

User Guide

Table Of Contents

INTRODUCTION.....	6
USER GUIDE.....	8
Software Installation	8
Installing MSI-based Applications for Users	9
Installing EXE-based Applications for Users	10
Installing MSI-based Applications for Computers.....	11
Installing EXE-based Applications for Computers.....	12
Uninstalling MSI-based Applications for Users.....	13
Uninstalling EXE-based Applications for Users.....	14
Uninstalling MSI-based Applications for Computers	15
Uninstalling EXE-based Applications for Computers.....	16
Patch Management.....	17
Patch Management Architecture	18
Patch Management Life Cycle.....	20
Scan Systems for Vulnerability	22
Installing Missing Patches.....	23
Patch Views	24
Viewing Applicable Patches.....	25
Viewing Latest Patches.....	27
Viewing Missing Patches	28
Viewing Installed Patches.....	29
Viewing Supported Patches.....	30
Viewing Healthy Systems	31
Viewing Vulnerable Systems	32
Viewing Highly Vulnerable Systems	33
Viewing Patch Reports.....	34
Viewing Vulnerable Systems Report.....	35
Viewing Vulnerable Patches Report	36
Viewing Supported Patches Report.....	37

- Hardware and Software Inventory 38
 - Hardware / Software Inventory and Asset Management 38
 - Software Metering 39
 - Viewing Computer Details 41
 - Viewing Hardware Details 42
 - Viewing Software Details 43
 - Viewing Inventory Alerts 45
 - Viewing Inventory Reports 46
 - Hardware Inventory Reports 47
 - Software Inventory Reports 49
 - Software License Compliance Reports 51
- Windows Tools 52
 - System Tools 53
 - Creating and Scheduling Tasks 54
 - Viewing and Modifying the Tasks 58
 - Viewing Task History 59
 - Remote Desktop Sharing 60
 - Remote Desktop Sharing - Pre-requisites 61
 - Connecting to Remote Desktop 63
 - Troubleshooting Tips 65
 - Wake on LAN 67
 - Remote Shutdown Tool 70
- Windows Configurations 75
 - User Configurations 76
 - Configuring Alerts 77
 - Executing Custom Scripts 78
 - Configuring Display Settings 80
 - Mapping Network Drives 82
 - Setting Environment Variables 84
 - Managing Files and Folders 86
 - Redirecting User-Specific Folders 89
 - Installing Software - MSI & EXE Packages 91
 - Configuring Internet Explorer Settings 95
 - Configuring IP Printer 97
 - Launching Applications 99
 - Displaying Message Box 101

Configuring MS Office Settings.....	102
Configuring Outlook Settings	104
Setting Path	107
Managing Permissions.....	108
Configuring Power Options	112
Configuring Registry Settings	115
Securing USB Devices.....	119
Configuring Security Policies	121
Configuring Shared Printer	123
Managing Shortcuts.....	125
Computer Configurations	128
Redirecting Common Folders	129
Executing Custom Scripts.....	131
Setting Environment Variables.....	133
Managing Files and Folders.....	135
Configuring Windows XP Firewall.....	138
Configuring General Computer Settings	140
Managing Windows Local Groups	141
Installing Patches.....	143
Installing Software - MSI & EXE Packages.....	145
Installing Windows Service Packs	149
Configuring IP Printer.....	151
Launching Applications	153
Displaying Legal Notices.....	155
Displaying Message Box.....	156
Setting Path	157
Managing Permissions.....	158
Configuring Registry Settings	162
Securing USB Devices.....	165
Scheduling Tasks	166
Configuring Security Policies	169
Managing Shortcuts.....	171
Configuring Windows Services	174
Managing Windows Local Users.....	176
Configuring Collections	180
Defining Targets.....	181
Managing Configurations and Collections	185

