ManageEngine

Desktop Central Admin Guide

Index

ManageEngine® Desktop Central

What is Desktop Management?

Desktop management is a comprehensive approach to managing all the computer systems within an organization. Despite its name, desktop management also includes overseeing laptops and other computing devices that are used within the organization. For IT managers, keeping users' computers up-to-date can be a challenge, especially given the never-ending task of upgrading software to prevent security breaches. Desktop management software helps administrators automate, standardize, secure, and audit all the computing devices within their enterprise.

For businesses with multiple servers, desktops, laptops, and tablets—each running different versions of different operating systems with their own set of software applications—it can be time-consuming and challenging to ensure they're all managed and secure. Not to mention this all has to be done while the admins look after the hardware and software inventory, configurations, security, patches, and software licenses.

What is 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 endpoints, it becomes more difficult to keep up with escalating demand on limited manpower.

Desktop Central is a Unified Endpoint Management (UEM) solution that enables you to secure and manage all forms of endpoints within your enterprise—including servers, desktops, laptops, tablets, smartphones, and point of sale (POS) devices—both inside and outside your organization's network from a central console.

Desktop Central enables configuring and managing endpoints from a single console. With pre-defined configuration options, administrators can perform almost all the regular endpoint administration / management activities with ease.

Desktop Central's capabilities cover the entire endpoint security and management spectrum, including:

- Automated patch management
- Software deployment

- Real-time asset management
- Remote system management
- OS imaging and deployment
- Modern management
- Mobile device management
- Configurations management
- Analytics and reporting

It automates the complete desktop and mobile device management life cycle from start to finish to help businesses cut their IT infrastructure costs, achieve operational efficiency, improve productivity, and combat network vulnerabilities.

Why Desktop Central?

Desktop Central to IT administrators is what IT administrators to an organization are. The realm of an IT administrator's responsibility keeps growing extensively.

Have you been using a myriad of management tools for managing desktops and smartphones in your enterprise?

Desktop Central is a one-stop solution for integrated management of endpoints such as desktops, laptops, smartphones and tablets. True to its name, Desktop Central helps you manage your endpoints from a central locus.

Have you been juggling between different operating systems?

Desktop Central manages assorted endpoints running on varied flavors of operating systems such as Windows, Mac and Linux from a single console. Worry not for variegated network environments such as Windows Active Directory, Windows Workgroups and Novell eDirectory can be managed seamlessly.

Has equipping new systems become a part of your daily routine?

Since every new user in the network costs hours in laborious setup time, Desktop Central's OS Imaging and Deployment truncates the time consumed by helping you provision new systems with just a few clicks.

Tired of the never-ending outpour of Microsoft patch releases?

Desktop Central's Patch Management facilitates automated patch deployment for heterogenous endpoints and third-party applications. Combat critical and zero-day vulnerabilities at the snap of a finger.

Do repetitive tasks span your entire workday?

Desktop Central supports over 50 configurations that automate any task which needs to be carried out on a regular basis, thereby saving a lot of time. Be it securing browsers or USB devices, all you'll have to do is, deploy a configuration.

You cannot manage what you cannot measure. Agree?

Desktop Central's Inventory Management provides details pertaining to the hardware and software assets of your network. Save your organization from legal jeopardy by having an eye on the installation of unlicensed applications.

Do you spend most of the day troubleshooting computers?

Desktop Central's Tools such as Remote Control, System Manager, Remote Shutdown & Wake on LAN come handy for sorting out issues in no time.

Do you find yourself at odds with the employees for helpdesk issues?

Desktop Central integrates with other ManageEngine products and third party helpdesk applications as well so that, helpdesk and desktop management functions can be performed

Have you been investing painstaking efforts for software deployment?

Desktop Central's Software Deployment lets you install, uninstall or update software applications remotely as well as automatically. Overcome challenges in deploying common applications based on the user's needs by publishing the software in Self-Service Portal.

Never been able to comprehend volumes of data when asked to do so?

Produce audit-ready reports effortlessly as Desktop Central helps you run comprehensive reports at the push of a button.

Do you work round the clock to keep your network secured?

Securing your network is no longer a Herculean task. Deploy security policies and configurations for securing browsers or imposing restrictions on the usage of blacklisted applications and unauthenticated devices.

Installation & Setup

Getting started with Desktop Central is as easy as pie. This section will walk you through the -

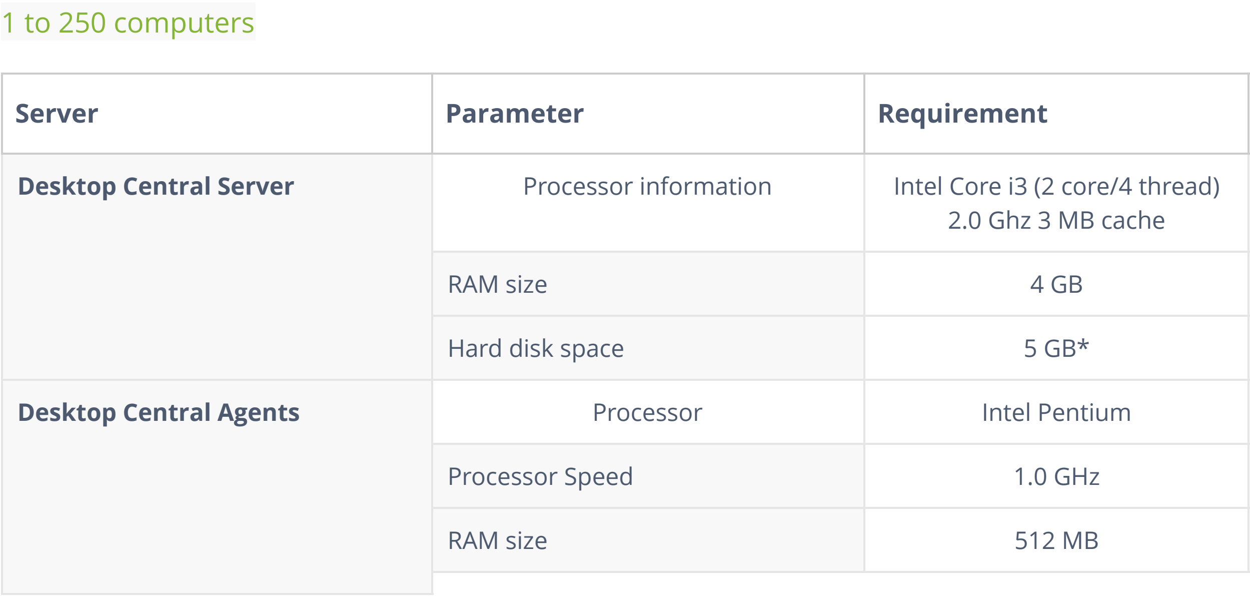
- Prerequisites to be met for installing Desktop Central
- Installation of the product
- Exclusion from antivirus
- Setting up Desktop Central

Setting up Desktop Central can only be done by users with administrative privileges.

