By default, the users created for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a user from the report displays the complete information of that user.

Recently Modified User Accounts

Provides the details of the user accounts modified recently. This is determined based on the value contained in the *modifyTimeStamp* attribute of the Active Directory.

To view the report, click the **Recently Modified User Accounts** link available under the General Reports category.

By default, the user accounts modified for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a user from the report displays the complete information of that user.

User Accounts without Logon Scripts

Provides the details of the users who do not have any scripts executed during their logon to the domain. This is determined based on the value contained in the *scriptPath* attribute of the Active Directory.

To view the report, click the **User Accounts without Logon Scripts** link available under the General Reports category. Clicking a user from the report displays the complete information of that user.

User Accounts in Multiple Groups

Provides the details of the user accounts that are in more than one groups. This also includes the nested groups i.e., groups that contain other groups as its members in the domain.

To view the report, click the **User Accounts in Multiple Groups** link available under the General Reports category.

User Accounts that Never Expires

Provides the list of user accounts that never expires. This is determined based on the value contained in the *userAccountControl* of the Active Directory.

To view the report, click the **User Accounts that Never Expires** link available under the General Reports category.

User Account Status Reports

Active User Accounts

Provides the list of users who have logged on to the domain in the past 30/60/90/180 days. This is determined based on the value contained in the *lastLogon* attribute of the Active Directory.

To view the report, click the **Active User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Inactive User Accounts

Provides the list of users who have not logged on to the domain in the past 30/60/90/180 days. This is determined based on the value contained in the *lastLogon* attribute of the Active Directory.

To view the report, click the **Inactive User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Disabled User Accounts

Provides the list of user accounts that are disabled by the administrator. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Disabled User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Locked User Accounts

Provides the details of the user accounts that have been locked out. The user account will get locked on frequent bad login attempts. The Account Lock Out Policy specifies the allowed number of bad login attempts after which the account will be locked. The account will be automatically unlocked after sometime. The locked user accounts are determined based on the value contained in the *lockoutTime* attribute of the Active Directory.

To view the report, click the **Locked User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Expired User Accounts

Provides the details of the user accounts that have expired. This is determined based on the value contained in the *accountExpires* attribute of the Active Directory.

To view the report, click the **Expired User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Password Based User Reports

Soon-to-Expire User Passwords

Provides the details of the users whose password will expire within the specified number of days. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Soon-to-Expire User Passwords** link available under the Password Based Reports category.

By default, the users whose passwords will expire in another seven days is shown. You can select a different period to view the report. Clicking a user from the report displays the complete information of that user.

Password Expired User Accounts

Provides the details of the users whose password has expired. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Password Expired User Accounts** link available under the Password Based Reports category. Clicking a user from the report displays the complete information of that user.

Password Never Expiring User Accounts

Provides the list of users whose password never expires. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Password Never Expiring User Accounts** link available under the Password Based Reports category. Clicking a user from the report displays the complete information of that user.

User Accounts Password that cannot be Changed

Provides the list of users who cannot change their password. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **User Accounts Password that cannot be Changed** link available under the Password Based Reports category. Clicking a user from the report displays the complete information of that user.

Privileged User Accounts

Domain Admin User Accounts

Provides the list of users who have domain administrative privileges.

To view the report, click the **Domain Admin User Accounts** link available under the Accounts with Privileged User Accounts category.

User Accounts with Dial-in Permissions

Provides the list of users who have dial-in permissions to access the domain. This is determined based on the value contained in the *msNPAllowDialinattribute* of the Active Directory.

To view the report, click the **User Accounts with Dial-in Permissions** link available under the Privileged User Accounts category.

Logon Based User Reports

Unused User Accounts

Provides the list of users who have not logged on to the domain since creation of the account. This is determined based on the value contained in the *lastLogon* of the Active Directory.

To view the report, click the **Unused User Accounts** link available under the Logon Based Reports category. Clicking a user from the report displays the complete information of that user.

Recently Logged On User Accounts

Provides the details of the users who have logged on in the past n days. The recently logged on users are determined based on their last logon time.

To view the report, click the **Recently Logged On User Accounts** link available under the Logon Based Reports category.

By default, the users logged on for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a user from the report displays the complete information of that user.

Last Logon Failed User Accounts

Provides the list of users whose last logon has failed. This is determined based on the value contained in the *badPasswordTime* and *badPwdCount* attributes of the Active Directory.

To view the report, click the **Last Logon Failed User Accounts** link available under the Logon Based Reports category. Clicking a user from the report displays the complete information of that user.

Active Directory Computer Reports

To access the Computer Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **Computer Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various Computer Reports provided by Desktop Central

- General Computer Reports
- Server Based Reports
- Computer OS Based Reports

General Computer Reports

All Computers

Provides the list of all the computer accounts available in the domain.

To view the report, click the **All Computers** link available under the General Reports category. Clicking a computer account from the report displays the complete information of that account.

Windows Workstation

Provides the details of the workstations in the domain. All the computers except Servers and Domain Controllers are termed as workstations.

To view the report, click the **Windows Workstation** link available under the General Reports category. Clicking a computer account from the report displays the complete information of that account.

Recently Added Computers

Provides the details of the computer objects that are created recently. This is determined based on the value contained in the *createTimeStamp* attribute.

To view the report, click the **Workstations** link available under the General Reports category.

By default, the report displays the computer accounts that are created in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a computer account from the report displays the complete information of that account.

Recently Logged On Computers

Provides the list of computer accounts through which an user has logged on to the domain. This is determined based on the value contained in the *lastLogon* attribute.

To view the report, click the **Recently Logged On Computers** link available under the General Reports category.

By default, the report displays the computer accounts through which an user has logged on to the domain in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a computer account from the report displays the complete information of that account.

Recently Modified Computer Accounts

Provides the details of the computer objects that are modified recently. This is determined based on the value contained in the *ModifyTimeStamp* attribute.

To view the report, click the **Recently Modified Computer Accounts** link available under the General Reports category.

By default, the report displays the computer accounts that are modified in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a computer account from the report displays the complete information of that account.

Disabled Computer Accounts

Provides the list of computer accounts that are disabled in the domain. This is determined based on the value contained in the *userAccountControl* of the Active Directory.

To view the report, click the **Disabled Computer Accounts** available under General Reports category. Clicking a computer account from the report displays the complete information of that account.

Computer Accounts by OU

Provides the list of computer accounts filtered by the OU it belongs to.

To view the report, click the **Computers Accounts by OU** available under General Reports category.

By default, the computer accounts of all the OUs in the domain are listed. Browse to select a specific OU and click **Generate** to view the computer accounts of that OU. Clicking a computer account from the report displays the complete information of that account.

Server Based Reports

Windows Servers

Provides the list of Windows Servers in the domain. This is determined based on the value contained in the *operatingSystem* attribute of the Active Directory.

To view the report, click the **Windows Servers** link available under the Server Based Reports category. Clicking a computer account from the report displays the complete information of that account.

Member Servers

Provides the details of the member servers in the domain.

To view the report, click the **Member Servers** link available under the Server Based Reports category. Clicking a computer account from the report displays the complete information of that account.

Domain Controllers

Provides the details of the domain controllers in the domain.

To view the report, click the **Domain Controllers** link available under the Server Based Reports category. Clicking a computer account from the report displays the complete information of that account.

Computer OS Based Reports

Computers by OS Service Pack

Provides the details of the computers based on the operating system and service pack versions.

To view the report, click the **Computers by OS Service Pack** available under OS Based Reports category. Select the Operating System and the Service Packs to filter the view. Clicking a computer account from the report displays the complete information of that account.

Active Directory Group Reports

To access the Group Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **Group Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various Group Reports provided by Desktop Central

- General Group Reports
- Group Type Reports
- Group Member Based Reports

Active Directory General Group Reports

All Groups

Provides the details of all the groups of the domain.

To view the report, click the **All Groups** link available under the General Reports category. Clicking a group from the report displays the complete information of that group.

Recently Created Groups

Provides the details of all the groups that are recently created. This is determined based on the value contained in the *createTimeStamp* of the Active Directory.

To view the report, click the **Recently Created Groups** link available under the General Reports category.

By default, the groups created for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a group from the report displays the complete information of that group.

Recently Modified Groups

Provides the details of all the groups that are recently modified. This is determined based on the value contained in the *modifyTimeStamp* of the Active Directory.

To view the report, click the **Recently Modified Groups** link available under the General Reports category.

By default, the groups modified in the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a group from the report displays the complete information of that group.

Groups by OU

Provides the list of groups filtered by the OU it belongs to.

To view the report, click the **Groups by OU** link available under the General Reports category.

By default, the groups of all the OUs in the domain are listed. Browse to select a specific OU and click **Generate** to view the groups of that OU. Clicking a group from the report displays the complete information of that group.

Active Directory Group Type Reports

Security Groups

Provides the details of the security groups available in the domain. This is determined based on the value contained in the *groupType* attribute of the Active Directory.

To view the report, click the **Security Groups** link available under the Group Type Based Reports category. Clicking a group from the report displays the complete information of that group.

