

# **Admin Guide**

## Table Of Contents

<b>INTRODUCTION.....</b>	<b>3</b>
<b>INSTALLATION &amp; SETUP .....</b>	<b>5</b>
System Requirements .....	6
Installing Desktop Central.....	8
Working with Desktop Central .....	10
Installing Service Pack.....	12
Licensing the Product .....	13
Understanding the Client UI.....	15
Setting Up Desktop Central .....	17
Configuring Desktop Central for Windows Vista / 2008.....	18
Defining Scope of Management .....	19
Adding Domain/Workgroup .....	20
Managing computers in LAN .....	23
Managing computers in WAN.....	25
Configuring Agent Settings .....	33
Configuring Mail Server .....	35
Configuring Help Desk Integration.....	36
Managing Custom Scripts.....	37
Configuring Server Settings.....	39
Creating Custom Groups .....	40
Personalizing the Client .....	42
User & Role Management .....	43
Setting Up Software Deployment.....	44
Configure Network Share for Software Repository.....	45
Managing Software Packages.....	46
Setting Up Patch Management.....	52
Configuring Proxy Server .....	53
Configuring Vulnerability DB Synchronization .....	54
Configuring Automated Patch Deployment .....	55
Configuring System Health Policy .....	57
Exclude Patches .....	58

Setting Up Asset Management .....	59
Scan Systems for Inventory .....	60
Manage Software Licenses .....	62
Create Software Groups.....	63
Manage Software Category.....	64
Configure Prohibited Software .....	65
Configure E-Mail Alerts .....	67
Schedule Inventory Scanning.....	68
Setting Up User Logon Reports.....	69
Setting Up Active Directory Reports .....	70
<b>APPENDIX.....</b>	<b>71</b>
Interpreting Error Messages .....	72
FAQs.....	75
Security Policies .....	78
Security Policies - Active Desktop .....	79
Security Policies - Desktop .....	81
Security Policies - Control Panel .....	82
Security Policies - Explorer.....	84
Security Policies - Internet Explorer.....	86
Security Policies - Network .....	89
Security Policies - System .....	91
Security Policies - Task Scheduler .....	93
Security Policies - Windows Installer.....	94
Security Policies - Start Menu and Taskbar.....	95
Security Policies - Microsoft Management Console .....	97
Security Policies - Computer .....	101
Windows System Tools .....	102
Check Disk Tool.....	103
Disk Cleanup Tool.....	104
Disk Defragmenter Tool.....	105
Data Backup and Restore.....	106
Data Restore.....	107
Dynamic Variables.....	108
Limitations.....	110
Glossary.....	112

# 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. It 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.

## 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](#)
- [Installing Desktop Central](#)
- [Working with Desktop Central](#)
- [Installing Service Pack](#)
- [Licensing the Product](#)
- [Understanding the Client UI](#)
- [Setting Up Desktop Central](#)

## System Requirements

- [Hardware Requirements for Desktop Central Server](#)
- [Hardware Requirements for Distribution Server](#)
- [Hardware Requirement for Desktop Central Agent](#)
- [Software 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 Server	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	2 GB*

No. of Computers Reporting to the Distribution Server	Processor	RAM	Hard Disk Space
		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 dynamically 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

#### Servers

- Windows 2000
- Windows 2003
- Windows 2008

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](#)
  - [Pre-Requisites for Installing Desktop Central Server](#)
  - [Ports Used by Desktop Central Server](#)
  - [Installing Desktop Central Server](#)
  - [Uninstalling Desktop Central Server](#)
- 

## 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
- 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
3. TCP Port 8443 - Used for Remote Desktop Sharing.

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](#)
- [Launching Desktop Central Client](#)
- [Steps to Perform after Initial Login](#)
- [Stopping 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	✓	✓	✓	✗
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](mailto: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

- [Tabbed Pane](#)
- [Quick Links](#)
- [Left Pane](#)
- [Content Pane](#)

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

## 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](#)
- [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

---

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

For running Desktop Central Service in Windows Vista or Windows 2008 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

When you install Desktop Central server in Windows Vista or Windows 2008 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 Scope of Management



### Defining 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



### 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 Controller Name	The name of the domain controller. If you have multiple domain controllers, provide the name of the domain controller that is nearest to the computer where Desktop Central Server is installed	Mandatory

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 / 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**.