Viewing System Uptime Report	187
Viewing Configuration Reports	188
Configuration Templates	189
Computer Configuration Templates	191
User Configuration Templates	194
User Logon Reports.....	195
Viewing User Logon Reports	196
General Reports	197
Usage Reports	198
History Reports	199
Active Directory Reports	200
Active Directory User Report	201
Active Directory General User Reports	202
User Account Status Reports.....	204
Password Based User Reports	206
Privileged User Accounts.....	207
Logon Based User Reports.....	208
Active Directory Computer Reports	209
General Computer Reports	210
Server Based Reports.....	212
Computer OS Based Reports	213
Active Directory Group Reports	214
Active Directory General Group Reports.....	215
Active Directory Group Type Reports	217
Member Based Reports	218
Active Directory Organization Unit Reports	220
Active Directory General OU Reports	221
OU Child Based Reports.....	222
Active Directory Domain Reports.....	223
General Domain Reports	224
Container Based Reports.....	225
Active Directory GPO Reports	226
General GPO Reports.....	227
GPO Link Based Reports.....	228
Inheritance Based Reports	229

GPO Status Based Reports	230
Special GPO Reports.....	232
Custom Reports.....	233
Creating Custom Reports	234
Custom Query Report.....	235
Making Help Desk Requests	237
APPENDIX.....	238
Interpreting Error Messages	239
FAQs.....	242
Security Policies	245
Security Policies - Active Desktop	246
Security Policies - Desktop	248
Security Policies - Control Panel	249
Security Policies - Explorer.....	251
Security Policies - Internet Explorer.....	253
Security Policies - Network	256
Security Policies - System	258
Security Policies - Task Scheduler	260
Security Policies - Windows Installer.....	261
Security Policies - Start Menu and Taskbar.....	262
Security Policies - Microsoft Management Console	264
Security Policies - Computer	268
Windows System Tools	269
Check Disk Tool.....	270
Disk Cleanup Tool.....	271
Disk Defragmenter Tool.....	272
Data Backup and Restore.....	273
Data Restore.....	274
Dynamic Variables.....	275
Limitations.....	277
Glossary.....	279

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.

User Guide

Software Installation

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

Software Distribution Features

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

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

- [Managing Software Packages](#)
- [Installing MSI-based Applications for Users](#)
- [Installing EXE-based Applications for Users](#)
- [Installing MSI-based Applications for Computers](#)
- [Installing EXE-based Applications for Computers](#)
- [Uninstalling MSI-based Applications for Users](#)
- [Uninstalling EXE-based Applications for Users](#)
- [Uninstalling MSI-based Applications for Computers](#)
- [Uninstalling EXE-based Applications for Computers](#)

Installing MSI-based Applications for Users

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

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

Installing EXE-based Applications for Users

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

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

Installing MSI-based Applications for Computers

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

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

Installing EXE-based Applications for Computers

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

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

Uninstalling MSI -based Applications for Users

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

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

Uninstalling EXE-based Applications for Users

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

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

Uninstalling MSI -based Applications for Computers

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

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

Uninstalling EXE-based Applications for Computers

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

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

Patch Management

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

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

Patch Management Features

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

Follow the links to learn more,

- [Patch Management Architecture](#)
- [Patch Management Life Cycle](#)
- [Setting up Patch Management Module](#)
- [Scan Systems for Vulnerability](#)
- [Viewing Applicable Patches](#)
- [Viewing Latest Patches](#)
- [Viewing Missing Patches](#)
- [Installing Missing Patches](#)
- [Viewing Installed Patches](#)
- [Viewing Supported Patches](#)
- [Viewing Healthy Systems](#)
- [Viewing Vulnerable Systems](#)
- [Viewing Highly Vulnerable Systems](#)
- [Viewing Patch Reports](#)

Patch Management Architecture

- [The Patch Management Architecture](#)
- [How it Works](#)

The Patch Management Architecture

The Patch Management consists of the following components:

- [External Patch Crawler](#)
- [Central Patch Repository](#)
- [Desktop Central Server](#)