Distribution Groups

Provides the details of the distribution groups available in the domain. This is determined based on the value contained in the *groupType* attribute of the Active Directory.

To view the report, click the **Distribution Groups** link available under the Group Type Based Reports category. Clicking a group from the report displays the complete information of that group.

Member Based Reports

Groups with Member Details

Provides the details of the groups with its member count, such as no. of users, computers, groups, etc.

To view the report, click the **Groups with Member Details** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Groups with Maximum Members

Provides the details of the large groups in the domain based on its members count.

To view the report, click the **Groups with Maximum Members** link available under the Member Based Reports category. You can customize the report by selecting the member count. Clicking a group from the report displays the complete information of that group.

Groups without Members

Provides the list of groups that do not have any members.

To view the report, click the **Groups without Members** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

User-only Groups

Provides the list of groups that have only users as its members.

To view the report, click the **User-only Groups link** available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Computer-only Groups

Provides the list of groups that have only computers as its members.

To view the report, click the **Computer-only Groups** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Nested groups

Provides the list of nested groups (groups within groups) in the domain.

To view the report, click the **Nested groups** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Active Directory Organization Unit Reports

To access the Organization Unit Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **OU Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various OU Reports provided by Desktop Central

- Active Directory General OU Reports
- OU Child Based Reports

Active Directory General OU Reports

All OUs

Provides the list of all the OUs of the domain.

To view the report, click the **All OUs** link available under the General Reports category. Clicking an OU from the report displays the complete information about that OU.

Recently Created OUs

Provides the list of OUs that are recently created. This is determined based on the value contained in the *createTimeStamp* attribute.

To view the report, click the **Recently Created OUs** link available under the General Reports category.

By default, the report displays the OUs created in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking an OU from the report displays the complete information about that OU.

Recently Modified OUs

Provides the list of OUs that are recently modified. This is determined based on the value contained in the *ModifyTimeStamp* attribute.

To view the report, click the **Recently Modified OUs** link available under the General Reports category.

By default, the report displays the OUs modified in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking an OU from the report displays the complete information about that OU.

OU Child Based Reports

OUs with Child Details

Provides the list of OUs with its child details, like no. of users, computers, groups, and OUs.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

OUs without Children

Provides the list of OUs that do not have any children.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

User-only OUs

Provides the list of OUs that have only users as their children.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

Computer-only OUs

Provides the list of OUs that have only computers as their children.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

Nested OUs

Provides the list of OUs that nested (OUs within OUs).

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

Active Directory Domain Reports

To access the Domain Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **Domain Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various Domain Reports provided by Desktop Central

- Active Directory General Domain Reports
- Active Directory Container Reports

General Domain Reports

Active Directory Sites

Active Directory Site Report provides the list of Sites with their attributes, such as Site name, subnet, netmask, and domain controller. Clicking a site from the report provides more details, such as the number of computers in each subnet, creation time, modified time, and so on.

To view the report, Click the **Active Directory Sites** link available under the General Reports category.

Active Directory Domains

Active Directory Domain Report provides the complete information of domain with the fully qualified Domain name, creation time, modified time, location, and its members.

To view the report, Click the **Active Directory Domains** link available under the General Reports category.

Active Directory Printers

Active Directory Printer Report provides the list of printers with their attributes such as name, host server name, model of printer, physical location and share name. Clicking the printer from the report gives details, such as Domain name, Active Directory URL, Model, Physical location, Share name, Modified time, Creation time, Printer Hosted Server name, Driver name, and Port name.

To view the report, Click the **Active Directory Printers** link available under the General Reports category.

Group Policy Creator Owners

Provides the members of Group Policy Creator Owners (GPCO) group. The members of this group can modify group policy for the domain.

To view the report, click the **Group Policy Creator Owners** link available under the General Reports category.

Container Based Reports

Users In "Users" Container

Provides the list of users in the "users" container of the domain.

To view the report, click the **Users In "Users" Container** link available under the Container Based Reports category.

Groups In "Users" Container

Provides the list of groups in the "users" container of the domain.

To view the report, click the **Groups In "Users" Container** link available under the Container Based Reports category.

Computers In "Computer" Container

Provides the list of computers in the "computer" container of the domain.

To view the report, click the **Computers In "Computer" Container** link available under the Container Based Reports category.

Groups In "Builtin" Container

Provides the list of groups in the "Builtin" container of the domain.

To view the report, click the **Groups In "Builtin" Container** link available under the Container Based Reports category.

Active Directory GPO Reports

To access the GPO Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **GPO Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various GPO Reports provided by Desktop Central

- General GPO Reports
- GPO Link Based Reports
- Inheritance Based Reports
- GPO Status Based Reports
- Special GPO Reports

General GPO Reports

All GPOs

Provides the list of GPOs that are created in the domain.

To view the report, click the **All GPOs** link available under the General Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Recently Created GPOs

Provides the list of GPOs that are recently created in the domain.

To view the report, click the **Recently Created GPOs** link available under the General Reports category. This is determined based on the value contained in the *createTimeStamp* attribute.

By default, the report displays the GPOs created in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a GPO from the report displays the complete information about that GPO.

Recently Modified GPOs

Provides the list of GPOs that are recently modified in the domain. This is determined based on the value contained in the *ModifyTimeStamp* attribute

To view the report, click the **Recently Modified GPOs** link available under the General Reports category.

By default, the report displays the GPOs modified in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a GPO from the report displays the complete information about that GPO.

GPOs by OUs

Provides the list of OUs and their linked GPOs.

To view the report, click the **GPOs by OUs** link available under the General Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPO Link Based Reports

GPOs Linked To OUs

Provides the list of GPOs that are linked to OUs in the domain. This is determined based on the value contained in the *gPLink* attribute of the Active Directory.

To view the report, click the **GPOs Linked To OUs** link available under the GPO Link Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs Linked To Domains

Provides the list of GPOs that are linked to domains. This is determined based on the value contained in the *gPLink* attribute of the Active Directory.

To view the report, click the **GPOs Linked To Domains** link available under the GPO Link Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs Linked To Sites

Provides the list of GPOs that are linked to sites. This is determined based on the value contained in the *gPLink* attribute of the Active Directory.

To view the report, click the **GPOs Linked To Sites** link available under the GPO Link Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Inheritance Based Reports

Block Inheritance enabled OUs

Provides the list of OUs that are prevented from inheriting GPOs from any of its parent container. This is determined based on the value contained in the *gPOptions* attribute of the Active Directory.

To view the report, click the **Block Inheritance enabled OUs** link available under the Inheritance Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Block Inheritance enabled Domains

Provides the list of domains that are prevented from inheriting GPOs from any of its parent container. This is determined based on the value contained in the *gPOptions* attribute of the Active Directory.

To view the report, click the **Block Inheritance enabled Domains** link available under the Inheritance Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Enforced GPOs

Provides the list of GPOs that have the enforced flag set. Enforced GPOs when applied to OUs are also applied to their children irrespective of whether Block Inheritance is set or not.

To view the report, click the **Enforced GPOs** link available under the Inheritance Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPO Status Based Reports

User Settings Enabled GPOs

Provides the list of GPOs that have Computer Settings disabled. These GPOs can be used to make the user settings.

To view the report, click the **User Settings Enabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Computer Settings Enabled GPOs

Provides the list of GPOs that have User Settings disabled. These GPOs can be used to make the computer settings.

To view the report, click the **Computer Settings Enabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

User and Computer Settings Enabled GPOs

Provides the list of GPOs that can be used to perform both user and computer settings.

To view the report, click the **User and Computer Settings Enabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Disabled GPOs

Provides the list of GPOs that have both User and Computer Settings disabled.

To view the report, click the **Disabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Unused GPOs

Provides the list of GPOs that are not used since creation.

To view the report, click the **Unused GPOs**link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Special GPO Reports

GPOs with Most Modified User Settings

Provides the list of GPOs that have user versions greater than 5. You have an option to select a different version number.

To view the report, click the **GPOs with Most Modified User Settings** link available under the GPO Version Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs with Most Modified Computer Settings

Provides the list of GPOs that have computer versions greater than 5. You have an option to select a different version number.

To view the report, click the **GPOs with Most Modified Computer Settings** link available under the GPO Version Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs with Most Modified User & Computer Settings

Provides the list of GPOs that have user or computer versions greater than 5. You have an option to select a different version number.

To view the report, click the **GPOs with Most Modified User & Computer Settings** link available under the GPO Version Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Custom Reports

While Desktop Central provides various canned reports on different modules like Patch Management, Asset Management, and so on, it is also possible to create customized reports to meet your specific requirement. Follow the links to learn more

- Wizard Based Custom Report
- Custom Query Report

Creating Custom Reports

In addition to the out-of-the-box reports, Desktop Central allows you to create custom reports by specifying the criteria and selecting the required parameters. Follow the steps below to create a custom report using Desktop Central:

1. Select the **Reports** tab from the Desktop Central Client.
2. Click the **New Custom Report** button available on the top-right. This opens the Custom Report page.
3. Specify the name for the report.
4. Select the Module. This is currently available only for the Asset Management module and will be extended for other modules in our subsequent updates.
5. Select the Sub Module as Computer, Hardware or Software.
6. Specify the criteria for generating the report. You can specify multiple criteria by clicking the "+" icon
7. Select the Columns to view in the report. You can change the position of the columns by using the up and down arrow icons.
8. Click on **Run & Save** button to save the report permanently. (or) Click **Run Report** if just a temporary report is needed.