## 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



### 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 WAN



### Managing computers in WAN

---

#### What is a Remote Office?

Most of the time your business will operate from a Head Office and branch offices that are geographically distributed. These branch offices that act as separate entities are termed as Remote Offices. As Network Managers you need to ensure the computers at your Head Office and Branch Offices are monitored alike. You will also need to manage the computers of roaming/mobile users who connect to your network via Internet. Some of the undeniable facts of managing computers that are spread across the WAN include:

- Bandwidth issues that degenerate the downloading speed, etc.
- Resultant costs associated with Bandwidth utilization.

The choice of action to manage these computers is once again scenario dependant. The following section will help you identify the solution that is ideal for you kind of infrastructure.

#### Identify the solution that suits your needs

The type of solution that you need to adopt depends primarily on the number of computers you are likely to manage at your branch/remote office. The options available include managing the Remote Office:

1. [Using a Distribution Server and WAN Agents](#): When the computers to be managed are greater in number.
2. [Directly using WAN Agents](#): When the number of computers is less than 10.

The Agent-Server Communication mode can also be changed later by [modifying the Remote Office details](#).

#### Managing Remote Office using Distribution Server and WAN Agents

Desktop Central's Distribution Server technology can help you plan and control bandwidth utilization and associated costs. The Distribution Server located at the remote location synchronizes the Configuration/Patch/Software repositories with the Desktop Central Server located at the Main Office at specific intervals. Now the WAN agents installed on the desktops at the remote location can download the patch/service pack/software from the Distribution Server locally within the Remote Office LAN. This mechanism clearly addresses the bandwidth related issues and also improves the efficiency and control-level that network managers/administrators can exercise on the remote machines.

## How to create Remote Office with Distribution Server?

Creating a Distribution Server at a remote office of your enterprise is quite simple. Follow the steps given below to accomplish this task:

1. Select Admin Tab.
2. Click Scope of Management link under Global Settings.
3. Select Remote Offices Tab.
4. Click Add Remote Office button. This opens the Add Remote Office page.
5. Specify Remote Office Name.

You will need to specify all the details under different sections:

- [Desktop Central Server Details](#)
- [Communication Details](#)
- [Distribution Server Details](#)
- [Distribution Server/WAN Agent to Desktop Central Communication](#)
- [Computers to be Managed](#)

### Desktop Central Server Details:

1. Specify the IP Address in case you have a secondary IP address for the DC Server.



**Note:** The HTTP and HTTPS ports represent the ones that have been designated for Desktop Central Server. The default ports for HTTP and HTTPS are 8020 and 8383 respectively. However these may vary based on what you have specified while installing Desktop Central Server.

### Communication Details:

Select the Communication Type as 'Through Distribution Server.'

### Distribution Server(DS) Details:

1. Specify the Domain NetBIOS Name
2. Specify the Computer Name on which DS is to be installed.
3. Specify the IP Address of the computer on which Distribution Server will be installed.



**Note:** It is recommended to have a dedicated computer as the distribution server with a static IP address. This will facilitate hassle-free communication of the Remote Agents with the Distribution Server.

4. Specify HTTP port for DS.
5. Specify HTTPS port for DS.



**Note:** The HTTP and HTTPS ports for communication between the WAN agents and the Distribution Server. The Distribution Server's default ports for HTTP and HTTPS are 8021 and 8384 respectively. However you can use different ports for the same.

- Specify the Replication Interval time.



**Note:** The Replication Interval Time is the interval at which you want the Distribution Server to synchronize with the Desktop Central Server. The default is two minutes. However you can customize the replication interval.

## Distribution Server/WAN Agent to Desktop Central Communication:

- Enable Secured Communications(HTTPS) checkbox to establish a secure communication set-up.
- Enable Proxy Configuration checkbox to specify the Proxy Host, Port, User Name and Password for that proxy.

### Computers to be Managed:

Specify the computer name/IP address of the remote computers you want to manage. Use comma to specify multiple computers. The computer names will be used to automate agent installation using the script. However computer names can given at a later stage also and hence it is not a mandatory field. After specifying all the above details, click Add to create the Distribution Server.