Prerequisites:

The following prerequisites need to be met for handling Desktop Central -

System requirements : The hardware and software requirements for installing Desktop Central



1 to 250 computers

Server	Parameter	Requirement
Desktop Central Server	Processor information	Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MB cache
	RAM size	4 GB
	Hard disk space	5 GB*
Desktop Central Agents	Processor	Intel Pentium
	Processor Speed	1.0 GHz
	RAM size	512 MB

Hard disk space	30 GB**	
Network requirement	Network card speed	Minimum 1 GBPS Network Interface Card (NIC)
	Bandwidth	Minimum 1 MBPS (T1 connection)

* May increase dynamically according to the frequency of scanning

** May increase dynamically depending on the operations performed on the client computer

251 to 500 computers

Server	**Parameter**	**Requirement**
Desktop Central Server	Processor information	Intel Core i3 (2 core/4 thread) 2.4 Ghz 3 MB cache
	RAM size	4 GB
	Hard disk space	10 GB*
Desktop Central Agents	Processor	Intel Pentium
	Processor Speed	1.0 GHz
	RAM size	512 MB
	Hard disk space	30 GB**
Network requirement	Network card speed	Minimum 1 GBPS Network Interface Card (NIC)
	Bandwidth	Minimum 1 MBPS (T1 connection)

* May increase dynamically according to the frequency of scanning

** May increase dynamically depending on the operations performed on the client computer

501 to 1000 computers

Server	Parameter	Requirement
Desktop Central Server	Processor information	Intel Core i3 (2 core/4 thread) 2.9 Ghz 3 MB cache
	RAM size	4 GB
	Hard disk space	20 GB*
Desktop Central Agents	Processor	Intel Pentium
	Processor Speed	1.0 GHz
	RAM size	512 MB
	Hard disk space	30 GB**
Network requirement	Network card speed	Minimum 1 GBPS Network Interface Card (NIC)
	Bandwidth	Minimum 1 MBPS (T1 connection)

* May increase dynamically according to the frequency of scanning

** May increase dynamically depending on the operations performed on the client computer

1001 to 3000 computers

Server	Parameter	Requirement
Desktop Central Server	Processor information	Intel Core i5 (4 core/8 thread) 2.3 GHz

RAM size	8 GB	
Hard disk space	30 GB*	
Desktop Central Agents	Processor	Intel Pentium
	Processor Speed	1.0 GHz
	RAM size	512 MB
	Hard disk space	30 GB**
Network requirement	Network card speed	Minimum 1 GBPS Network Interface Card (NIC)
	Bandwidth	Minimum 1 MBPS (T1 connection)

* May increase dynamically according to the frequency of scanning

** May increase dynamically depending on the operations performed on the client computer

3001 to 5000 computers

Server	**Parameter**	**Requirement**
Desktop Central Server	Processor information	Intel Core i7 (6 core/12 thread) 3.2 GHz
	RAM size	8 GB
	Hard disk space	40 GB*
Desktop Central Agents	Processor	Intel Pentium

Processor Speed	1.0 GHz	
RAM size	512 MB	
Hard disk space	30 GB**	
Network requirement	Network card speed	Minimum 1 GBPS Network Interface Card (NIC)
	Bandwidth	Minimum 1 MBPS (T1 connection)
SQL Server	Processor information	Intel Core i7 (6 core/12 thread) 3.2 GHz. 12 MB cache
	RAM size	8 GB
	Hard disk space	30 GB*
	Edition	Standard/Enterprise

* May increase dynamically according to the frequency of scanning

** May increase dynamically depending on the operations performed on the client computer

5001 to 10000 computers

Server	**Parameter**	**Requirement**
Desktop Central Server	Processor information	Intel Xeon E5 (8 core/16 thread) 2.6 GHz
	RAM size	16 GB
	Hard disk space	60 GB*
Desktop Central Agents	Processor	Intel Pentium

Processor Speed	1.0 GHz	
RAM size	512 MB	
Hard disk space	30 GB**	
Network requirement	Network card speed	Minimum 1 GBPS Network Interface Card (NIC)
	Bandwidth	Minimum 1 MBPS (T1 connection)
SQL Server	Processor information	Intel Xeon E5 (8 core/16 thread) 2.6 GHz. 20 MB cache
	RAM size	16 GB
	Hard disk space	40 GB*
	Edition	Standard/Enterprise

* May increase dynamically according to the frequency of scanning

** May increase dynamically depending on the operations performed on the client computer

10001 to 15000 computers

Server	Parameter	Requirement
Desktop Central Server	Processor information	Intel Xeon E5 (12 core/24 thread) 2.7 GHz
	RAM size	32 GB
	Hard disk space	100 GB*
Desktop Central Agents	Processor	Intel Pentium

Processor Speed	1.0 GHz	
RAM size	512 MB	
Hard disk space	30 GB**	
Network requirement	Network card speed	Minimum 1 GBPS Network Interface Card (NIC)
	Bandwidth	Minimum 1 MBPS (T1 connection)
SQL Server	Processor information	Intel Xeon E5 (12 core/24 thread) 2.7 GHz. 30 MB cache
	RAM size	32 GB
	Hard disk space	80 GB*
	Edition	Standard/Enterprise

* May increase dynamically according to the frequency of scanning

** May increase dynamically depending on the operations performed on the client computer

While managing more than 10,000 computers/devices -

1. It is recommended to install SQL server and Desktop Central server in different machines for performance enhancement purposes.
2. Use Windows Server operating systems
3. Use Enterprise grade hard drives or solid state drives (SSD).
4. It is recommended to install Distribution Server for every 1000 computers.

15001 to 20000 computers

Server	**Parameter**	**Requirement**
	Processor information	Intel Xeon E5 (14 core/28

Desktop Central Server		thread) 2.7 GHz
	RAM size	32 GB
	Hard disk space	120 GB*
Desktop Central Agents	Processor	Intel Pentium
	Processor Speed	1.0 GHz
	RAM size	512 MB
	Hard disk space	30 GB**
Network requirement	Network card speed	Minimum 1 GBPS Network Interface Card (NIC)
	Bandwidth	Minimum 1 MBPS (T1 connection)
SQL Server	Processor information	Intel Xeon E5 (14 core/28 thread) 2.7 GHz. 30 MB cache
	RAM size	64 GB
	Hard disk space	120 GB*
	Edition	Standard/Enterprise

* May increase dynamically according to the frequency of scanning

** May increase dynamically depending on the operations performed on the client computer

While managing more than 10,000 computers/devices -

1. It is recommended to install SQL server and Desktop Central server in different machines for performance enhancement purposes.