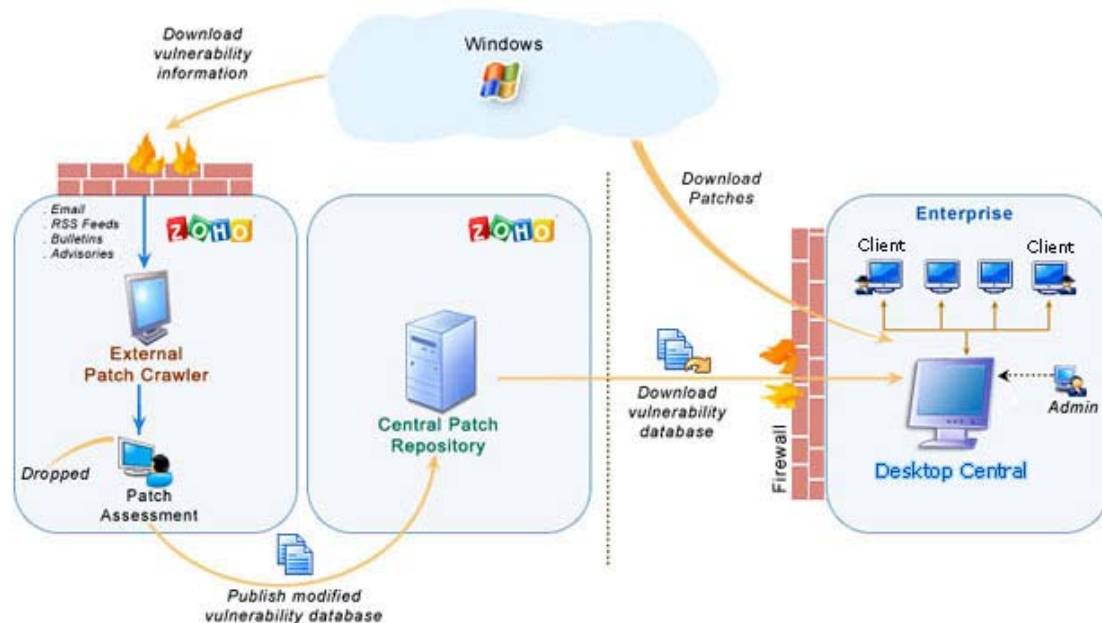


Fig: Patch Management Architecture

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

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

The *Central Patch Repository* is a portal in the Zoho Corp. site, which hosts the latest vulnerability database that has been published after a thorough analysis. This database

is exposed for download by the Desktop Central server situated in the customer site, and provides information required for patch scanning and installation.

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

How it Works?

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

- [Patch Assessment or Scanning](#)
- [Patch Download and Deployment](#)

Patch Assessment or Scanning

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

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

Patch download and deployment

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

See Also: [Patch Management Life Cycle](#), [Setting Up Patch Management Module](#), [Scan Systems for Vulnerability](#), [Patch Reports](#)

Patch Management Life Cycle

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

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

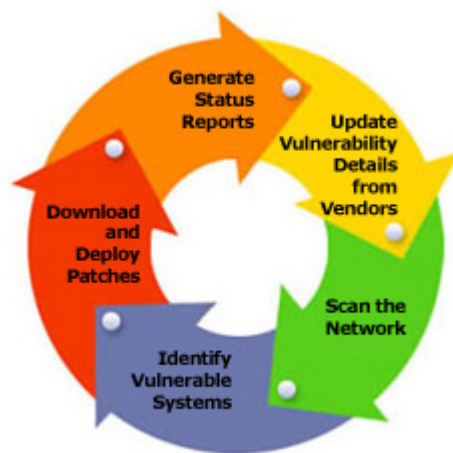


Fig: Patch Management Life Cycle

Update Vulnerability Details from Vendors

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

Scan the Network

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

Identify Patches for Vulnerabilities

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

Download and Deploy Patches

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

Generate Status Reports

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

See Also: [Patch Management Architecture](#), [Setting Up Patch Management Module](#), [Scan Systems for Vulnerability](#), [Patch Reports](#)

Scan Systems for Vulnerability

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

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

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


To reschedule the scan, refer to the [Configure Patch Scan Mode and Scan Interval](#)

See Also: [Patch Management Architecture](#), [Patch Management Life Cycle](#), [Setting Up Patch Management Module](#), [Patch Reports](#)

Installing Missing Patches

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

From the Applicable and Missing Patches Views

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

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

From the Latest and All Supported Patches Views

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

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

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

This opens the [Installing Patches Configuration](#) with the selected patches added. You can then select the targets and deploy the patches.

From the Install Patches Configuration

Like any other configuration, you can manually define a configuration for [installing patches](#) in computers.