   Note: If you choose the **Run Report** option, you can edit the report and later on save the same. Likewise if you intend to make any changes to a saved report, you can make use of the Edit option in the **Custom Report** Page.

9. You have an option to save this report as PDF and CSV formats.

Custom Query Report

Desktop Central provides the following types of reports:

- Canned reports on various modules like Patch Management, Asset Management, Active Directory, and so on.
- Wizard-based Custom Reports to retrieve any specific information

In addition to the above report types, it also provides an ability to retrieve the required information from the database using the Query Report. This might be useful in cases where you are not able to get the required information from the Canned or the Custom Reports.

The Query Report can be created using the **New Query Report** button available under **Reports tab --> Custom Report**. You may have to provide the SQL Query and create the report. The report can be saved for future reference and / or exported to CSV format for further processing.

From where can I get the Query?

Contact desktopcentral-support@manageengine.com with the details of your requirement. Alternatively, you can also submit your request online.

Our support team will process your requirement and send you the query.

Built-in Date Functions

Date is stored in the Long format in the database. You will not be able to interpret the date on seeing this long format. In order to convert this to readable date format, two built-n functions are included:

- LONG_TO_DATE() - for displaying the date in the results
- DATE_TO_LONG() - for using the date within the query

LONG_TO_DATE()

This function can be used to convert the date from the long value to the date format. Consider the following example:

You wish to retrieve software details along with the date and time at which the software was detected. The query you would normally use is:

```
Select SOFTWARE_NAME, DETECTED_TIME from invsoftware

SOFTWARE_NAME        DETECTED_TIME

Adobe Reader         1234558984892

Skype                8945934747893
```

In the above result, you will see the Detected Time in long format, which is not readable. Now, modifying the query as below will give you the desired output

```
Select SOFTWARE_NAME, LONG_TO_DATE(DETECTED_TIME) from
invsoftware



SOFTWARE_NAME        DETECTED_TIME_DATE_FORMAT

Adobe Reader         09/12/2009 15:35

Skype                07/13/2009  13.25
```

DATE_TO_LONG()

This function can be used to convert the Date format to Long value. Consider the example where you wish to retrieve the details of the software detected between two specific dates. You should use the query as below:

```
select * from invsoftware where DETECTED_TIME between
DATE_TO_LONG(08/01/2009 00:00:00) and

DATE_TO_LONG(08/31/2009 00:00:00)
```

The date should be specified in the following format: mm/dd/yyyy hh:mm:ss

Date Templates

For retrieving the data between some predefined dates, you can make use of the date templates. The following date templates are supported:

- Today - <from_today> - <to_today>
- Yesterday - <from_yesterday> - <to_yesterday>
- This Week - <from_thisweek> - <to_thisweek>
- Last Week - <from_lastweek> - <to_lastweek>
- This Month - <from_thismonth> - <to_thismonth>

- Last Month - <from_lastmonth> - <to_lastmonth>
- This Quarter - <from_thisquarter> - <to_thisquarter>
- Last Quarter - <from_lastquarter> - <to_lastquarter>

Making Help Desk Requests

The Users of the computers that are managed using Desktop Central can submit help desk requests from the Desktop Central Icon displayed in the system tray. Right-clicking the Tray Icon will display the following menus:

1. Send Request to Help Desk - to make a helps desk request
2. Apply User Configurations - to apply the configurations that are available for them.
3. Apply Computer Configurations - to apply the configurations that are available for all the users of that computer.
4. Scan and Upload Patch Details - to manually scan and update the server for Patch Management
5. Scan and Upload Inventory Details - to manually scan and update the server with software/hardware inventories.
6. View User Logon Reports - to view their login history.

Please note that the Administrator should have enabled these options for the users to view and use.

Appendix

This section includes the following topics:

- Interpreting Error Messages
- Knowledge Base
- FAQs
- Security Policies
- Windows System Tools
- Data Backup and Restore
- Dynamic Variables
- Limitations
- Glossary

Interpreting Error Messages

1001: Storage Error Occurred

The configurations defined using Desktop Central are stored in the database. If we are unable to store the configuration details, this error message is shown. The reasons could be any of the following:

- Could not establish connection with the database.
- Violations in data definitions.

1002: Unknown error

This error is shown when any runtime error occurs, which is not defined in Desktop Central. Please contact desktop central support with the details of the error.

1003: DB Error

This error is shown when the database connection is lost.

1004: DB Error

This error message is shown when you try to access the data, which has been deleted from the database.

1010: Invalid User

While defining the scope of management, if the user name provided is invalid, this error message is shown.

1011: User is already Inactive

When you try to add an user which is already present in the Inactive User list, this error message is shown.

1101: Invalid Container name

While defining targets for the configuration or while defining the scope of management, if an invalid / nonexistent container name is given this error occurs. The error message is shown, when you click Add more targets button or during deployment.

1103: Group Policy Object (GPO) creation failed

For every configuration a Group Policy Object (GPOs) will be created. When the GPO could not be created due to some access restrictions, etc., this error is shown.

1104: Group Policy Object (GPO) deletion failed

When an already defined configuration is deleted, the corresponding GPO is also deleted. This error is shown, when the GPO could not be deleted.

1105: Group Policy Object (GPO) linking failed

When a configuration defined, a GPO will be created and linked with the targets specified. This error is shown, when the linking fails.

1106: Group Policy Object (GPO) unlinking failed

When an already defined configuration is suspended, respective GPO will be unlinked from the targets. This error is shown, when the unlinking fails.

1107: WMI query failed

Desktop Central fetches the computer details through WMI. The WMI query may fail in the following cases:

1. Authentication failure

2. When the machine is shutdown
3. When the RPC server is not running.

1108: Active Directory error occurred

Pertains to the Active Directory related error. Please create a support file by clicking the **Support File** link available under the **Support** tab and send it to support@desktopcentral.com. Our support team will be able to assist you on this.

1109: Unable to Extract Information from the given Msi Package

The possible reason for this error could be that the MSI package is corrupted.

1110: Access is Denied

The Active Directory credentials are taken while you define the scope of management. This credential is stored in Desktop Central, which will be used for deploying configurations. When this credential becomes invalid or if it does not have necessary privileges, this error is shown.

One possible reason is that the credential is modified outside the Desktop Central.

1111: File Copy Failed

This error message is shown, when the user do not have necessary privileges to copy a file. Check whether the credentials supplied while defining the Scope of Management has necessary privileges.

1112: Folder Copy Failed

This error message is shown, when the user do not have necessary privileges to copy a folder. Check whether the credentials supplied while defining the Scope of Management has necessary privileges.

1113: The Given User Account is not a valid Domain Administrator

When the user account provided in the Scope of Management does not belong to a Domain Administrator group.

1114: The Given Password is wrong

The password provided in the Scope of Management is not valid.

1115: Active Directory/Domain Controller not Found

This error message is shown when no Active Directory/Domain Controller is found in your network. Desktop Central requires either of the two to perform the configurations.

1222: The network is not present or not started

This error message is shown when Desktop Central is unable to discover any domain. To fix this, start the Workstation service in the machine where Desktop Central is installed.

FAQs

1. What are the system requirements for Desktop Central?

Hardware Requirements for Desktop Central Server

No. of Computers Managed	Processor	RAM	Hard Disk Space
Upto 250 Computers	Single processor Intel P4 ~1.5 GHz	1 GB	2 GB*
251 to 500 Computers	Single processor (Intel P4 or Xeon 2.0 Ghz (Dual Core), 800+ Mhz FSB, 4 MB cache)	2 GB	2 GB*
501 to 1000 Computers	Single processor (Intel Xeon ~2.4 Ghz Dual Core, 800+ Mhz FSB, 4MB cache)	4 GB	3 GB*
1001 to 3000 Computers	Dual processor (Intel Xeon ~2.0 Ghz Dual Core, 1000 Mhz FSB,4 MB cache)	4 GB	5 GB*
3001 to 5000 Computers	Dual Processor (Intel Xeon processors Quad-Core at 2 ~ 3 GHz, 1000+ MHz FSB, 4 MB Cache)	6+ GB @ 667 Mhz. ECC	20 GB (HDD speed @ 7200 ~ 10,000 rpm)

No. of Computers Managed	Processor	RAM	Hard Disk Space
5001 to 10000 Computers	Quad Processor (Intel Xeon processors Quad-Core at 2 ~ 3 GHz, 1000+ MHz FSB, 4 MB Cache)	8+ GB @ 667 Mhz. ECC	50 GB (HDD speed @ 7200 ~ 10,000 rpm)

Environment - Active Directory based Windows 2000/2003 domain setup.