2. Use Windows Server operating systems
3. Use Enterprise grade hard drives or solid state drives (SSD).
4. It is recommended to install Distribution Server for every 1000 computers.

20001 to 25000 computers

Server	Parameter	Requirement
Desktop Central Server	Processor information	Intel Xeon E5 (16 core/32 thread) 2.7 GHz
	RAM size	32 GB
	Hard disk space	150 GB*
Desktop Central Agents	Processor	Intel Pentium
	Processor Speed	1.0 GHz
	RAM size	512 MB
	Hard disk space	30 GB**
Network requirement	Network card speed	Minimum 1 GBPS Network Interface Card (NIC)
	Bandwidth	Minimum 1 MBPS (T1 connection)
SQL Server	Processor information	Intel Xeon E5 (14 core/28 thread) 2.7 GHz. 30 MB cache
	RAM size	64 GB
	Hard disk space	120 GB*

Edition	Standard/Enterprise

* May increase dynamically according to the frequency of scanning

** May increase dynamically depending on the operations performed on the client computer

While managing more than 10,000 computers/devices -

1. It is recommended to install SQL server and Desktop Central server in different machines for performance enhancement purposes.
2. Use Windows Server operating systems
3. Use Enterprise grade hard drives or solid state drives (SSD).
4. It is recommended to install Distribution Server for every 1000 computers.

Above 25000 computers

For managing more than 25000 computers, contact Desktop Central Support. We will customize Desktop Central server setup based on your network.

Distribution Server

Hardware Requirements for Distribution Servers

The hardware requirements for distribution servers include the following:

No. of Computers Managed Using the Distribution Server	Processor Information	RAM Size	Hard Disk Space
1 to 500	Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MB cache	4 GB	6 GB*
501 to 1000	Intel Core i3 (2 core/4 thread) 2.9 Ghz 3 MB cache	4 GB	12 GB*
1001 to 3000	Intel Core i5 (4 core/8 thread) 2.3 GHz	8 GB	16 GB*
3001 to 5000	Intel Core i7 (6 core/12 thread) 3.2 GHz	8 GB	20 GB*

* May increase depending on the number of software applications and patches that are deployed

Note : It is highly recommended to install Distribution Server for every 1000 computers.

Software Requirements

This section gives you information about the software requirements for Desktop Central Server, Agent and Distribution Server.

Supported Operating Systems

For Desktop Central Server & Distribution Servers

You can install Desktop Central Server & Distribution Servers on any of these Windows operating system versions:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2008*
- Windows Server 2008 R2*
- Windows Server 2012 R2*
- Windows Server 2016*
- Windows Server 2019*

* - **recommended for managing 5000 or more endpoints.**

For Desktop Central Agents

You can use Desktop Central to manage the computers running on the below mentioned operating system.

Supported Database

Desktop Central supports the following databases:

- PGSQL
- MSSQL

        - SQL Server 2005
        - SQL Server 2008
        - SQL Server 2012
        - SQL Server 2014
        - SQL server 2016
        - SQL server 2017

Supported Web Servers

Desktop Central uses the following web servers:

- Apache (for static file services)
- Nginx (for static file services)
- Tomcat (for application related services)

Ports : List of ports to be opened for seamless agent-server communication

Ports to be opened on the Agent

To enable remote installation of the Agent, you should open these ports, these ports may not be required post agent installation.

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

Ports to be opened on the Server

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

Ports to be Opened on the Distribution Server

- 8021: Used for communication between the agents in Remote Offices and the

Distribution Server

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

Supported browsers :

- Microsoft Internet Explorer 10 and later versions
- Mozilla Firefox 44 and later versions
- Google Chrome 47 and later versions
- Microsoft Edge

Application and OS versions :

When you try downloading Desktop Central, you would come across 32-bit and 64-bit options available for download. Here's the difference between a 32-bit and a 64-bit application:

A system comprises three layers: the processor, the operating system and the application. To run either a 64-bit OS or 32-bit OS, we require support from the lower level, processor. Similarly, to run either a 64-bit or a 32-bit application, we require support from all the lower levels such as OS and processor.

There are two types of processors, namely, 32-bit and 64-bit. These refer to the processor architecture and tell us how much memory can be accessed from the CPU register. For instance, a 32-bit system can access 232 memory addresses, i.e 4 GB of RAM and a 64-bit system can access 264 memory addresses, i.e actually 18 billion GB of RAM. The key difference between these processors is the number of calculations performed per second.

- In general, 32-bit programs can run on a 64-bit system but 64-bit programs cannot run on a 32-bit system. This is because 64-bit applications include instructions that will not be recognized by a 32-bit processor.
- A 32-bit OS will run on both 32-bit and 64-bit processors and on the other hand, 64-bit OS will run on only a 64-bit processor. The same can be concluded with 32-bit and 64-bit applications. The main reason behind this is that 64-bit systems are backward compatible with 32-bit systems.

Depending on the architecture of your processor and operating system, download either 32-bit or 64-bit version of Desktop Central.

Installing Desktop Central

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

Uninstalling Desktop Central Server

It is recommended to uninstall the agent from the client computers prior to uninstalling the product. If the client computers are in the same LAN as that of the Desktop Central Server, the agents can be uninstalled from the SoM page of the Desktop Central web console.

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

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

Decoding Desktop Central

Here are a few steps that will help you in traversing the product -

- Working with Desktop Central
- Understanding the client UI
- Licensing the product
- Installing service pack

Working with Desktop Central

Starting Desktop Central

The following are methods of starting Desktop Central -

- Select **Start** -> **Programs** -> **ManageEngine Desktop Central** -> **Start Desktop Central**
- In the **notification area of the task bar** -> **Right click on** -> **ManageEngine Desktop Central icon** -> **Start Service**
- Run **services.msc** -> **Right click on** -> **ManageEngine Desktop Central Server** -> **Start**

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

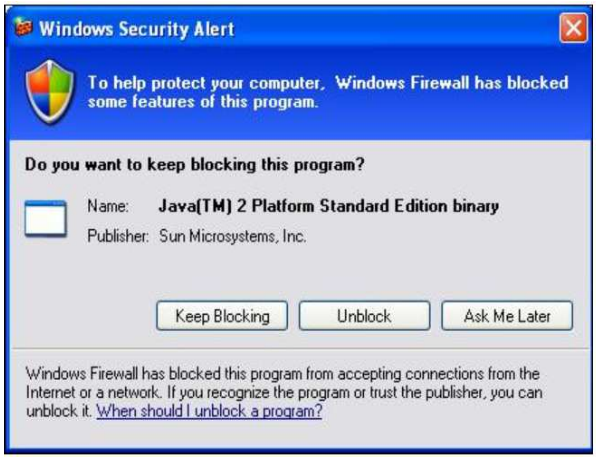
The following processes are started along with the Desktop Central:

1. java.exe - Desktop Central Server
2. postgres.exe - Database Server
3. wrapper.exe - For system tray operations
4. MEDCCPUMonitor.exe - For troubleshooting purposes

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

1. Java(TM) 2 Platform Standard Edition binary - Java.

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



To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: Java(TM) 2 Platform Standard Edition binary

Publisher: Sun Microsystems, Inc.