## How to deploy the Distribution Server at the Branch Office?

On successful creation of Distribution Server, the Desktop Central Application will display the SoM page. You will find the status as "Yet to Install" for the newly created Distribution Server. Follow the steps given below to proceed with the deployment process:

- Click on Download Agent icon of Remote Office tab.
- Save the Distribution Server zip file in the machine on which Distribution Server needs to be installed. You should login as an administrator in that computer to install the Distribution Server.
- Extract the contents of the zip file i.e. dssetup folder on the same machine.
- Open a command prompt (Start --> Run --> type cmd).
- Navigate to the working folder dssetup in the command prompt. Example: c:\Remote-Office\dssetup, where Remote-Office is folder in which the dssetup has been extracted.
- Run the command setup.bat and select the option as 1 to deploy the Distribution Server alone. Refer to the Remote Agent Installation section to install WAN agents also.

## How to deploy WAN Agent on the Branch Office Desktops?

WAN Agent can be installed during two stages:

- During Distribution Server Deployment.
- After Distribution Server Deployment.

To deploy WAN agent during Distribution Server deployment,

1. Navigate to the working folder dssetup in the command prompt. Example:  
c:\Remote-Office\dssetup, where Remote-Office is folder in which the dssetup has been extracted.
2. Edit the computers.txt and specify the computers where the WAN Agents have to be installed.
3. Run the command setup.bat and select the option as 2.
4. Specify the Administrator user name and password when prompted. This can be a domain administrator or a common user who has administrator privileges in all the computers where the WAN agent has to be installed. The user name should be prefixed with the domain or the workgroup name - eg. zohocorp\administrator
5. This will deploy both the Distribution Server and also WAN agents on the branch office computers specified in computers.txt.

To deploy WAN agent after Distribution Server deployment,

1. Navigate to the working folder dssetup in the command prompt. Example:  
c:\Remote-Office\dssetup, where Remote-Office is folder in which the dssetup has been extracted.
2. Edit the computers.txt and specify the computers where the WAN Agents have to be installed.
3. Run the command setup.bat and select the option as 3.
4. Specify the Administrator user name and password when prompted. This can be a domain administrator or a common user who has administrator privileges in all the computers where the WAN agent has to be installed. The user name should be prefixed with the domain or the workgroup name - eg. zohocorp\administrator
5. This will deploy the WAN agents on the branch office computers specified in computers.txt.

## **Manage Remote Office directly using WAN Agents**

When the number of computers is less than 10 and if there are no bandwidth related issues, you can opt to manage your branch office desktops using WAN Agents. The topics that will be covered in this section include:

- [Adding Details of Branch/Remote Offices](#)
- [Installing Agents in Branch/Remote Office Computers](#)

### **Adding Details of Branch/Remote Offices**

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 the Admin tab to invoke the Admin page.
2. Click the Scope of Management link available under Global Settings. This invokes the Scope of Management page.
3. The Computers tab is selected by default showing all the computers that have been added already.
4. Select the Remote offices tab. This will list the details of the remote offices that have been already added. The Remote Office Name as "Local Office" will be added by default, which pertains to the LAN where Desktop Central Server is installed.

5. Click Add Remote Office and specify the following details:
  1. Remote Office Name
  2. Specify the IP Address of the computer where Desktop Central Server is installed. 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.
  3. Select the Communication Type as Direct Communication.
  4. Specify the interval at which the agents from remote office computers should contact the Desktop Central Server for instructions. The default value is 2 minutes, which is configurable.
  5. Select the Enable Secured Communication (HTTPS) check box for secured communication between the Desktop Central Server and Agent.
  6. If the systems in the branch office connects to internet through a proxy server, select the Proxy Configuration option and specify the proxy server details of the remote office.
  7. Specify the computer name/IP address of the remote computers you want to manage. Use comma to specify multiple computers. The computer names will be used to automate agent installation using the script. However computer names can given at a later stage also and hence it is not a mandatory field.
  8. After specifying all the above details, click Add
  9. Click Add.

## Importing Details of Branch/Remote Offices

Instead of adding the details of the branch/remote offices as explained in the previous section, you can also simplify the process further using the CSV Import option. This method is especially useful when you are want to add multiple remote offices at a single instance. Follow the steps given below to add remote office(s) importing a CSV file.