Supported platforms - Windows 2000 Professional, Windows XP Professional, Windows Vista, Windows 7, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server, Virtual Servers (VM Ware)

Supported Browsers - IE 5.5 and above, Netscape 7.0 and above, Mozilla 1.5 and above. You must install and enable Java plugin to use the software.

2. What operating systems are supported by Desktop Central?

Desktop Central supports the following operating systems:

- Windows 2000 Professional
- Windows XP Professional
- Windows Vista
- Windows 7
- Windows 2000 Server
- Windows 2003 Server
- Windows 2008 Server
- Virtual Servers (VM Ware)

3. What is the difference between Free and Professional Editions?

While the free edition can be used to manage up to 25 desktops free of cost, the professional edition can be used to manage the number of desktops for which it is licensed for. The free edition can be upgraded to professional edition at any point of time by obtaining a valid license from ManageEngine.

4. Do I have to write scripts for using Desktop Central?

No, you do not have to write scripts for using any of the pre-defined configurations provided by Desktop Central. Just select the configuration, specify the required inputs, and deploy.

5. What is Scope of Management?

Scope of Management is used to define what are the computers to be managed using this software. When an Administrator use this software first time, he/she can use it with small set of computers then can slowly add more computers under management.

6. Do I need to define configurations separately or can I group them and define?

Configurations that are intended for the same set of targets can be grouped and defined as collections. However, when the targets differ, you have to define them separately.

7. When are the configurations applied?

1. All user configurations, except Custom Script configuration, are applied during user logon.
2. All computer configurations, except Custom Script configuration, are applied during system startup.
3. Custom Script configuration can be applied during user logon/logoff or system startup/shutdown.
4. Both user and computer configurations are applied every 90 minutes through Windows Group Policies.

8. How to access Desktop Central client or console from the remote?

To access the Desktop Central client from remote, open a supported browser and type http://<host name>:<port number> in the address bar,

where <host name> refers to the name / IP Address of the machine running Desktop Central,

<port number> refers to the port at which the product is started, the default being 8020.

9. What is "Define Target"?

Define Target is the process of identifying the users or computers for which the configuration have to be applied. The targets can be all users/computers belonging to a Site, Domain, OUs, Groups, or can be a specific user/computer. You also have an option to exclude some desktops based on the machine type, OS type, etc.

10. My free trial expired before I was through evaluating Desktop Central. Can I receive an extension?

Customer satisfaction is our prime motive. During the trial period of 30 days, unlimited number of desktops can be managed by Desktop Central. After the trial period the software automatically switches to the free edition where only 25 desktops can be managed.

If you feel you would like to test the software for more number of desktops, but your trial period has expired, Kindly contact us so that we can arrange for a temporary license for few more days as per your requirement. You may note that the transition is smooth with no data loss and the configurations are not lost at any point of time. We want to make sure you are completely satisfied that the software is satisfying your need and solving your problem before buying it.

11. Why is Desktop Central configuration done through a Web interface?

Desktop administrators are always on the move. Desktop Central, with its web-based interface, facilitates the administrators to access the product from anywhere in the network not requiring them to be glued at one place for managing the desktops using the product.

12. How is Desktop Central licensed?

Desktop Central is licensed on annual subscription based on the number of Desktop it would manage. You can get the Pricing for the specific number of desktops from our online store.

Security Policies

Using Desktop Central, you can define the security restrictions for the users and computers in the domain. This section provides you a brief description about the various security restrictions that can be applied using the product. Follow the links to learn more about the supported security policies under each category:

- Active Desktop
- Desktop
- Control Panel
- Explorer
- Internet Explorer
- Network
- System
- Task Scheduler
- Windows Installer
- Start Menu and Taskbar
- Microsoft Management Console
- Computer

Security Policies - Active Desktop

Desktop Central supports configuring the following security policies in Active Desktop category:

Security Policy	Description
Remove Active Desktop item from Settings menu	This setting will remove the Active Desktop options from Settings on the Start Menu.
Remove all desktop items	Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, My Computer, and My Network Places.
Restrict adding any desktop items	Prevents users from adding Web content to their Active Desktop.
Restrict deleting any desktop items	Prevents users from deleting Web content from their Active Desktop. This setting removes the Delete button from the Web tab in Display in Control Panel.
Restrict editing any desktop items	Prevents users from changing the properties of Web content items on their Active Desktop. This setting disables the Properties button on the Web tab in Display in Control Panel.
Restrict closing any desktop items	Restrict closing any desktop items. This setting removes the check boxes from items on the Web tab in Display in Control Panel.
Do not allow HTML wallpaper	Permits only bitmap images for wallpaper. This setting limits the desktop background ("wallpaper") to bitmap (.bmp) files.
Restrict changing wallpaper	Specifies the desktop background ("wallpaper") displayed on all users' desktops. This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation.
Enable active desktop	Enables Active Desktop and prevents users from disabling it. This prevents users from trying to enable or disable Active Desktop while a policy controls it.
Disable active desktop	Disables Active Desktop and prevents users from enabling it. This prevents users from trying to enable or disable Active Desktop while a policy controls it.
Prohibit changes	Prevents the user from enabling or disabling Active Desktop or changing the Active Desktop configuration. This is a

Security Policy	Description
	comprehensive setting that locks down the configuration you establish by using other policies in this folder. This setting removes the Web tab from Display in Control Panel.
Allow only bitmapped wall paper	Permits only bitmap images for wallpaper. This setting limits the desktop background ("wallpaper") to bitmap (.bmp) files.
Enable filter in Find dialog box	Displays the filter bar above the results of an Active Directory search. The filter bar consists of buttons for applying additional filters to search results.
Hide AD folder	Hides the Active Directory folder in My Network Places. The Active Directory folder displays Active Directory objects in a browse window.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Desktop

Desktop Central supports configuring the following security policies in Desktop category:

Security Policy	Description
Hide and disable all items on the desktop	Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, My Computer, and My Network Places.
Remove my documents icon on the desktop	This setting removes the My Documents icon from the desktop, from Windows Explorer, from programs that use the Windows Explorer windows, and from the standard Open dialog box.
Hide my network places icon in desktop	Removes the My Network Places icon from the desktop.
Hide Internet explorer icon on desktop	Removes the Internet Explorer icon from the desktop and from the Quick Launch bar on the taskbar.
Prevent adding, dragging, dropping and closing the taskbar tool	Prevents users from manipulating desktop toolbars. If you enable this setting, users cannot add or remove toolbars from the desktop. Also, users cannot drag toolbars on to or off of docked toolbars.
Prohibit adjusting desktop toolbar	Prevents users from adjusting the length of desktop toolbars. Also, users cannot reposition items or toolbars on docked toolbars.
Don't save settings at exit	Prevents users from saving certain changes to the desktop.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Control Panel

Desktop Central supports configuring the following security policies in Control Panel category:

Security Policy	Description
Hide Accessibility Options Applet	Prevents access to the accessibility applet in control panel
Hide Add/Remove Hardware Applet	Prevents access to the Add/Remove Hardware Applet in control panel
Hide Add/Remove Programs Applet	Removes Add/Remove Programs Applet in control panel
Hide Client Services for Network Applet	Netware supporting client service applet will be removed from control panel
Hide Data Sources (ODBC) Applet	Removes open data base connection applet from control panel
Hide Date/Time Applet	Removes date/time applet in control panel
Hide Desktop Themes Applet	Removes desktop themes applet
Hide Display Applet	Removes display applet from control panel
Hide Games Controller Applet	Removes Games Controller Applet from control panel
Hide Internet Options Applet	Hide internet option applet
Hide Keyboard and Mouse Applet	Removes keyboard and mouse applet
Hide Network Connections Applet #1	Removes LAN connection 1
Hide Network Connections Applet #2	Removes LAN connection 2
Hide Mail Applet	Removes mail configuring applet from control panel
Hide Phone and Modem Options Applet (2000+)	Removes phone and modem options applet
Hide Power Options Applet	Removes power option from control panel

Security Policy	Description
Hide Regional Options Applet	Removes regional options applet
Hide Scanners and Cameras Applet	Removes scanners and cameras applet
Hide Sounds and Multimedia Applet	Removes sounds and multimedia applet
Hide System Applet	Removes system applet
Hide Users and Passwords Applet	Removes users and passwords applet from control panel
Disable control panel	Disables all Control Panel programs. This setting prevents Control.exe, the program file for Control Panel, from starting. As a result, users cannot start Control Panel or run any Control Panel items.
Remove add/remove programs	Prevents users from using Add or Remove Programs. This setting removes Add or Remove Programs from Control Panel and removes the Add or Remove Programs item from menus.
Hide change or remove programs page	Removes the Change or Remove Programs button from the Add or Remove Programs bar. As a result, users cannot view or change the attached page.
Hide add new programs page	Removes the Add New Programs button from the Add or Remove Programs bar. As a result, users cannot view or change the attached page.
Hide add/remove Windows components page	Removes the Add/Remove Windows Components button from the Add or Remove Programs bar. As a result, users cannot view or change the associated page.
Remove support information	Removes links to the Support Info dialog box from programs on the Change or Remove Programs page.
Hide appearance and themes page	Removes the Appearance and Themes tabs from Display in Control Panel.
Hide screen saver tab	Removes the Screen Saver tab from Display in Control Panel.
Hide settings tab	Removes the Settings tab from Display in Control Panel.
Password protect the screen saver	Determines whether screen savers used on the computer are password protected.
Prevent changing wall paper	Prevents users from adding or changing the background design of the desktop.