See Also: [Viewing Applicable Patches](#), [Viewing Latest Patches](#), [Viewing Missing Patches](#), [Viewing Installed Patches](#), [Viewing Supported Patches](#), [Viewing Healthy Systems](#), [Viewing Vulnerable Systems](#), [Viewing Highly Vulnerable Systems](#)

Patch Views

- [Viewing Applicable Patches](#)
 - [Viewing Latest Patches](#)
 - [Viewing Missing Patches](#)
 - [Viewing Installed Patches](#)
 - [Viewing Supported Patches](#)
 - [Viewing Healthy Systems](#)
 - [Viewing Vulnerable Systems](#)
 - [Viewing Highly Vulnerable Systems](#)
-

Viewing Applicable Patches





Viewing Applicable Patches

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

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


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

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

- **Patch ID:** A unique reference ID in Desktop Central for every patch
- **Bulletin ID:** The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the [Bulletin Details](#) view, which provides more info about the Bulletin and the vulnerability
- **Patch Name:** The name of the patch. Clicking this link, will lead you to the [Patch Details](#) view, which provides more details about the patch.
- **Severity:** Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Affected Systems:** Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed.
- **Installed Systems:** Refers to the count of the systems where the patch has been installed.
- **Missing Systems:** Refers to the count of the systems that do not have the patches installed yet.
- **Action:** You can initiate the following actions by clicking the icons:
 -  - Scan the systems that do not have the patch installed to reconfirm the status.
 -  - To deploy the patch on the missing systems. This opens the [Installing Patches Configuration](#) with the patch added to the configuration; select the targets and deploy.

Installing Patches

You can install the patches in any of the following ways:

- by clicking the  icon of a patch
- by selecting the patches to be installed and by clicking the **Install Patches** button.

Both the above operations, will open the [Installing Patches Configuration](#), with the selected patches added. Select the targets and deploy the configuration.

Bulletin Details

Bulletin details includes the following:

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

Patch Details

The following patch details are shown:

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

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

See Also: [Viewing Latest Patches](#), [Viewing Missing Patches](#), [Installing Missing Patches](#), [Viewing Installed Patches](#), [Viewing Supported Patches](#), [Viewing Healthy Systems](#), [Viewing Vulnerable Systems](#), [Viewing Highly Vulnerable Systems](#)

Viewing Latest Patches



Viewing Latest Patches

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

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

The following details of the patches are displayed:

- **Patch ID:** A unique reference ID in Desktop Central for every patch
- **Bulletin ID:** The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the [Bulletin Details](#) view, which provides more info about the Bulletin and the vulnerability
- **Download Status:** Determines whether the patch is downloaded from the net (vendor site) and is made available in the Desktop Central's Patch Repository for deployment.
- **Patch Name:** The name of the patch. Clicking this link, will lead you to the [Patch Details](#) view, which provides more details about the patch.
- **Reboot:** Specifies whether the patch installation requires a system reboot or not.
- **Severity:** Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.

You can initiate the following actions from here:

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

See Also: [Viewing Applicable Patches](#), [Viewing Missing Patches](#), [Installing Missing Patches](#), [Viewing Installed Patches](#), [Viewing Supported Patches](#), [Viewing Healthy Systems](#), [Viewing Vulnerable Systems](#), [Viewing Highly Vulnerable Systems](#)

Viewing Missing Patches





Viewing Missing Patches

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

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


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

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

- **Patch ID:** A unique reference ID in Desktop Central for every patch
- **Bulletin ID:** The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the [Bulletin Details](#) view, which provides more info about the Bulletin and the vulnerability
- **Patch Name:** The name of the patch. Clicking this link, will lead you to the [Patch Details](#) view, which provides more details about the patch.
- **Severity:** Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Affected Systems:** Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed.
- **Installed Systems:** Refers to the count of the systems where the patch has been installed.
- **Missing Systems:** Refers to the count of the systems that do not have the patches installed yet.
- **Action:** You can initiate the following actions by clicking the icons:
 -  - Scan the systems that do not have the patch installed to reconfirm the status.
 -  - To deploy the patch on the missing systems. This opens the [Installing Patches Configuration](#) with the patch added to the configuration; select the targets and deploy.