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Fig: Java Alert

Launching the Desktop Central Client

To launch the Desktop Central client,

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

Steps to perform after initial login

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

- Define the scope of management - Scope can be limited to a small set of computers or the whole domain.
- Define and apply configurations to either users or computers. The applied configurations will take effect during user logon for user configurations and during reboot for computer configurations.
- Setup Patch Management Module
- Setup Software Deployment Module
- Setup Inventory Management

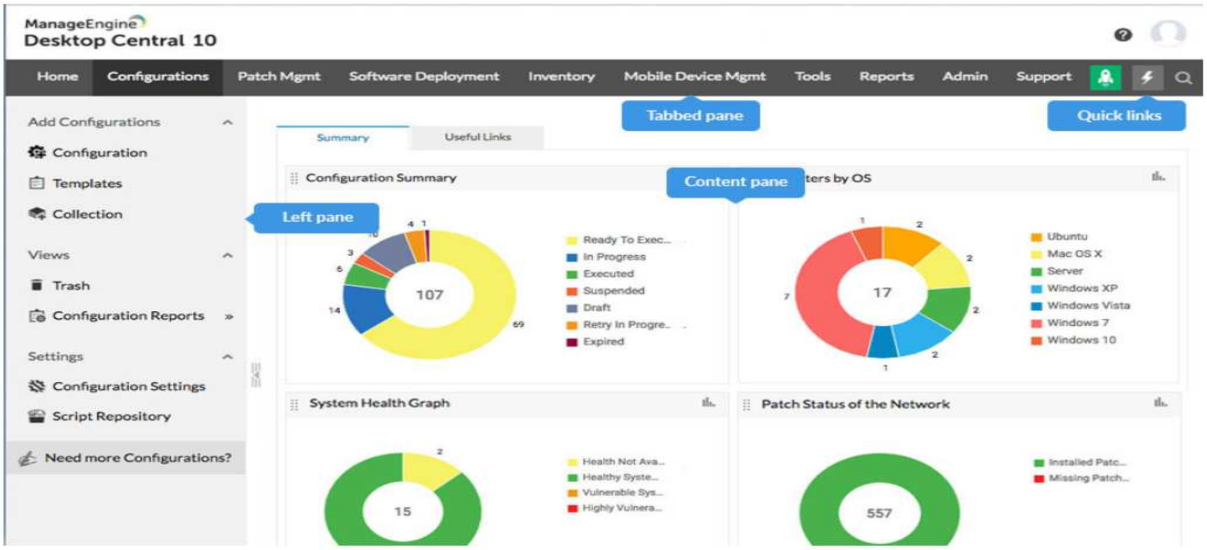
Stopping Desktop Central

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

Understanding the Client UI

- Tabbed Pane
- Quick Links
- Left Pane
- Content Pane

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



Tabbed Pane

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

- **Home**: The home tab provides a quick summary of the configurations defined in the form of charts. Apart from the configuration summary, it also provides Inventory summary and the health/patch status of the network.
- **Configurations**: The configurations tab provides the core functions of the product. It has links to define configurations and collections and view the defined configurations based on the type and status.
- **Patch Mgmt**: This provides the details of the available and missing patch details along

with options to install them.

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

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

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

Quick Links

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

Left Pane

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

Content Pane

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

Licensing the Product

1. Desktop Central is available in four variants :
    - UEM Edition
    - Enterprise Edition
    - Professional Edition
    - Free Edition
2. To know more about the features available in various editions, refer Edition Comparison Matrix.
3. During the evaluation phase, **UEM Edition** will be installed and the product can be evaluated for 30 days. After 30 days, it automatically gets converted to **Free Edition**, unless the license is upgraded to **UEM/Professional/Enterprise Edition.**
4. Download the product from our website.
5. For purchasing the license or for any pricing related queries, please contact sales@manageengine.com.

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

a. When you purchase the product, the license file will be sent through e-mail which can be used to upgrade the product.

b. Click the **License** link available in the top right corner of the web console. This opens the license details of the product.

c. Click **Choose File** and upload the license file received from ManageEngine.

d. Click on **Upgrade**.

Exclusion from Antivirus

Desktop Central and its dependent folders like Distribution Server, Desktop Central Agent need to be excluded from the Anti-virus to ensure hassle free functioning. Antivirus might restrict the Desktop Central server from synchronizing/downloading the patch binaries, agent upgradation, or upgrading Desktop Central server to latest version.

Follow the simple steps to check if Desktop Central folder has been excluded from Antivirus:

Note - While running the test, it is recommended to ignore pop-ups from the antivirus software. Pop-ups appear because the test will stimulate the antivirus software using the EICAR test file. The EICAR Standard Antivirus Test File is developed by the European Institute for Computer Antivirus Research (EICAR) to test the response of computer antivirus programs.

1. Click this link to download the zip file and extract it in the folder location ManageEngine\DesktopCentral_Server\bin\.
2. Double click to run the Antivirus-Checker.bat file.
3. Ignore pop-ups from the antivirus software, that appear while running the test.
4. At the end of the test, you can view either of the two possible results on your window i.e. Antivirus has been excluded or Antivirus has not been excluded.
5. After running the test, go to Desktop Central home page and select 'Update Test Result' button in the message box.

Ensure Desktop Central folders are excluded from antivirus to experience uninterrupted service while managing your endpoints.

Installing Service Pack

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

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

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

The steps to apply a Service Pack are as follows:

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

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

Setting Up Desktop Central

After installing Desktop Central, the administrator has to setup various modules in Desktop Central based on the requirements.

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

Learn to crawl before you can walk.

- Local office management
- Remote office management
- Roaming users management
- Desktop Central in a DMZ
- Desktop Central in AWS
- Desktop Central in Azure
- Mac management
- Linux management

Learn to walk before you can run.