Security Policy	Description
Remove display in control panel	Disables Display in Control Panel.
Browse the network to find the printers	If you enable this setting or do not configure it, when users click "Add a network printer" but do not type the name of a particular printer, the Add Printer Wizard displays a list of all shared printers on the network and invites users to choose a printer from among them.
Prevent addition of printers	Prevents users from using familiar methods to add local and network printers.
Prevent deletion of printers	Prevents users from deleting local and network printers. If a user tries to delete a printer, such as by using the Delete option in Printers in Control Panel, a message appears explaining that a setting prevents the action.

---

he policy descriptions are taken from Microsoft Help Documentation

Security Policies - Explorer

Desktop Central supports configuring the following security policies in Explorer category:

Security Policy	Description
Remove folder options menu item from the tools menu	Removes the Folder Options item from all Windows Explorer menus and removes the Folder Options item from Control Panel. As a result, users cannot use the Folder Options dialog box.
Remove Shutdown from Start menu and task manager	Removes shutdown from the start menu and task manager dialog.
Remove File menu from Explorer	Removes the File menu from My Computer and Windows Explorer
Remove 'Map network drive' and 'Disconnect network drive'	Prevents users from using Windows Explorer or My Network Places to map or disconnect network drives.
Remove Context Menu in Shell folders	Removes context menus which appears while right clicking any folder in the explorer
Turn on classic shell	This setting allows you to remove the Active Desktop and Web view features. If you enable this setting, it will disable the Active Desktop and Web view.
Allow only approved Shell extensions	This setting is designed to ensure that shell extensions can operate on a per-user basis. If you enable this setting, Windows is directed to only run those shell extensions that have either been approved by an administrator or that will not impact other users of the machine.
Do not track Shell shortcuts during roaming	Determines whether Windows traces shortcuts back to their sources when it cannot find the target on the user's system.
Remove search button from Windows explorer	Removes the Search button from the Windows Explorer toolbar.
Hides the manage item on the Windows explorer context menu	Removes the Manage item from the Windows Explorer context menu. This context menu appears when you right-click Windows Explorer or My Computer.
Remove hardware tab	This setting removes the Hardware tab from Mouse, Keyboard, and Sounds and Audio Devices in Control Panel. It also removes the Hardware tab from the Properties dialog box for all local drives, including hard drives, floppy disk

Security Policy	Description
	drives, and CD-ROM drives.
Remove DFS tab	Removes the DFS tab from Windows Explorer.
Remove UI to change menu animation setting	Prevents users from selecting the option to animate the movement of windows, menus, and lists. If you enable this setting, the "Use transition effects for menus and tooltips" option in Display in Control Panel is disabled.
Remove UI to change keyboard navigation indicator setting	When this Display Properties option is selected, the underlining that indicates a keyboard shortcut character (hot key) does not appear on menus until you press ALT.
No 'computers near me' in My Network places	Removes the "Computers Near Me" option and the icons representing nearby computers from My Network Places. This setting also removes these icons from the Map Network Drive browser.
No 'Entire network' in My Network places	Removes the Entire Network option and the icons representing networked computers from My Network Places and from the browser associated with the Map Network Drive option.
Do not request alternate credentials	This setting suppresses the "Install Program As Other User" dialog box for local and network installations. This dialog box, which prompts the current user for the user name and password of an administrator, appears when users who are not administrators try to install programs locally on their computers.
Request credentials for network installations	This setting displays the "Install Program As Other User" dialog box even when a program is being installed from files on a network computer across a local area network connection.
Hide logoff menu item	This option removes Log Off item from the Start Menu. It also removes the Log Off button from the Windows Security dialog box.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Internet Explorer

Desktop Central supports configuring the following security policies in Internet Explorer category:

Security Policy	Description
Restrict using new menu option	Prevents users from opening a new browser window from the File menu.
Restrict using open menu option	Prevents users from opening a file or Web page from the File menu in Internet Explorer.
Restrict using Save As... menu option	Prevents users from saving Web pages from the browser File menu to their hard disk or to a network share.
Restrict on search customization	Makes the Customize button in the Search Assistant appear dimmed.
Restrict importing and exporting of favorites	Prevents users from exporting or importing favorite links by using the Import/Export Wizard.
Restrict using find files (F3) within browser	Disables using the F3 key to search in Internet Explorer and Windows Explorer.
Restrict using save as Web page complete format option	Prevents users from saving the complete contents that are displayed on or run from a Web page, including the graphics, scripts, linked files, and other elements. It does not prevent users from saving the text of a Web page.
Restrict closing of browser	Prevents users from closing Microsoft Internet Explorer.
Restrict full screen menu option	Prevents users from displaying the browser in full-screen (kiosk) mode, without the standard toolbar.
Restrict viewing source menu option	Prevents users from viewing the HTML source of Web pages by clicking the Source command on the View menu.
Hide favorites menu	Prevents users from adding, removing, or editing the list of Favorite links.
Restrict using Internet Options... menu option	Prevents users from opening the Internet Options dialog box from the Tools menu in Microsoft Internet Explorer.
Remove 'Tip of the Day' menu option	Prevents users from viewing or changing the Tip of the Day interface in Microsoft Internet Explorer.
Remove 'For Netscape Users' menu option	Prevents users from displaying tips for users who are switching from Netscape.

Security Policy	Description
Remove 'Tour' menu option	Remove the Tour menu option.
Remove 'Send Feedback' menu option	Prevents users from sending feedback to Microsoft by clicking the Send Feedback command on the Help menu.
Restrict using 'Open in New Window' menu option	Prevents using the shortcut menu to open a link in a new browser window.
Restrict using 'save this program to disk' option	Prevents users from saving a program or file that Microsoft Internet Explorer has downloaded to the hard disk.
Remove context (right-click) menus	Prevents the shortcut menu from appearing when users click the right mouse button while using the browser.
Hide the General Option Screen	Removes the General tab from the interface in the Internet Options dialog box.
Hide Security Option Screen	Removes the Security tab from the interface in the Internet Options dialog box.
Hide Content Option Screen	Removes the Content tab from the interface in the Internet Options dialog box.
Hide Connections Option Screen	Removes the Connections tab from the interface in the Internet Options dialog box.
Hide Programs Option Screen	Removes the Programs tab from the interface in the Internet Options dialog box.
Hide Advanced Option Screen	Removes the Advanced tab from the interface in the Internet Options dialog box.
Restrict changing home page settings	Prevents users from changing the home page of the browser. The home page is the first page that appears when users start the browser.
Restrict changing color settings	Prevents users from changing the default Web page colors.
Restrict changing link color settings	Prevents users from changing the colors of links on Web pages.
Restrict changing font settings	Prevents users from changing font settings.
Restrict changing language settings	Prevents users from changing language settings.
Restrict changing Cache settings	Prevents users from changing Cache settings.
Restrict changing history	Prevents users from changing history settings.

Security Policy	Description
settings	
Restrict changing accessibility setting	Prevents users from changing accessibility settings.
Restrict changing Content Advisor settings	Prevents users from changing the content advisor settings.
Restrict changing certificate settings	Prevents users from changing certificate settings in Internet Explorer. Certificates are used to verify the identity of software publishers.
Restrict changing Profile Assistant settings	Prevents users from changing Profile Assistant settings.
Restrict changing AutoComplete clear form	Prevents Microsoft Internet Explorer from automatically completing forms, such as filling in a name or a password that the user has entered previously on a Web page.
Restrict changing AutoComplete save password form	Disables automatic completion of user names and passwords in forms on Web pages, and prevents users from being prompted to save passwords.
Restrict using Internet Connection Wizard	Prevents users from running the Internet Connection Wizard.
Restrict changing connection settings	Prevents users from changing dial-up settings.
Restrict changing Automatic Configuration settings	Prevents users from changing automatic configuration settings. Automatic configuration is a process that administrators can use to update browser settings periodically.
Restrict changing proxy settings	Prevents users from changing proxy settings.
Restrict changing Messaging settings	Prevents users from changing the default programs for messaging tasks.
Restrict changing Calendar and Contact settings	Prevents users from changing the default programs for managing schedules and contacts.
Restrict Reset Web Settings feature	Prevents users from restoring default settings for home and search pages.
Restrict changing Check if Default Browser setting	Prevents Microsoft Internet Explorer from checking to see whether it is the default browser.
Restrict changing any Advanced settings	Prevents users from changing settings on the Advanced tab in the Internet Options dialog box.