1. Select the Admin tab to invoke the Admin page.
2. Click the Scope of Management link available under Global Settings. This invokes the Scope of Management page.
3. The Computers tab is selected by default showing all the computers that have been added already.
4. Select the Remote offices tab. This will list the details of the remote offices that have been already added. The Remote Office Name as "Local Office" will be added by default, which pertains to the LAN where Desktop Central Server is installed.
5. Click the Import Remote Offices link. This opens the Import Remote Offices dialog.
6. Click on the Browse button to select the CSV file that needs to be imported.
7. Click on Import.

Once the above procedure is complete, the remote offices that you have just imported will be listed under the Remote Offices tab.

## Some important CSV file specifications

1. The first line of the CSV file is the header specifying the column names.
2. 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 their Description

1. REMOTE\_OFFICE\_NAME - The Remote Office name
2. POLLING\_INTERVAL - Communication Interval / Replication Interval based on the Communication Type. The default value is 2 minutes
3. SERVER\_IP - The IP Address of the Desktop Central Server, which is accessible from the Remote Office Computers.
4. HAS\_DS - The values can be Yes or No. Yes means that the communication Type is through the Distribution Server. The default value is 'No' if newly added or the previous value in case of modification. If the value is yes, the following columns are mandatory:
  1. DS\_DOMAIN\_NAME - Domain Netbios Name of the Distribution Server
  2. DS\_NAME - Computer Name where Distribution Server will be installed
  3. DS\_IP - IP Address of the computer where Distribution Server will be installed
  4. DS\_PORT - HTTP Port through with the Distribution Server and WAN Agents communicate
  5. DS\_HTTPS\_PORT - HTTPS Port through with the Distribution Server and WAN Agents communicate
5. PROTOCOL - The mode of communication between Distribution Server, WAN Computers and Desktop Central Server. The default is HTTP
6. HAS\_PROXY - The values can be Yes or No. 'Yes' means the communication between the Distribution Server/WAN Computers to the Desktop Central Server happens through the Proxy Server. The default is 'No' if newly added or the previous value in case of modification. If the value is 'yes', the following columns are mandatory:
  1. PROXY\_SERVER - The name / IP Address of the Proxy Server
  2. PROXY\_PORT - The Proxy Port
  3. PROXY\_USER - The user name for accessing the Proxy Server
  4. PROXY\_PASSWORD - The password of the proxy user account.
7. COMPUTERS - The computer names in that remote office. If more than one computer is being 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 CSV file import method offers simplified options to edit Remote Office parameters. Let us say, you want to change the proxy server name for your remote offices. You don't have to manually edit the proxy details of each and every remote office. This can be done by creating a CSV file that contains only the remote office name and the parameter that needs to be updated; the proxy server name in this case for instance.

```

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

```

## Installing Agents in Branch/Remote Office Computers



**Note:** Desktop Central agents have to be manually downloaded and installed in Branch/Remote Office computers. To install agent in multiple computers in the same location, you can use the command line tool provided.

### Install Agent in a Single Computer

1. Download the Desktop Central agent from the SoM Page using the 'Download Agent ' Link. Please make sure you have downloaded the Agent with respective Remote Office name. 'Local Office' refers to the LAN where Desktop Central Server is installed.
2. After downloading the DC Agents, install it in the Branch Office computers manually.
3. Extract the zip to a directory.
4. Open a command prompt and change directory to <Extracted\_Dir>/directsetup
5. Execute the following command:

```

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

```

### Install Agent in Multiple Computers in the same location

1. Download the Desktop Central agent from the SoM Page 'Download Agent ' Link. Please make sure you have downloaded the Agent with respective Remote Office name. 'Local Office' refers to the LAN where Desktop Central Server is installed.
2. After downloading the DC Agents, please install it in the Branch Office computers manually.
3. Extract the zip to a directory.