Installing Patches

You can install the patches in any of the following ways:

- by clicking the  icon of a patch
- by selecting the patches to be installed and by clicking the **Install Patches** button.

Both the above operations, will open the [Installing Patches Configuration](#), with the selected patches added. Select the targets and deploy the configuration.

See Also: [Viewing Applicable Patches](#), [Viewing Latest Patches](#), [Installing Missing Patches](#), [Viewing Installed Patches](#), [Viewing Supported Patches](#), [Viewing Healthy Systems](#), [Viewing Vulnerable Systems](#), [Viewing Highly Vulnerable Systems](#)

Viewing Installed Patches



Viewing Installed Patches

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

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

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

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

- **Patch ID:** A unique reference ID in Desktop Central for every patch
- **Bulletin ID:** The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the [Bulletin Details](#) view, which provides more info about the Bulletin and the vulnerability
- **Patch Name:** The name of the patch. Clicking this link, will lead you to the [Patch Details](#) view, which provides more details about the patch.
- **Severity:** Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Affected Systems:** Refers to the total count of the systems that require this patch to be installed. This also includes the systems where the patch has already been installed.
- **Installed Systems:** Refers to the count of the systems where the patch has been installed.

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

See Also: [Viewing Applicable Patches](#), [Viewing Latest Patches](#), [Viewing Missing Patches](#), [Installing Missing Patches](#), [Viewing Supported Patches](#), [Viewing Healthy Systems](#), [Viewing Vulnerable Systems](#), [Viewing Highly Vulnerable Systems](#)

Viewing Supported Patches



Viewing Supported Patches

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

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

- **Patch ID:** A unique reference ID in Desktop Central for every patch
- **Bulletin ID:** The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the [Bulletin Details](#) view, which provides more info about the Bulletin and the vulnerability
- **Download Status:** Determines whether the patch is downloaded from the net (vendor site) and is made available in the Desktop Central's Patch Repository for deployment.
- **Patch Name:** The name of the patch. Clicking this link, will lead you to the [Patch Details](#) view, which provides more details about the patch.
- **Reboot:** Specifies whether the patch installation requires a system reboot or not.
- **Severity:** Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
- **Superceded By:** Indicates that the patch is outdated and have another patch that is more recently released and has taken its place.

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

See Also: [Viewing Applicable Patches](#), [Viewing Latest Patches](#), [Viewing Missing Patches](#), [Installing Missing Patches](#), [Viewing Installed Patches](#), [Viewing Healthy Systems](#), [Viewing Vulnerable Systems](#), [Viewing Highly Vulnerable Systems](#)

Viewing Healthy Systems



Viewing Healthy Systems

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

The following details about the healthy systems are shown here:

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

See Also: [Viewing Applicable Patches](#), [Viewing Latest Patches](#), [Viewing Missing Patches](#), [Installing Missing Patches](#), [Viewing Installed Patches](#), [Viewing Supported Patches](#), [Viewing Vulnerable Systems](#), [Viewing Highly Vulnerable Systems](#)

Viewing Vulnerable Systems



Viewing Vulnerable Systems

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

The following details about the vulnerable systems are shown here:

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

See Also: [Viewing Applicable Patches](#), [Viewing Latest Patches](#), [Viewing Missing Patches](#), [Installing Missing Patches](#), [Viewing Installed Patches](#), [Viewing Supported Patches](#), [Viewing Healthy Systems](#), [Viewing Highly Vulnerable Systems](#)

Viewing Highly Vulnerable Systems



Viewing Highly Vulnerable Systems

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

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

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

See Also: [Viewing Applicable Patches](#), [Viewing Latest Patches](#), [Viewing Missing Patches](#), [Installing Missing Patches](#), [Viewing Installed Patches](#), [Viewing Supported Patches](#), [Viewing Healthy Systems](#), [Viewing Vulnerable Systems](#)

Viewing Patch Reports



Viewing Patch Reports

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

- [Vulnerable Systems Report](#)
- [Vulnerable Patches Report](#)
- [Supported Patches Report](#)