1. Setting up Patch Management
2. Setting up Software Deployment
3. Setting up Asset Management
4. Automate mundane administrative tasks using Configurations
5. Manage endpoints seamlessly using Tools that come handy
6. Generate audit-ready Reports and gain better clarity

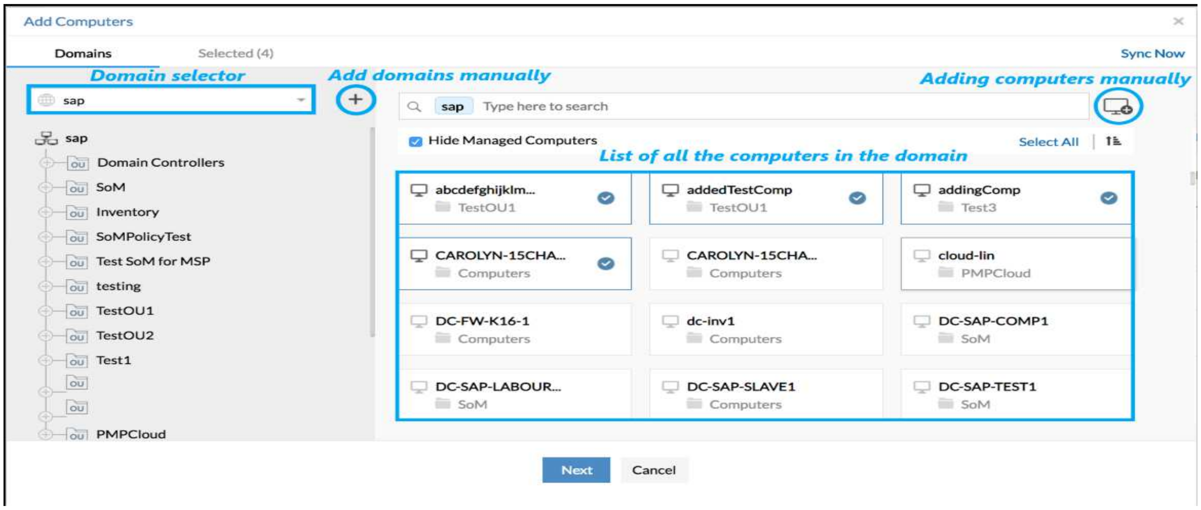
Configuring Agent settings

This document will explain you on the following:

- Installing Agents from Desktop Central Console
- Installing Agents Using Windows GPO (only for Windows)
- Installing Agents Manually
- Retry Agent Installation
- Uninstalling Agents
- Removing the Computers
- Identifying the Live Status of Desktop Central Agent

Installing Agents from Desktop Central Console

- The client computers can be added from **Admin tab -> SoM -> Computers --> Add Computers** button. This will list the domains and workgroups that have been added.

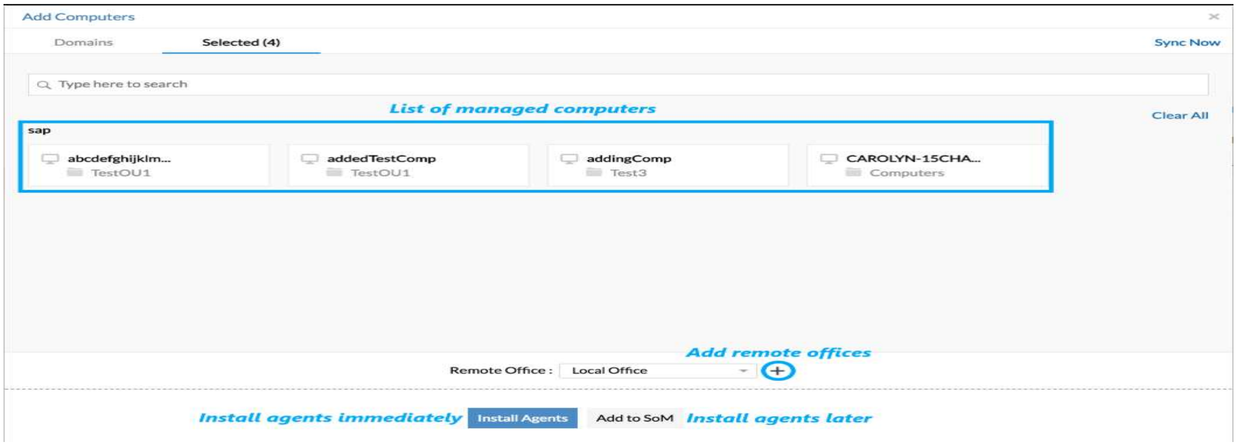


- Click the Select Computers link pertaining to a domain/workgroup. This opens the Select Computers dialog listing all the available computers of the domain/workgroup.
- Select the computers that have to be managed using Desktop Central and click OK. You

can also manually specify the computer names instead of choosing them from the list. The selected computers gets added to the Selected Computers table in the Add Computers view.

- Repeat steps 2 and 3 for adding computers from multiple domains/workgroups.

- Select either the "Add to SoM or Add & Install agents" button to install the Desktop Central agents in the selected computers immediately for the latter and to just add the computers for the former. You need to install the agents later to manage them.



If you are trying to deploy agents to Mac/Linux computers, then ensure that you have provided the root credentials for the deployment to happen remotely.

- Click Done to add the selected computers. All the selected computers gets added to the Scope of Management.

The Scope of Management page will list all the computers that are being managed by Desktop Central along with the status of the agent installation and the agent version. Agents can also be installed at a later stage, by selecting the computers from **Admin -> SoM** page and clicking the **Install Agent** button from the Desktop Central Console. If you have problems in installing the agents, refer to our online knowledge base for possible causes and solutions.

Installing Agents Using Windows GPO

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

Installing Agents Manually

To install a LAN agent manually, follow the steps given below:

1. Under **SoM**, select the **local office** you have added.
2. In the **Download Agent** column, against the local office you have added, click the **Download LAN Agent** icon
3. Save the .zip file in the computer on which you want to install the agent
4. Extract the contents of the zip file
5. Open a command prompt with run as admin privilege and navigate to the location of extracted zip folder and run the command **setup.bat**
6. Select option 1 to install agent in this computer

You have now successfully deployed LAN agent.

Installing Agents using IP Addresses and IP Ranges

You can also install agents using IP addresses and IP ranges by using a .exe file with support files to install agents using a command-line tool. Refer our document for steps to install an agent using IP addresses and IP ranges.

Retry Agent Installation

Enabling this settings will automatically retry to install the Desktop Central agents, on the failed targets. If one of the target computers is not reachable, instead of manually retrying to install the agent, you can specify the number of times, the automatic retry should happen. You can also specify the maximum frequency for this to be repeated. The retry process will be performed based on the specified frequency for the specified number of days. Mail alerts can be configured to notify when the agent installation has succeeded on one or more computers. Follow the steps mentioned below to configure retry agent installation process:

1. Click **Admin -> SoM -> Settings.**
2. Enable the check box, to retry agent installation process

3. Specify the frequency and the number of days for the retry process to happen.

4. Specify the email address to which the notifications need to be sent.

You have successfully configured the settings to retry agent installation on failed computers.