4. Edit the computernames.txt file and add all the computer names to which the agent has to be installed. Each computer has to be specified in a separate line.
5. Open a command prompt and change directory to <Extracted\_Dir>/directsetup
6. Run the command setup.bat.
7. Specify the Administrator user name and password when prompted. This can be a domain administrator or a common user who has administrator privileges in all the computers where the WAN agent has to be installed. The user name should be prefixed with the domain or the workgroup name - eg. zohocorp\administrator
8. This will install the desktop central agents in all the computers specified in the computernames.txt file.
9. The logs.txt file located in <Extracted\_Dir>/directsetup will have the details on the errors encountered during installation, if any.

## Modifying Remote Office Details

In situations where you wish 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 for a Remote Office and you wish the communication now happen through the Distribution Server, you can modify the Remote Office to make this change by following the steps below:

1. Select **SoM --> Remote Offices** tab
2. Click the Modify icon from the Action column pertaining to the Remote Office that has to be changed.
3. Change the necessary parameters and click **Modify**.



**Note:** If you have changed the mode of communication from Direct to Distribution Server, you need to install and start the Distribution Server in the specified computer. Till then, the computers in that Remote Office will not get the configurations applied. However, you can still be able to deploy the configurations, patches, software, etc to those computer.

## 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. If it requires authentication, select the Requires Authentication check box and specify the user name and password.
5. 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.

## Managing Custom Scripts

---

- [Adding the Script Details](#)
  - [Modifying the Script Details](#)
  - [Removing the Script Details](#)
- 

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.

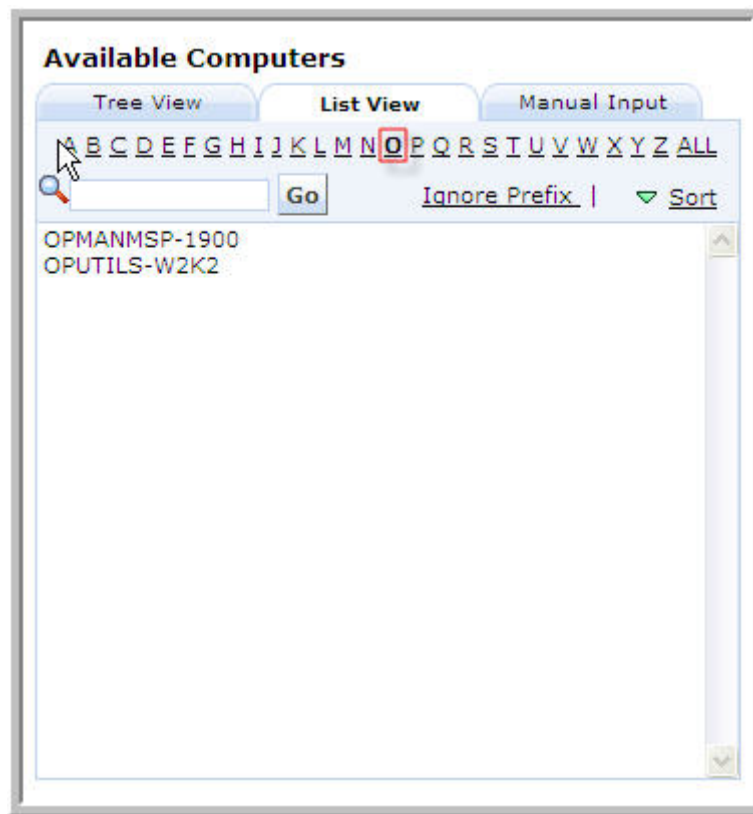
To create a custom group, follow the steps below:

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.

## 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.

## User & Role Management

---

- [Overview](#)
- [Role Management](#)

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

---

To deploy software using Desktop Central, the administrator has to first add the software packages by specifying the location and the installation switches. Only Desktop Central users with administrative privileges can add software packages. Separate packages have to be added for MSI and EXE based software applications. The packages thus added can then be used to deploy the software to the users and computers by defining a [Install Software Configuration](#). You can also specify the Network Share for Software Repository to store all the Software binaries (MSI / EXE).

The following section describes the steps involved in adding a software package in Desktop Central:

- [Configure Network Share for Software Repository](#)
- [Managing Software Packages](#)

## Configure Network Share for Software Repository

---

The Desktop Central application automatically prompts to configure Network Share path when proceeding with Software Deployment. However you can exit this screen using the *Skip* button. This section will guide you to configure Network Share for Software Repository.