Viewing Vulnerable Systems Report



Viewing Vulnerable Systems Report

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

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

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

Application and Patch Summary Report

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

See Also: [Viewing Vulnerable Patches Report](#), [Viewing Supported Patches Report](#), [Viewing Task Status Report](#)

Viewing Vulnerable Patches Report



Viewing Vulnerable Patches Report

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

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

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

See Also: [Viewing Vulnerable Systems Report](#), [Viewing Supported Patches Report](#), [Viewing Task Status Report](#)

Viewing Supported Patches Report



Viewing Supported Patches Report

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

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

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

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

See Also: [Viewing Vulnerable Systems Report](#), [Viewing Vulnerable Patches Report](#), [Viewing Task Status Report](#)

Hardware and Software Inventory

Hardware / Software Inventory and Asset Management

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

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

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

Inventory Management Features

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

Follow the links to learn more,

- [Software Metering](#)
- [Viewing Computer Details](#)
- [Viewing Hardware Details](#)
- [Viewing Software Details](#)
- [Viewing Inventory Alerts](#)
- [Viewing Inventory Reports](#)

Software Metering

Software Metering helps you to monitor the software usage in your organization. Desktop Central Software Metering and Software Inventory helps you to achieve the following:

- Get the list of [software used by each user](#)
- Get the list of [prohibited software](#) used in your network
- Get the [software usage details](#), which helps you to plan software purchases
- Get the [software license compliance](#) status, which helps you to plan additional license purchases or cancel unused licenses.

Software License Management

Desktop Central provides an option to [input the license details](#) of the commercial software used in the network. These details are used in arriving at the software compliance status for each software installed in the network. The software compliance status helps to know software licensing details like the number of software licenses purchased, the number of software licenses that are currently in use and the number of software licenses that are remaining. When the number of software licenses that are used exceeds the actual software licenses purchased, it means that you are not compliant and need to purchase more licenses to become compliant.

The Software License Management provides the following compliance status:

- **Under-Licensed:** When the software copies in use is greater than the copies purchased. This means that you do not have adequate licenses and need to purchase more licenses to become compliant.
- **Over-Licensed:** When the software copies in use is less than the copies purchased. This means that you have purchased more licenses than you actually use.
- **Compliant:** When the software copies in use is almost same as the copies purchased.

Prohibited Software Details

Every organization will have a set of software that are prohibited to be used in accordance with the company policies. Detecting such prohibited software will help in tackling the compliance issues that might arise later. Desktop Central provides an option to [add the list of prohibited software](#) of your company. When any such software is detected it can be configured to be notified through an email to take necessary action.

Software Usage Statistics

It is important to monitor the software usage statistics and record them. Desktop Central provides the details of all the software installed in the network with the total number of copies with the usage details of each software like, Frequently Used, Occasionally Used, or Rarely Used. This will give a complete picture of the used and unused software in the network. This helps to decide on the software purchases and renewals based on the

actual usage. The savings on the license renewal cost can be huge when unused or very rarely used software are known well before the renewal time.

The Software Usage can be any of the following:

- **Frequently Used:** Refers to the software that are used more often.
- **Occasionally Used:** Refers to software that are less frequently used.
- **Rarely Used:** Refers to the software that are rarely being used.

Software Metering Reports

The [Software Inventory Reports](#) and the [Software Compliance Reports](#) helps the administrators to get the Software Metering details and subsequently helps to decide on the software purchases and renewals.

Viewing Computer Details

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

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

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

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

Viewing Hardware Details

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

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

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

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

Viewing Software Details

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

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

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

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

To Add License Details

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

To Specify Software and Access Type

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

To Assign Software to a specific Category

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

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

Viewing Inventory Alerts

Desktop Central generates Email Alerts to notify the following:

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

Based on the [alert configuration](#), alerts are generated. You can view the alerts selecting the **Inventory** tab and clicking the **Alerts** link from the left pane.

You can filter the view based on the Alert Type, which can be any of the following:

- Hardware Added
- Hardware Removed
- Allowed Software Installed
- Allowed Software Uninstalled
- Prohibited Software Installed
- Prohibited Software uninstalled
- Software Under-Licensed
- License Expired
- Prohibited Software Identified
- New Computer Identified

Viewing Inventory Reports



Viewing Inventory Reports

Desktop Central provides various out-of-the-box inventory reports to view the software and hardware inventory details of the systems in the network. It also provides reports for verifying the license compliance and software metering.