Uninstalling Agents

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

Removing the Computers

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

Identifying the Live Status of Desktop Central Agent

Desktop Central updates the live status of computers periodically. This data is updated every ten minutes or while an on-demand operation is performed on a client computer. You can see the live status of the Desktop Central agents by clicking on SoM, under "Computers" View. The following status will be displayed:

1. The computer icon will be in green color if the Desktop Central Agent is live.

2. The computer icon will be in red, if the Desktop Central agent is down. Desktop Central agent can be down in the following scenarios:

    a. If the computer is not in the network

    b. If the computer is shutdown

    c. If the Desktop Central agent service has been stopped

    d. If the Desktop Central agent has been crashed

3. The computer icon will be in grey, if Desktop Central agent is not installed in it. Those computers are discovered in the SoM because they are added to the active directory but not managed by Desktop Central.

Managing Computers in Wide Area Networks (WAN)

With rapid increase in globalization, most companies have their branch offices spread across different places of the world. Managing the computers in these branch offices effectively is always a tedious job for the system administrators. With Desktop Central in hand, managing computers in WAN across remote office will turn out to be a much easier process. To manage computers in a remote location you have to add remote offices. You can add and modify the remote offices according to your requirement. Communication across these remote offices is possible by two ways

- Through Distribution Server
- Direct communication with Desktop Central server

When to use distribution server

Distribution server acts as a communication layer between your remote office computers and the Desktop Central server. It replicates the software and patch binaries from the Desktop Central server and gives it to the computers in that remote office. The remote office computers, instead of getting the patch and software binaries individually from the Desktop Central server, gets it from the Distribution server, thus saving your WAN bandwidth. So, it is ideal to use a Distribution Server, if you have a limited WAN bandwidth and if you can afford to keep one computer which should be always running, to serve the purpose of Distribution server. We recommend Distribution server when you manage more than 10 computers in your remote office.

When to use direct communication

When you choose your communication type as Direct communication, all the remote office computers will get the required data from the Desktop Central server directly. You can use this option, if you have limited computers in your remote office, say less than 10, or if you do not have any bandwidth limitation.

Adding a remote office

For managing computers in WAN you have to add a remote office. You can add the remote office directly by selecting the **Remote offices** tab and clicking **Add Remote office**. The following points are needed to be taken care while adding a remote office.

1. As discussed above, decide on the communication type you wish to choose while adding a remote office. Either **Through Distribution server** or **Direct communication**.
2. If you choose the communication type **Through Distribution server**, it is recommended that you have a dedicated computer for your distribution server and this computer should have static IP address for hassle free communication between the remote office computers and the distribution server.
3. Select a **Replication Policy** that meets your need and associate it with the remote office to optimize your bandwidth utilization while transferring large binaries from Desktop Central server to Distribution Server. Know more on Replication Policy and its significance here
4. To install Distribution server and WAN agents automatically, under **Remote office agent Installation** section, ensure that you specify the **Domain credentials** with administrator privileges to all the computers managed in the remote office.
5. You can add the computers to be managed either directly by clicking the Add computers option, or by importing a CSV file. For adding multiple computers, the CSV file should contain computer name given in separate lines.

Adding Multiple Remote offices

You can also add the remote office by importing a CSV file. For adding multiple remote offices, the CSV file should contain remote office names given in separate lines.

Modifying a remote office

You can also modify the remote office, by clicking the **Modify** icon, under the **Actions** column against the remote office you want to modify. If you have modified the communication type from Direct communication to **Through Distribution server**, you have to install a Distribution server to manage that remote office.

To know about installing WAN agents and Distribution server click here.

To know about managing computers of roaming users click here.

Installing WAN agents and Distribution server

While adding a remote office, if you have chosen the communication type through a distribution server, installing a distribution server is a mandatory step. Similarly you have to install WAN agents across all the computers you are managing in a remote office.

Installing Distribution Server to Remote Offices

Distribution server is needed to be installed on a dedicated computer with static IP address for hassle free communication. Distribution server can be installed either manually or automatically.

Installing Distribution server automatically

Distribution Server can be installed automatically while adding a remote office by following the below steps,

- While adding the remote office, in the **Remote Agent Installation** section, enable **Install WAN Agent automatically** check box, to install distribution server automatically.

To install Distribution server automatically, under **Remote office agent Installation** section, ensure that you specify the **Domain credentials** with administrator privileges to all the computers managed in the remote office.

Alternatively, it can also be installed automatically by following the steps given below,

- Under **SoM**, select the **Remote Offices** tab.
- In the **Actions** column, click actions and select **Install DS** against the remote office you have added.

Installing Distribution server manually

- Distribution server can be installed manually to the required remote office, by following the steps given below:

- Under **SoM**, select the **Remote Offices** tab
- In the **Download Agent** column, against the remote office you added, click the Download WAN Agent + Distribution Server icon
- Save the .zip file in the computer on which you want to install the distribution server
- Extract the contents of the zip file
- Open command prompt with run as admin privilege and navigate to the location of extracted zip folder and run the command **setup.bat**
- Select option 1 to install distribution server in this computer or select option 3 to install distribution server in this computer and the WAN agents in multiple computers. Before selecting the option to install WAN agents in multiple computers check if you have added all the computers while adding a remote office or edit the .txt file in the extracted folder and add all the computers name to which the agent has to be installed. Each computer has to be specified in separate line.

You have now successfully deployed the distribution server to the required remote office.

Installing WAN Agents to Computers in Remote Offices

WAN agents are needed to be installed in the computers you want to manage in a remote office. Wan agents can be installed either manually or automatically.

Installing WAN agents automatically

WAN agents can be installed automatically while adding remote office. To deploy WAN agents automatically while adding a remote office, follow the steps given below,

- While adding a remote office, in the **Remote office agent installation** section, enable **Install WAN agent automatically** check box to install WAN agents automatically. When the communication is happening through Distribution server, the WAN agent installation will be initiated when the distribution server contacts the Desktop Central server.

🛈 To install WAN agents automatically, under **Remote office agent Installation** section, ensure that you specify the **Domain credentials** with administrator privileges to all the computers managed in the remote office.

🛈 If you move computers across various remote offices, the targeted remote office agents will get installed in the computers automatically.

You have successfully installed WAN agents to computers in a remote office.

ℹ You can also retry agent installation on failed targets automatically, by enabling the **Retry agent installation** check box available in **Settings**under **SOM**.