1. Click on *Software Deployment* tab. This opens the Software Deployment workflow page.
2. Click on *Add MSI* (or) *Add EXE*. This opens the Network Share dialog.
3. Specify the Network Share in the *Edit Network Share* text field. You can also use the *Browse* button to select the path.
4. Select the Domain Name from the drop down list.
5. Click on the *Save & Continue* button.

All the software binaries (MSI / EXE) should be maintained in the specified Network Share. The Share should be accessible from all the client computers and should have 'Read and Execute' permission to the 'Everyone' group.

## Managing Software Packages



### Managing Software Packages

- [Adding MSI/EXE Packages](#)
- [Executing Scripts in Software installation](#)
- [Modifying MSI/EXE Packages](#)
- [Removing MSI/EXE 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
<b>Package</b>	
Package Name	Name of the Software Package
Select the path type	Select any of the following: <ul style="list-style-type: none"> <li>• Network Path: If the software has to be installed in computers in the same LAN, select this option</li> <li>• HTTP Path: If the software has to be installed in computers in branch offices over the VPN tunnel or internet, select this option</li> </ul>
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.

Parameter	Description
<b>Advanced Options</b> (optional)	
<b>Installer / Uninstaller Settings</b>	
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	<p>For applications that supports customizations prior to installation, you can customize the installation and specify it here.</p> <p>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.</p> <p>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, specify the location as Office2003\Custom.mst. Multiple mst files can be specified as semi-colon separated.</p> <p>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.</p>
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.
<b>Package Properties</b>	
Manufacturer	Name of the software vendor
Version	The software version
Language	The software language version
Package Description	Description of the software package

Parameter	Description
<b>Run Script before Installing Software</b>	
Script / Command Name	Specify the commands or scripts that has to be executed before installing the software. Refer to <a href="#">Executing Scripts in Software installation</a> for more details.
Arguments	Specify the arguments for the pre-installation 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.
<b>Run Script after Installing Software</b>	
Script / Command Name	Specify the commands or scripts that has to be executed after installing the software. Refer to <a href="#">Executing Scripts in Software installation</a> 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.
<b>Run Script before Uninstalling Software</b>	
Script / Command Name	Specify the commands or scripts that has to be executed before uninstalling the software. Refer to <a href="#">Executing Scripts in Software installation</a> 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.
<b>Run Script after Uninstalling Software</b>	
Script / Command Name	Specify the commands or scripts that has to be executed after uninstalling the software. Refer to <a href="#">Executing Scripts in Software installation</a> 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.

- Click **Add Package**. The package gets added to the table below.
- 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
<b>Package</b>	
Software Name	Name of the Software Application. Click on the <i>Select from Pre-Defined Application</i> link. This opens the <i>Select Application</i> 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: <ul style="list-style-type: none"> <li>• <i>Network Path</i>: If the software has to be installed in computers in the same LAN, select this option</li> <li>• <i>HTTP Path</i>: If the software has to be installed in computers in branch offices over the VPN tunnel or internet, select this option</li> </ul>
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: <ol style="list-style-type: none"> <li>1. msixec.exe \Skype\skype.msi /qn</li> <li>2. googlesetup.exe /S</li> </ol>
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

Parameter	Description
<b>Advanced Options</b> (optional)	
<b>Installer / Uninstaller Settings</b>	
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.
<b>Package Properties</b>	
Manufacturer	Name of the software vendor
Version	The software version
Language	The software language version
Package Description	Description of the software package
<b>Run Script before Installing the Software</b>	
Script / Command Name	Specify the commands or scripts that has to be executed before installing the software. Refer to <a href="#">Executing Scripts in Software installation</a> for more details.
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.
<b>Run Script after Installing the Software</b>	
Script / Command Name	Specify the commands or scripts that has to be executed after installing the software. Refer to <a href="#">Executing Scripts in Software installation</a> 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.
<b>Run Script before Uninstalling the Software</b>	
Script / Command Name	Specify the commands or scripts that has to be executed before uninstalling the software. Refer to <a href="#">Executing Scripts in Software installation</a> 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.
<b>Run Script after Uninstalling the Software</b>	
Script / Command Name	Specify the commands or scripts that has to be executed after uninstalling the software. Refer to <a href="#">Executing Scripts in Software installation</a> 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.