- [Hardware Inventory Reports](#)
- [Software Inventory Reports](#)
- [Software Compliance Reports](#)

Hardware Inventory Reports



Hardware Inventory Reports

- [Computers by OS](#)
 - [Computers by Manufacturer](#)
 - [Computers by Memory](#)
 - [Computers by Age](#)
 - [Computers by Device Type](#)
 - [Computer by Disk Usage](#)
-

Computers by OS

Provides the details of the computers by their operating system. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a [remote connection](#) to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by OS** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Manufacturer

Provides the details of the computers by their manufacturer. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a [remote connection](#) to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Manufacturer** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Memory

Provides the details of the computers by their RAM size. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a [remote connection](#) to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Memory** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Age

Provides the details of the computers by their year of manufacturing. A graphical representation of the computers summary is also provided. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a [remote connection](#) to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Age** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computers by Device Type

Provides the details of the computers based on their type like, Laptop, Portable, Desktop etc. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a [remote connection](#) to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computers by Device Type** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Computer by Disk Usage

Provides the details of the computers along with their total and free hard disk space. You can filter the view by domain or by specifying the disk usage criteria. Clicking a specific computer from the report provides more detailed information about the hardware and software details along with their usage metrics. From the computer details view, you can also establish a [remote connection](#) to the computer by clicking the Connect button

To view the report, select the **Inventory** tab and choose the **Computer by Disk Usage** link available under Hardware Reports category by hovering the mouse over the **Inventory Reports**

Software Inventory Reports



Software Inventory Reports

- [Software by Manufacturer](#)
 - [Recently Installed Software](#)
 - [Prohibited Software](#)
 - [Software Usage by Computer](#)
 - [Software Product Keys](#)
-

Software by Manufacturer

Provides the details of the software installed in the scanned systems based on their vendors along with the total number of copies installed. Clicking the copies count will show the computers that have the software installed. You can filter the view by selecting a vendor from the combo box.

To view the report, select the **Inventory** tab and choose the **Software by Manufacturer** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Recently Installed Software

Provides the list of software installed recently. You can choose to select a pre defined period or provide a custom period to get the software list.

To view the report, select the **Inventory** tab and choose the **Recently Installed Software** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Prohibited Software

Provides the list of prohibited software detected in the network.

To view the report, select the **Inventory** tab and choose the **Prohibited Software** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software Usage by Computer

Provides the list of software and their usage statistics in individual computers.

To view the report, select the **Inventory** tab and choose the **Software Usage by Computer** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software Product Keys

Provides the list of Product Keys that were used for installing the software. The Product Keys can be identified for the following software:

1. Adobe Photoshop
2. Macromedia Dreamweaver
3. Macromedia Flash
4. Microsoft Office
5. Microsoft SQL Server
6. Microsoft Visual Studio

To view the report, select the **Inventory** tab and choose the **Software Product Keys** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software License Compliance Reports



Software License Compliance Reports

- [Software License Compliance Report](#)
 - [Software Licenses to be Renewed](#)
-

Software License Compliance Report

Provides the details of the commercial software with their software license compliance status. The software license compliance status is determined based on the input provided in the [Manage Software Licenses](#).

To view the report, select the **Inventory** tab and choose the **License Compliance Report** link available under License Reports category by hovering the mouse over the **Inventory Reports**

Software Licenses to be Renewed

Provides the list of software whose licenses have to be renewed shortly. You can choose the time period from the combo box. You can also view the software licenses that has already expired by selecting the appropriate option. Based on the Software Metering and the usage statistics, you can decide whether to renew the licenses or not.

To view the report, select the **Inventory** tab and choose the **Licenses to be Renewed** link available under License Reports category by hovering the mouse over the **Inventory Reports**

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.

Security Policy	Description
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 an 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.

Security Policy	Description
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.

Security Policy	Description
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.

See Also: [Windows System Tools](#), [Creating and Scheduling Tasks](#), [Viewing and Modifying the Tasks](#), [Viewing Task History](#), [Check Disk](#), [Disk Cleanup](#)

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.