Installing WAN agents manually

To install a WAN agent manually, follow the steps given below:

- Under **SoM**, select the **Remote Offices** tab
- In the **Download Agent** column, against the remote office you added, click the **Download WAN Agent** icon
- Save the .zip file in the computer on which you want to install the distribution server
- Extract the contents of the zip file
- If you are installing agents on multiple computers, add all the names of the computers in which the agent has to be installed in the computernames.txt file
- Open a command prompt with run as admin privilege and navigate to the location of extracted zip folder and run the command **setup.bat**
- Select option 2 to install WAN agent in this computer or select option 4 to install WAN agents in multiple client computers. Before selecting the option to install WAN agents in multiple computers check if you have added all the computers while adding a remote office or edit the .txt file in the extracted folder and add all the computers name to which the agent has to be installed. Each computer has to be specified in separate line.
- Specify the administrator's user name and password when prompted

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

Managing Computers of Roaming users

The job of an IT administrator gets more challenging when it comes in managing computers of their sales and marketing teams. Users of these teams tend to roam around regularly, thus keeping their computers in track turns out to be a difficult job. In these scenarios, possibilities are high for computers to move from one remote office to another on regular basis. Desktop Central has different agents for different locations, for example a local office agent will not be the same as the remote office agent. Similarly each remote office has different agents as well. To make your management easier, you can have a defined set of IP ranges for different offices. This enables the Desktop Central Server to identify the agents with respect to the IP range. With Desktop Central you can manage computers of users who move between remote offices, as well as those who access the Desktop Central server via internet.

Users who move between remote offices

When your users will roam only within the remote offices, you can add an IP scope and manage their computers. So whenever a computer or laptop is moving from a local office to a remote location, a new IP address is automatically assigned to that computer or laptop by the DHCP server in the remote office network. The Desktop Central agent then determines whether the new IP address, that was assigned, is within the IP range of the new remote office. When a change is detected, the respective remote office agent is deployed automatically. Thus **IP scope** is used to automatically detect and deploy the respective WAN agent. Follow the below steps to add an IP scope,

- Under **SoM**, Click the **IP Scope** tab
- Click **Add Scope**
- In the **Select Remote Office** list, select the required remote office name
- Select either of the following types of IP Scope:
    - **IP Address Range**: Enter the start and end IP addresses
    - **Subnet**: Enter the subnet mask and subnet IP address
- Click **Save**

You have successfully configured IP scope.

If there is a rare chance of computers movement across remote office, instead of defining the IP scope, you can move these computers using the **Move to** option available in **Computers** tab under **SoM**.

Users who access Desktop Central server via internet

Users who tend to travel apart from the remote offices like sales and marketing executives tend to access Desktop Central server via internet. For these users, you can configure a default remote office, such that if a user does not fall under the IP scope of any remote office, they will be automatically assigned to the default remote office. Default remote office works only if IP Scope is configured for other local office or a remote office. Follow the below steps to configure "Default Remote Office"

1. Under **SoM**, click **IP Scope** tab
2. Click **Configure Default Remote Office**
3. Enable the check box to **Enable Default Remote Office**.
4. From the drop down select the remote office/local office which needs to be set as default.
5. Click **Save** to save changes.

Thus managing computers of roaming users is made easier.

Desktop Central in Amazon and Azure

For those who wish to ease their server management using Microsoft Azure virtual machine or Amazon EC2 instance, can now install Desktop Central at your virtual machine or instance and manage your desktops and mobile devices with ease.

- Install Desktop Central at Microsoft Azure
- Install Desktop Central at AWS

Setting up Desktop Central in DMZ

Demilitarized Zone secures the computers of your enterprise from data breaches and vulnerabilities by creating an additional layer of security to your in-house computers. The server from which the services are periodically accessed is exposed directly to the internet.

Refer this document for learning how to setup Desktop Central in DMZ.

Managing Mac Computers

Desktop Central can be used to manage computers with Mac operating Systems. Desktop Central has separate agents to manage Mac computers. This document will explain you on the following:

- Supported Mac OS
- Configuring Mac Agent Settings
- Installing Mac Agents
- Installing Mac Agents Remotely
- Uninstalling Mac Agents
- Supported Features

Supported Mac OS

Desktop Central currently supports the following Mac versions:

- 10.6 Snow Leopard
- 10.7 Lion
- 10.8 Mountain Lion
- 10.9 Mavericks
- 10.10 Yosemite
- 10.11 El Capitan
- 10.12 Sierra
- 10.13 High Sierra
- 10.14 Mojave

Note: Desktop Central currently supports managing Mac OS with Intel Processor

Configuring Mac Agent Settings

Desktop Central has different agents for windows and Mac computers. Mac agents will not be created by default. You can create Mac agents by configuring the settings in the scope of management. This will help you automatically create Mac agents for the local office and the remote offices. To Configure the Mac agent settings follow the steps mentioned below.

- Click the **Admin** tab to invoke the **Admin** page.
- Click the **Agent Settings** link available under SoM Settings.
- Select **Mac Agent Settings tab**

- Specify the **root credentials** for installing the agents remotely to target computer. Ensure that remote login is enabled on the target computer.
- Select the domain or the workgroup to group Mac computers (this is virtual grouping and will not impact on its functions). Agents that are pushed remotely from SoM --> Add Computers will be shown under the respective Domain/Workgroup from which they are added.

While adding credentials it is recommended that the user account falls under active directory else the credentials can be added under workgroup type. This credential will be used for automatic installation of agents across local office computers irrespective of their domain.

- Click **Save Changes** to create Mac agents.

Mac agents can be download from the SoM page.

Installing Mac Agents

Mac agents can be installed manually in the computers that need to be managed. Agents can be installed manually in every computer or through SSH. To install the agent, log-in into the computer as an administrator and follow the steps mentioned below.

- Click the **Admin** tab to invoke the **Admin** page.
- Click on **Scope of Management** link and click on**Computer tab.**
- Click on **Download Agent** link.

You will have a drop down list, from which you can choose and download the appropriate agent. If the managed computers are in the same LAN, download **Mac local agent.** If the managed computers are in remote locations, download agents appropriately. Follow the steps mentioned below to install the agents manually,

- Login into the Mac computer as administrator and navigate to the location where the agent is downloaded.
- Extract the zip file and locate **DesktopCentral_MacAgent.pkg** and serverinfo.plist file.
- Double click to install the agent.
- Enter administrators password when prompted to complete installation.

Installing Mac Agents Remotely

If you wanted to install agents for computers within the LAN, then you can choose the computers and invoke agent installation from the Desktop Central web console **Admin tab --> SoM -->Select computers and invoke agent installation**. If you wanted to install agents to computers which belongs to a different remote office, then you will have to use SSH.

Installing Mac agents to remote office computers can be done easily through SSH. Using a Mac computer you can remotely connect to other computers and install the Mac agents. To know about installing agents follow the steps mentioned below.