- Click **Add Package**. The package gets added to the table below.
- 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:


- Prior to installing the software
- After installing the software
- Prior to uninstalling the software
- 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.

## 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](#)
- [Excluding Patches for Scan](#)

## Configuring Proxy Server



### 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](#)
- [HTTP Proxy Configuration](#)
- [FTP Proxy Configuration](#)

#### 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



### 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



## 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 [excluded](#) 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.

## Exclude Patches



### Exclude Patches

---

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

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

#### To Exclude Applications:

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

#### To Exclude Specific Patches:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click Exclude Patch link available under Patch Settings
3. Click on Exclude 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 Excluded Patches list.
  3. Click Update. The patches listed under Excluded 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



### 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. Right-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 Scan 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](mailto:desktopcentral-support@manageengine.com)
5. If you get an error as DCOM not enabled, [enable DCOM](#) and try scanning again.

## Manage Software Licenses



### Manage Software Licenses

---

Desktop Central allows you to add the details of the licenses purchased along with their expiry date. This data will be used to arrive at the License Compliance Reports and Software Metering.

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 Software 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/Edit Software License link.
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 comments, if required.
9. Click Update License.

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.

## 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



### 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



### Configure Prohibited Software

---

- [Adding Prohibited Software](#)
  - [Removing Prohibited Software](#)
  - [Configuring Auto-Uninstalling Policy](#)
  - [Exclude Custom Groups from Auto-Uninstallation of 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 Custom Groups from Software Uninstallation

In certain occasions, you will need to allow the usage of prohibited software by certain custom groups. 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 and add it in 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 the groups under **Custom Groups** and move it to the **Excluded Groups** list.
4. Click on **Save** to save changes.

## Configure E-Mail Alerts



### 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



### 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.

## 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

---

1. 1001: Storage Error Occurred
  2. 1002: Unknown Error
  3. 1003: DB Error
  4. 1004: DB Error
  5. 1010: Invalid User
  6. 1011: User is already Inactive
  7. 1101: Invalid container name
  8. 1103: Group Policy Object (GPO) creation failed
  9. 1104: Group Policy Object (GPO) deletion failed
  10. 1105: Group Policy Object (GPO) linking failed
  11. 1106: Group Policy Object (GPO) unlinking failed
  12. 1107: WMI query failed
  13. 1108: Active Directory error occurred
  14. 1109: Unable to Extract Information from the given Msi Package
  15. 1110: Access is Denied
  16. 1111: File Copy Failed
  17. 1112: Folder Copy Failed
  18. 1113: The Given User Account is not a valid Domain Administrator
  19. 1114: The Given Password is wrong
  20. 1115: Active Directory/Domain Controller not Found
  21. 1222: The Network is not present or not started
- 

### 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 a 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 is 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](mailto: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?](#)
2. [What operating systems are supported by Desktop Central?](#)
3. [What is the difference between Free and Professional Editions?](#)
4. [Do I have to write scripts for using Desktop Central?](#)
5. [What is Scope of Management?](#)
6. [Do I need to define configurations separately or can I group them and define?](#)
7. [When are the configurations applied?](#)
8. [How to access Desktop Central UI or console from the remote ?](#)
9. [What is "Define Target"?](#)
10. [My free trial expired before I was through evaluating Desktop Central. Can I receive an extension?](#)
11. [Why is Desktop Central configuration done through a Web interface?](#)
12. [How is Desktop Central licensed?](#)

### 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)
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 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.

Security Policy	Description
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
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.

Security Policy	Description
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.
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.

The 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 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.

Security Policy	Description
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.
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.

<b>Security Policy</b>	<b>Description</b>
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 settings	Prevents users from changing history 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	Prevents users from changing automatic configuration settings. Automatic configuration is a process that

Security Policy	Description
settings	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.
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 removing components for a LAN or RA connection	Determines whether administrators can add and remove 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).

Security Policy	Description
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, 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

Security Policy	Description
	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 menu	Allows you to remove the Run command from the Start 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.