Security Policy	Description
Restrict changing Automatic Install of IE components	Prevents Internet Explorer from automatically installing components.
Restrict changing automatic check for software updates	Prevents Internet Explorer from checking whether a new version of the browser is available.
Restrict changing showing the splash screen	Prevents the Internet Explorer splash screen from appearing when users start the browser.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Network

Desktop Central supports configuring the following security policies in Network category:

Security Policy	Description
Hide 'Entire Network' from Network Neighborhood	Removes all computers outside of the user's workgroup or local domain from lists of network resources in Windows Explorer and My Network Places.
AlphaNumeric password	Windows by default will accept anything as a password, including nothing. This setting controls whether Windows will require a alphanumeric password, i.e. a password made from a combination of alpha (A, B, C...) and numeric (1, 2 ,3 ...) characters.
Enable access to properties of RAS connections available to all users	Determines whether a user can view and change the properties of remote access connections that are available to all users of the computer.
Ability to delete all user remote access connection	Determines whether users can delete all user remote access connections.
Ability to enable/Disable LAN connections	Determines whether users can enable/disable LAN connections.
Ability to rename LAN	Determines whether users can rename LAN or all user remote access connections.
Prohibit access to properties of LAN	Determines whether users can change the properties of a LAN connection.
Prohibit access to properties of components of LAN	Determines whether Administrators and Network Configuration Operators can change the properties of components used by a LAN connection.
Prohibit access to the advanced settings item on the advanced menu	Determines whether the Advanced Settings item on the Advanced menu in Network Connections is enabled for administrators.
Prohibit access to the dial-up preferences item on the advanced menu	Determines whether the Dial-up Preferences item on the Advanced menu in Network Connections folder is enabled.
Allow configuration of connection sharing (User)	Determines whether users can use the New Connection Wizard, which creates new network connections.
Prohibit adding and	Determines whether administrators can add and remove

Security Policy	Description
removing components for a LAN or RA connection	network components for a LAN or remote access connection. This setting has no effect on non-administrators. If you enable this setting the Install and Uninstall buttons for components of connections are disabled, and administrators are not permitted to access network components in the Windows Components Wizard.
Prohibit TCP/IP advanced configuration	Determines whether users can configure advanced TCP/IP settings. If you enable this setting, the Advanced button on the Internet Protocol Properties dialog box is disabled for all users (including administrators).
Prohibit viewing of status for an active connection	Determines whether users can view the status for an active connection. The connection status taskbar icon and Status dialog box are not available to users (including administrators).
Remove 'make available offline'	Prevents users from making network files and folders available offline. This setting removes the "Make Available Offline" option from the File menu and from all context menus in Windows Explorer.
Sync offline files before logging off	Determines whether offline files are fully synchronized when users log off.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - System

Desktop Central supports configuring the following security policies in System category:

Security Policy	Description
Restrict using registry editing tools	Disables the Windows registry editors, Regedit.exe
Remove task manager	If this setting is enabled and users try to start Task Manager, a message appears explaining that a policy prevents the action.
Restrict using Lock Workstation	Prevents users from locking their workstation
Restrict Changing Password	Prevents users from changing the password.
Restrict using Passwords applet in Control Panel	Prevents users from changing the account password of local users through the password applet in control panel.
Restrict using Change Passwords page	Prevents users from accessing change password
Hide Background page	Prevents users using background page
Hide Remote Administration page	Removes remote administration page
Hide User Profiles page	Removes user profiles pages
Hide Device Manager page	Removes device manager page
Hide Hardware Profiles page	Prevents hardware profile page form being accessed
Don't display the getting started welcome screen at logon	Suppresses the welcome screen. This setting hides the welcome screen that is displayed on Windows 2000 Professional and Windows XP Professional each time the user logs on.
Download missing COM components	Directs the system to search Active Directory for missing Component Object Model components that a program requires.
Prevent access to registry accessing tools	Disables the Windows registry editors, Regedit.exe and Regedit.exe.
Run legacy logon scripts hidden	Windows 2000 displays the instructions in logon scripts written for Windows NT 4.0 and earlier in a command window as they run, although it does not display logon scripts written for Windows 2000. If you enable this setting,

Security Policy	Description
	Windows 2000 does not display logon scripts written for Windows NT 4.0 and earlier.
Run logoff scripts visible	If the setting is enabled, the system displays each instruction in the logoff script as it runs. The instructions appear in a command window.
Run logon scripts synchronously	If the setting is enabled, Windows Explorer does not start until the logon scripts have finished running. This setting ensures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.
Run logon scripts visible	If the setting is enabled, the system displays each instruction in the logon script as it runs. The instructions appear in a command window.
Do not process the legacy run list	If the setting is enabled, the system ignores the run list for Windows NT 4.0, Windows 2000, and Windows XP.
Do not process the runonce list	You can create a customized list of additional programs and documents that are started automatically the next time the system starts (but not thereafter). These programs are added to the standard list of programs and services that the system starts. If you enable this setting, the system ignores the run-once list.
Create a new GPO links disabled by default	This setting creates all new Group Policy object links in the disabled state by default. After you configure and test the new object links, either by using Active Directory Users and Computers or Active Directory Sites and Services, you can enable the object links for use on the system.
Enforce show policies only	Prevents administrators from viewing or using Group Policy preferences. A Group Policy administration (.adm) file can contain both true settings and preferences. True settings, which are fully supported by Group Policy, must use registry entries in the Software/Policies or Software/Microsoft/Windows/CurrentVersion/Policies registry subkeys. Preferences, which are not fully supported, use registry entries in other subkeys.
Turn off automatic update of ADM files	Prevents the system from updating the Administrative Templates source files automatically when you open Group Policy.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Task Scheduler

Desktop Central supports configuring the following security policies in Task Scheduler category:

Security Policy	Description
Hide property pages	This setting removes the Properties item from the File menu in Scheduled Tasks and from the context menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in Detail view and in the task preview.
Prevent task run or end	Prevents users from starting and stopping tasks manually.
Prohibit drag and drop	Prevents users from adding or removing tasks by moving or copying programs in the Scheduled Tasks folder.
Prohibit new task creation	Prevents users from creating new tasks
Prohibit task deletion	Prevents user from deleting users from the scheduled tasks folder
Remove advanced menu	Prevents users from viewing or changing the properties of newly created tasks.
Prohibit browse	This setting removes the Browse button from the Schedule Task Wizard and from the Task tab of the properties dialog box for a task. Also, users cannot edit the "Run" box or the "Start in" box that determine the program and path for a task.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Windows Installer

Desktop Central supports configuring the following security policies in Windows Installer category:

Security Policy	Description
Always install with elevated privileges	This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.
Prohibit rollback	This setting prevents Windows Installer from recording the original state of the system and sequence of changes it makes during installation. It also prevents Windows Installer from retaining files it intends to delete later. As a result, Windows Installer cannot restore the computer to its original state if the installation does not complete.
Disable media source for any install	Prevents users from installing programs from removable media.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Start Menu and Taskbar

Desktop Central supports configuring the following security policies in Start Menu and Taskbar category:

Security Policy	Description
Remove user's folder from the start menu	Hides all folders on the user-specific (top) section of the Start menu. Other items appear, but folders are hidden. This setting is designed for use with redirected folders. Redirected folders appear on the main (bottom) section of the Start menu.
Remove links and access to Windows update	Prevents users from connecting to the Windows Update Web site.
Remove common program groups from start menu	Removes items in the All Users profile from the Programs menu on the Start menu.
Prohibit user from changing My Documents path	Prevents users from changing the path to the My Documents folder.
Remove My Documents from start menu	Removes the Documents menu from the Start menu.
Remove programs on settings menu	Prevents Control Panel, Printers, and Network Connections from running.
Remove network connections from start menu	Prevents users from running Network Connections.
Remove favorites from start menu	Prevents users from adding the Favorites menu to the Start menu or classic Start menu.
Remove search from start menu	Removes the Search item from the Start menu, and disables some Windows Explorer search elements. This setting removes the Search item from the Start menu and from the context menu that appears when you right-click the Start menu. Also, the system does not respond when users press the Application key (the key with the Windows logo)+ F.
Remove help menu from start menu	Removes the Help command from the Start menu.
Remove run from start	Allows you to remove the Run command from the Start

Security Policy	Description
menu	menu, Internet Explorer, and Task Manager.
Add logoff to the start menu	Adds the "Log Off <username>" item to the Start menu and prevents users from removing it.
Remove logoff on the start menu	Removes the "Log Off <username>" item from the Start menu and prevents users from restoring it.
Remove and prevent access to the shutdown command	Prevents users from shutting down or restarting Windows. This setting removes the Shut Down option from the Start menu and disables the Shut Down button on the Windows Security dialog box, which appears when you press CTRL+ALT+DEL.
Remove drag-and-drop context menu on the start menu	Prevents users from using the drag-and-drop method to reorder or remove items on the Start menu. Also, it removes context menus from the Start menu.
Prevent changes to taskbar and start menu settings	Removes the Taskbar and Start Menu item from Settings on the Start menu. This setting also prevents the user from opening the Taskbar Properties dialog box.
Remove context menu for the taskbar	Hides the menus that appear when you right-click the taskbar and items on the taskbar, such as the Start button, the clock, and the taskbar buttons.
Do not keep the history of recently opened documents	Prevents the operating system and installed programs from creating and displaying shortcuts to recently opened documents.
Clear history of recently opened documents history on exit	Clear history of recently opened documents on exit.
Turn off personalized menus	Disables personalized menus. Windows 2000 personalizes long menus by moving recently used items to the top of the menu and hiding items that have not been used recently.
Turn off user tracking	Disables user tracking. This setting prevents the system from tracking the programs users run, the paths they navigate, and the documents they open.
Add 'run in separate memory space' check box to run dialog box	Lets users run a 16-bit program in a dedicated (not shared) Virtual DOS Machine (VDM) process.
Do not use the search based method when resolving shell shortcuts	Prevents the system from conducting a comprehensive search of the target drive to resolve a shortcut.