<b>Security Policy</b>	<b>Description</b>
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.
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 defragmentation 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 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

Security Policy	Description
	determines whether this snap-in is permitted or prohibited.
Restrict/permit Fax services snap-in	<p>If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited.</p> <p>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.</p>
Restrict/permit Indexing services snap-in	<p>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.</p>
Restrict/permit Internet Information Services snap-in	<p>If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited.</p> <p>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.</p>
Restrict/permit Local users and groups snap-in	<p>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.</p>
Restrict/permit Performance logs and alerts snap-in	<p>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.</p>
Restrict/permit Services snap-in	<p>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.</p>
Restrict/permit Shared folders snap-in	<p>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.</p>
Restrict/permit System information snap-in	<p>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.</p>

Security Policy	Description
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.
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.

<b>Security Policy</b>	<b>Description</b>
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](#)
- [Disk Cleanup Tool](#)
- [Disk Defragmenter Tool](#)

## 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 files 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.

<b>See Also:</b> <a href="#">Windows System Tools</a> , <a href="#">Creating and Scheduling Tasks</a> , <a href="#">Viewing and Modifying the Tasks</a> , <a href="#">Viewing Task History</a> , <a href="#">Check Disk</a> , <a href="#">Disk Cleanup</a>
--

## Data Backup and Restore

---

Desktop Central stores all the configuration details, status of deployed configurations, User Logon Reports, Active Directory reports, etc., in the database. Backing up the data is necessary to prevent the data loss that may happen due to unforeseen circumstances.

- [Manual Data Backup](#)
- [Scheduled Data Backup](#)
- [Data Restore](#)

### Manual Data Backup

Follow the steps given below to take a back up of the ManageEngine Desktop Central data manually:

1. Open a command prompt
2. Go to `<Install_Dir>/DesktopCentral_Server/bin` directory.
3. Execute the **backupDB.bat** as given below:  
**backupDB.bat <destination\_directory>**

For example, **backupDB.bat c:\DesktopCentralBackup**

The backup file will be created and stored in the specified location in date-time.zip format. An example of the backup file name: **061018-1635.zip**



**Note:** The MySQL database should be running prior to running the script. If Desktop Central is running, the database will also be running. If not, start the database using the **startDB.bat** located under the `<Install_Dir>/DesktopCentral_Server/bin` directory.

### Scheduled Data Backup

Follow the steps given below to schedule the data backup:

1. Select the **Admin** tab
2. Click the **Database Backup** link available under the Tools category. This opens the Database Backup screen.
3. Specify the time for performing the backup operation. The time should be specified in hh:mm:sec format. The database will be backed up at this time everyday.
4. Select the number of backups to be maintained. The older ones will automatically be deleted.
5. Specify the location to store the backed up database.
6. Select the "*Notify when the database backup fails*" option and specify the email addresses if you want to be notified in cases of any failures. Please note that you should have configured your mail server settings to get notified.
7. Click **Save Changes**.

**Note:**

1. The destination directory specified as the argument should be an existing directory. If you specify a nonexistent directory, the data backup will not happen.
2. The MySQL database should be running when the task is called. If Desktop Central is running, the database will also be running.

## Data Restore

To restore the backed up data, follow the steps below:

1. Open a command prompt
2. Go to `<Install_Dir>/DesktopCentral_Server/bin` directory.
3. Execute the **restoreDB.bat** file as given below:

**restoreDB.bat** *<backup file name>*

The back up file name has to be the .zip file from which you wish to restore the data. This will restore the data from the backup file.

**Note:**

1. Desktop Central should be shutdown prior to restoring the data.
2. 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 interpreter	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

Dynamic Variable	Description	Example Value of the Variable
\$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.
6. Shared and IP Printer configurations will not work in Windows Vista , Windows 2008 and Windows 7 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

---

- [Site](#)
  - [Domain](#)
  - [Organizational Unit](#)
  - [Group](#)
  - [User](#)
  - [Computer](#)
  - [IP Address](#)
  - [Group Policy Object \(GPO\)](#)
  - [Client Side Extension \(CSE\)](#)
  - [Define Target](#)
  - [Scope of Management](#)
  - [Inactive Users](#)
  - [Collection](#)
  - [Applicable Patches](#)
  - [Latest Patches](#)
  - [Missing Patches](#)
  - [Missing Systems](#)
  - [Affected Systems](#)
  - [Informational Patches](#)
  - [Obsolete Patches](#)
- 

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.