Security Policy	Description
Do not use the tracking based method when resolving shell shortcuts	Prevents the system from using NTFS tracking features to resolve a shortcut.
Gray unavailable Windows installer programs start menu shortcuts	Displays Start menu shortcuts to partially installed programs in gray text. This setting makes it easier for users to distinguish between programs that are fully installed and those that are only partially installed.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Microsoft Management Console

Desktop Central supports configuring the following security policies in Microsoft Management Console category:

Security Policy	Description
Restrict user from entering author mode	Users cannot create console files or add or remove snap-ins. Also, because they cannot open author-mode console files, they cannot use the tools that the files contain.
Restrict users to the explicitly permitted list of snap-ins	All snap-ins are prohibited, except those that you explicitly permit. Use this setting if you plan to prohibit use of most snap-ins. To explicitly permit a snap-in, open the Restricted/Permitted snap-ins setting folder and enable the settings representing the snap-in you want to permit.
Restrict/permit Component services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Computer management snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Device manager snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Disk management snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Disk de-fragmentation snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

Security Policy	Description
Restrict/permit Event viewer snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Fax services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Indexing services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Internet Information Services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Local users and groups snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Performance logs and alerts snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Shared folders snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

Security Policy	Description
Restrict/permit System information snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Telephony snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit WMI control snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit System properties snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Group policy snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Group policy tab for active directory tool snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Administrative templates (computer) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Administrative templates (users) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Folder redirection snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

Security Policy	Description
Restrict/permit Internet explorer maintenance snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Remote installation services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Scripts (logon/logoff) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Scripts(startup/shutdown) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Security settings snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Software installation (computer) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Software installation (user) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Computer

Desktop Central supports configuring the following security policies in Computer category:

Security Policy	Description
Disable ctrl+alt+del requirement for logon	Determines whether pressing CTRL+ALT+DEL is required before a user can log on.
Restrict CD-ROM access to locally logged-on user only	Determines whether a CD-ROM is accessible to both local and remote users simultaneously.
Restrict Floppy access to locally logged-on user only	Determines whether removable floppy media is accessible to both local and remote users simultaneously.
Prevent users from installing printer drivers	It prevents users from installing printer drivers on the local machine.
Prevent user from changing file type association	Disables the buttons on the File Types tab. As a result, users can view file type associations, but they cannot add, delete, or change them.

The policy descriptions are taken from Microsoft Help Documentation

Windows System Tools

Check Disk Tool

The Check Disk tool creates a status report of the disk based on its file system. The errors in the disk is also displayed. It can also be used to correct the disk errors.

Desktop Central supports the following options to run the check disk tool:

- *Verbose*: Displays the name of each file in every directory as the disk is checked.
- *Quick Check*: This option is available only for the NTFS File system. Selecting this option will perform the check disk operation quickly by skipping the checking of cycles within the folder structure and by performing a less vigorous check of index entries.

See Also: Windows System Tools, Creating and Scheduling Tasks, Viewing and Modifying the Tasks, Viewing Task History, Disk Defragmenter, Disk Cleanup

Disk Cleanup Tool

The Disk Cleanup utility helps to cleanup the unwanted filed in the disk to increase the free space.

Desktop Central cleans the windows system for the following:

- *Remove Active Setup Temp Folders*
- *Compress old files*
- *Remove content indexer*
- *Remove downloaded Program Files*
- *Remove internet cache files*
- *Remove memory dump files*
- *Remove Office setup files*
- *Remove offline files*
- *Remove web pages*
- *Remove old check disk files*
- *Empty recycle bin*
- *Remove remote desktop cache files*
- *Remove setup log files*
- *Remove old system restore positions.*
- *Remove Temporary files*
- *Remove temporary offline files*
- *Remove uninstall backup images*
- *Remove webclient and web publisher cache files*

See Also: Windows System Tools, Creating and Scheduling Tasks, Viewing and Modifying the Tasks, Viewing Task History, Disk Defragmenter, Check Disk

Disk Defragmenter Tool

Adapted from Windows Help Documentation

Volumes become fragmented as users create and delete files and folders, install new software, or download files from the Internet. Computers typically save files in the first contiguous free space that is large enough for the file. If a large enough free space is not available, the computer saves as much of the file as possible in the largest available space and then saves the remaining data in the next available free space, and so on.

After a large portion of a volume has been used for file and folder storage, most of the new files are saved in pieces across the volume. When you delete files, the empty spaces left behind fill in randomly as you store new ones.

The more fragmented the volume is, the slower the computer's file input/output performance will be.

Desktop Central provides option to run the defragmenter tool on multiple machines simultaneously. It supports the following options:

- *Verbose*: Displays the complete analysis and defragmentation reports
- *Analyze*: Analyzes the volume and displays a summary of the analysis report.
- *Force Defragmentation*: Forces defragmentation of the drive regardless of whether it needs to be defragmented.

See Also: Windows System Tools, Creating and Scheduling Tasks, Viewing and Modifying the Tasks, Viewing Task History, Check Disk, Disk Cleanup

Data Back up and Restore

Desktop Central stores information like configuration details, status of deployed configurations, and details about reports, like User Logon reports and Active Directory reports, in a database. Creating a backup of this database and certain important files like configuration files is necessary to prevent loss of data.

You can back up data automatically, by scheduling a back up using Desktop Central, or taking a back up manually. You can also restore this data when required. For example, assume that your hard disk crashes and you have to re-install Desktop Central. You can use the last back up you took to restore all the required information. Note that this is possible only if the backup file is stored in a computer other than yours.

Scheduling Data Backup

You can use Desktop Central to take a back up of the database regularly. For example, if you want to take a back up of the database every Friday at 5 p.m., you can schedule the same using Desktop Central.

To schedule back up of data, follow the steps given below:

1. Select the **Admin** tab
2. In the **Tools** section, click **Database Backup**
3. Specify the time at which you want the back up to be taken, in hour:minute:second (hh:mm:ss) format

	The time should be specified in the 24-hour format. For example, if you want the database back up to be taken at 6 p.m., the time should be specified as 18:00:00.

4. Select the number of backup files that you want Desktop Central to save

	Using this option you can select how many database backup files should be saved. The older backup files will be deleted. For example, if you want only 7 backup files saved, select 7. This will ensure that at all times only 7 backup files are saved.

5. Specify the location where you want the backup files to be stored
6. Check the **Notify when the database backup fails** checkbox
7. Specify the email address (es) to which you want an e-mail message sent, if the database back up failslease note that you should have configured your mail server settings to get notified.

Ensure that you have configured your mail server settings to receive notifications.

6. Click **Save Changes**

You have scheduled an automatic data backup to take place automatically at a specified time.

Manual Data Backup and Restore

You can manually back up and restore the database. You can do this using the Backup-Restore Utility GUI.

Opening the Backup-Restore Utility Graphical User Interface (GUI)

To open the Backup-Restore Utility GUI, follow the steps given below:

1. Right-click **start>Explore>Local Disk (C:)>Program Files>DesktopCentral_Server>bin**
2. Double-click backuprestore.bat

You've opened the Backup-Restore Utility GUI.

Creating a backup file

1. On the Backup-Restore Utility GUI, click the **Backup** tab
2. Select the location where you want to save the backup file

If you're using a network share, the directory should have write permission for everyone in the network.

3. Click **Backup**

A backup file is created and saved in the specified location. The file will be named using the buildnumber-date-time.zip format. For example, 70120-Oct-25-2010-13-26.zip where 70120 is the build number, Oct 25th 2010 is the date and 13:26 is the time.

Restoring a backup file

Ensure that you have shut down the Desktop Central server before restoring a backup file.

1. On the Backup-Restore Utility GUI, click the **Restore** tab

2. Browse and select the required backup file.
3. Click **Restore**

The build number of the Desktop Central server should match the build number of the backup file you are restoring.

This will restore the specified data to Desktop Central server.

If remote database is configured with the Desktop Central server, ensure that it is running on a remote machine. After restoration, the changes made after the backup date will not be available.

Dynamic Variables

Dynamic Variables are those that are replaced dynamically by Desktop Central while applying the configurations. As the name implies, the value of these variables are not the same for all the users/computers.

For example, to redirect the shortcuts of the start menu that are common for all the users to the system drive, you can use the dynamic variable **$SystemDrive**. This will be replaced by the corresponding system drive of that computer (like C, D, etc.) while deploying the configuration.

The table below lists the dynamic variable supported by Desktop Central:

Dynamic Variable	Description	Example Value of the Variable
$ComSpec	Specifies the path to the command interpretor	C:\WINNT\system32\cmd.exe
$HomePath	Refers to the home directory as defined in UMD/AD	\\JOHNSMITH\
$NtType	Role of NT/2000/XP computer	Server, Workstation
$OS	Short name of currently installed operating system	Windows_NT
$OSVersion	2000 & XP will report back as NT	Windows 2000
$OStype	2000 & XP will report back as NT	NT
$OsBuildNumber	Refers to the build number of the currently installed operating system	1381, 2195
$OsCsdVersion	Refers to the service pack of the currently installed operating system	Service Pack 4
$ProfileDirDU	Will be replaced by the full path of the "Default User" profile	C:\Documents and Settings\Default User
$ProfilesDir	Will be replaced by the full path of where user profiles are stored	C:\Documents and Settings

$ShellCache	Will be replaced by the path to current user's Temporary Internet Files shell folder	C:\Documents and Settings\JohnSmith\Local Settings\Temporary Internet Files
$ShellCookies	Will be replaced by the path to current user's Internet Cookies shell folder	C:\Documents and Settings\JohnSmith\Cookies
$ShellDesktop	Will be replaced by the path to current user's Desktop shell folder	C:\Documents and Settings\JohnSmith\Desktop
$ShellFavorites	Will be replaced by the path to current user's Favorites shell folder (also referred to as "IE Bookmarks").	C:\Documents and Settings\JohnSmith\Favorites
$ShellHistory	Will be replaced by the path to current user's History shell folder	C:\Documents and Settings\JohnSmith\Local Settings\History
$ShellMyPictures	Will be replaced by the path to current user's My Pictures shell folder	C:\Documents and Settings\JohnSmith\My Documents\My Pictures
$ShellNetHood	Will be replaced by the path to current user's Network Neighborhood shell folder	C:\Documents and Settings\JohnSmith\NetHood
$ShellPersonal	Will be replaced by the path to current user's Personal shell folder (also referred to as "My Documents")	C:\Documents and Settings\JohnSmith\My Documents
$ShellPrintHood	Will be replaced by the path to current user's Printer Neighborhood shell folder	C:\Documents and Settings\JohnSmith\PrintHood
$ShellPrograms	Will be replaced by the path to current user's Start Menu Programs shell folder	C:\Documents and Settings\JohnSmith\Start Menu\Programs
$ShellRecent	Will be replaced by the path to current user's Recent Documents shell folder	C:\Documents and Settings\JohnSmith\Recent
$ShellSendTo	Will be replaced by the path to current user's Send To shell folder	C:\Documents and Settings\JohnSmith\SendTo
$ShellStartMenu	Will be replaced by the path to current user's Start-Menu shell folder	C:\Documents and Settings\JohnSmith\Start Menu

$ShellStartup	Will be replaced by the path to current user's Start Menu Startup shell folder	C:\Documents and Settings\JohnSmith\Start Menu\Programs\Startup
$ShellTemplates	Will be replaced by the path to current user's Templates shell folder	C:\Documents and Settings\JohnSmith\Templates
$SystemDrive	Refers to the drive where OS files are located	C:
$SystemRoot	Will be replaced by the path to operating system folder	C:\WINNT
$TempDir	Will be replaced by the path to the temporary directory on the client	C:\Documents and Settings\JohnSmith\Local Settings\Temp
$WinDir	Will be replaced by the path to user's Windows folder (usually same as SystemRoot, exception would be a terminal server)	C:\WINNT

Limitations

1. When a site is chosen as the target for a user configuration, the status of the configuration will always be In Progress. This is because, it is not possible to get the exact user counts of individual sites.
2. When a user login to different computers in a domain, the status of the configurations defined for that user will reflect the status of the latest deployment.
3. When an already defined configuration is modified and re-deployed, the previous data will be overwritten and will not be shown in history reports.
4. Remote Shutdown Tool will not work for Windows 2000 computers.
5. Disk Defragmentation is not supported in Windows 2000 computers.

Known Issues

1. Printers shared in a Domain cannot be shared to computers in a Workgroup or vice-versa.
2. Redirecting folders between computers of different Domains or between a Workgroup and a Domain computer is not supported.
3. Software Installation will not work in the following cases:
    1. Package is in computer share of one Domain and you are trying to install it to a computer in another Domain.
    2. Package is in computer share of a Domain and you are trying to install it to a computer in a Workgroup or vice-versa.
    3. Package is in computer share of one Workgroup and you are trying to install it to a computer in another Workgroup.
4. In Custom Script configuration, Logoff and shutdown scripts cannot be executed.

Known Issues in deploying Configuration to Windows Vista Client Machines

1. When Security Policies are deployed to Windows Vista machines, the status will be shown as successful, but, the policies will not be applied.

Known Issues in Desktop **Sharing**

1. If the remote computer is shutdown using Remote Desktop Sharing, the viewer will not close by itself and has to be closed manually. It will display a blue screen showing a message "Meeting has stopped".
2. When connecting from Firefox/Flock browsers, Desktop Central Add-on (xpi) will be installed every time you access a remote computer using the Active X viewer. If you do not accept to install the xpi within 20 seconds, the remote service will be killed and you will not be able to access it. You have to close the viewer and have to connect again.

3. In Java viewer, Zoom In, Zoom Out, and Full Screen icons in the toolbar will not work.
4. When a remote connection is established, a message "You are now controlling the desktop" will appear. If you do not click OK within 20 seconds, the connection will close automatically. You have to close the viewer and have to connect again.

Glossary

This section provides the description or definitions of the terms used in Desktop Central.

Site

One or more well connected (highly reliable and fast) TCP/IP subnets. A site allows administrators to configure Active Directory access and replication topology quickly and easily to take advantage of the physical network. When users log on, Active Directory clients locate Active Directory servers in the same site as the user.

Domain

Domain is a group of computers that are part of a network and share a common directory database. A domain is administered as a unit with common rules and procedures. Each domain has a unique name.

Organizational Unit (OU)

An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain. An

organizational unit is the smallest scope to which a Group Policy object can be linked, or over which administrative authority can be delegated.

Group

A collection of users, computers, contacts, and other groups. Groups can be used as security or as e-mail distribution collections. Distribution groups are used only for e-mail. Security groups are used both to grant access to resources and as e-mail distribution lists.

User

The people using the workstations in the network are called users. Each user in the network has a unique user name and corresponding password for secured access.

Computer

The PCs in the network which are accessed by users are known as computer or workstation. Each computer has unique name.

IP Address

The expansion of IP Address is Internet Protocol Address. An unique IP Address is provided for each workstation, switches, printers, and other devices present in the network for identification and routing of information.

Group Policy Object (GPO)

A Group Policy Object (GPO) is a collection of settings that define what a system will look like and how it will behave for a defined group of users.

Client Side Extension (CSE)

Desktop Central installs an Windows-compliant agent or a Client Side Extension (CSE) in the machines that are being managed. This is used to get the status of the applied configurations from the targets.

Define Target

Define Target is the process of identifying the users or computers for which the configuration have to be applied. The targets can be all users/computers belonging to a Site, Domain, OUs, Groups, or can be a specific user/computer. You also have an option to exclude some desktops based on the machine type, OS type, etc.

Scope of Management

Scope of Management (SOM) is used to define the computers that have to be managed using this software. Initially the administrator can define a small set of computers for

testing the software and later extend it to the whole domain. This provides more flexibility in managing your desktops using this software.

Inactive Users

In a Windows Domain there may be cases where the user accounts have been created for some machines but they remain inactive for some reasons. For example, users like Guest, IUSER_WIN2KMASTER, IWAM_WIN2KMASTER, etc., will never login. These user accounts are referred to as Inactive Users. In order to get the accurate configuration status of the active users, it is recommended that the Admin User add the inactive user accounts in their domain so that these users (user accounts) may not be considered for calculating the status.

Collection

Configurations that are intended for the same set of targets can be grouped as a collection.

Applicable Patches

This is a subset of the patches released by Microsoft that affect your network systems / applications. This includes all the patches affecting your network irrespective of whether they are installed or not.

Missing Patches

This refers to the patches affecting your network that are not installed.

Latest Patches

This refers to the patches pertaining to the recently released Microsoft bulletins.

Missing Systems

This refers to the systems managed by Desktop Central that requires the patches to be installed.

Affected Systems

This refers to the systems managed by Desktop Central that are vulnerable. This includes all the systems that are affected irrespective of whether the patches have been installed or not.

Informational Patches

There maybe some vulnerabilities for which Desktop Central is not able to determine if the appropriate patch or work around has been applied. There could also be patches for which

manual intervention is required. These are categorized as Informational Items. Remediation of these issues usually involves a configuration change or work around rather than a patch.

Obsolete Patches

These are patches that are outdated and have another patch that is more recently released and has taken its place (Superseding Patch). If these patches are missing, you can safely ignore them and deploy the patches that supersede them.

Some definitions are adapted from Microsoft Help Documentation.