- Login into the Mac computer as administrator
- Download the Mac agent.
- Copy the downloaded Mac agent
- Open the terminal
- Navigate to the location where the agent is downloaded.
- Type **scp DCMacAgent.zip adminusername@hostname:** to copy the agent to the target computer.
    - where adminusername - administrator user name of the remote computer
    - hostname - local host name of the remote computer
    - Agent is copied in the location ~/Users/adminusername in target computer
- Install the agent in the remote computer
- To login into the target computer using SSH type **ssh adminusername@hostname**
- Navigate to the location where the agent is copied, Unzip the agent zip file by typing **unzip -oq DCMacAgent.zip**
- Install the agent using the command **sudo installer -pkg DesktopCentral_MacAgent.pkg -target /**
- Enter the administrator password when prompted to complete agent installation.
- Once the agents are installed successfully, the Mac computers will be listed in the SoM page in the Desktop Central web console.

Uninstall Mac agents

To uninstall the agents from the computers, follow the steps mentioned below.

- Login into the computer as administrator and open the terminal.
- Navigate to the directory /Library/DesktopCentral_Agent/uninstall
- Type **sudo chmod 744 uninstall.sh,** and enter administrator password when prompted.
- Type the command **sudo ./uninstall.sh,** this command removes all the files except logs.

Supported Features

Desktop Central currently supports the following features for Mac computers.

- Patch Management
- Software Deployment
- Managing software License
- Managing Software Category
- Hardware and software inventory reports
- Alerting by email for every hardware or software changes.
- Configurations
- Remote Control
- Remote Shutdown

Managing Linux Computers

Administrators can use Desktop Central to manage computers running Linux operating system. This document will explain you on the following:

- Supported Linux OS
- Configuring Linux Agent Settings
- Installing Desktop Central Agents
- Installing Desktop Central Agent Remotely
- Uninstalling Desktop Central Agents

Supported Linux OS

Desktop Central currently supports the following Linux versions:

- Ubuntu 10.04 and later versions
- RedHat Enterprise Linux 6 and later versions
- CentOS 6 and later versions
- Fedora 19 and later versions
- Mandriva 2010 and later versions
- Debian 7 and later versions
- Linux Mint 13 and later versions
- Open SuSe 11 and later versions
- Suse Enterprise Linux 11 and later versions

Configuring Linux Agent Settings

Desktop Central has different agents for managing windows, Mac and Linux computers. Mac and Linux agents will not be created by default. You can create Linux agents by configuring the settings in the scope of management. This will help you automatically create Linux agents for the local office and the remote offices. To Configure the Linux agent settings follow the steps mentioned below.

- Click the **Admin** tab to invoke the **Admin** page.
- Click the **Agent Settings** link available under SoM Settings.
- Select **Linux Agent Settings tab**

- Select the domain or the workgroup to group Linux computers (this is virtual grouping and will not impact on its functions). Agents that are pushed remotely from SoM --> Add Computers will be shown under the respective Domain/Workgroup from which they are added.

The credentials added will be used for automatic installation of agents across local office computers irrespective of their domain. While adding credentials, it is recommended that the user account falls under active directory else the credentials can be added under workgroup type.

- Click **Save Changes** to create Linux agents.

Linux agents can be download from the SoM page, by choosing the appropriate agent, such as LAN agent or WAN agent for specific Remote offices.

Installing Desktop Central Agents

Linux agents can be installed manually in the computers that need to be managed. Agents should be downloaded on the Linux computer manually before initiating the installation process. For invoking the installation in client computers, SSH port (default port 22) should be open in the computers where the agent needs to be installed. SSH port is used only for agent installation purposes and not for agent-server communication. Follow the steps mentioned below.

- Go to the terminal as a root user. If you do not login as a root user, open the terminal and use sudo command to perform each operation mentioned below and enter password whenever prompted. This provides you the root privilege.
- Navigate to the location, where the agent is downloaded and Unzip the DCLinuxAgent.zip by using the command "**unzip -e DCLinuxAgent.zip**".
- Verify if, **"DesktopCentral_LinuxAgent.bin" & "serverinfo.json"** are located in the same path
- Execute the Command, "**chmod +x DesktopCentral_LinuxAgent.bin**" as a root user. This prepares the executable for installation.
- Run the Installer using "**./DesktopCentral_LinuxAgent.bin**". Agent will be installed by default in "**/usr/local/desktopcentralagent**" directory.
- If you wanted to change the installation location of the agent, use this command "**./DesktopCentral_LinuxAgent.bin -d <new_location>**" .

You can see that the Desktop Central agent is successfully installed on the Linux computer. You need to install the agents manually on the computers, which needs to be managed using Desktop Central. Once the agent installation is completed, the computer will be scanned automatically and the following details will be updated to the Desktop Central server:

- **System Details** : All details about the computer, like Users, Groups and Services. This does not include details on the network shares mapped to the computer.
- **Hardware Details** : All hardware details of the computer like, BIOS, Disk Drives, Physical Memory, Processors, Network Adapters etc. This does not include details on Printers and Ports.
- **Software Details** : All details on the software that is installed on the managed computer, with the version of the application and installation date etc.

Installing Desktop Central Agent Remotely

ℹ If you wanted to install agents for computers within the LAN, then you can choose the computers and invoke agent installation from the Desktop Central web console **Admin tab --> SoM -->Select computers and invoke agent installation**. If you wanted to install agents to computers which belongs to a different remote office, then you will have to use SSH port (default port 22)

When you want to push Desktop Central agents to remote office computers, you can install them using SSH (default port 22), provided the port should be open. Follow the steps mentioned below to install Desktop Central agent using SSH (default port 22):

- Login to a Linux computer
- Download the appropriate agent, based on the remote office
- Copy the downloaded Desktop Central agent to the remote computer on which the agent needs to be installed
  - Go to terminal as root user
  - Navigate to the location where the agent is being copied/downloaded
  - Type "**scp DCLinuxAgent.zip username@hostname:<Path_To_Storage_Directory_If_Needed>"** to copy the agent to the target computer, enter password if prompted
    where **username** refers to the root user name of the target computer
    hostname refers to the local host name of the target computer
    If no path is specified, then the agent will be copied to **"/home/username"** in the target computer
- Install the agent by following the steps mentioned below:
  - Go to the terminal and Type **"ssh rootusername@hostname"** to login to the target computer
  - Login as a root user. If you do not login as rootuser, open the terminal and use sudo command to perform each operation mentioned below and enter password whenever prompted. This provides you the root

privilege.

- Navigate to the location, where the agent is downloaded/copied, if the downloaded agent is a remote office agent, then extract**<Remote_Office_Name>.zip** and navigate to Unzip the DCLinuxAgent.zip by using the command "**unzip -e DCLinuxAgent.zip**".
- Verify if, **"DesktopCentral_LinuxAgent.bin" & "serverinfo.json"** are located in the same path
- Execute the Command, "**chmod +x DesktopCentral_LinuxAgent.bin**" as a root user. This prepares the executable for installation.
- Run the Installer using "**./DesktopCentral_LinuxAgent.bin**". Ensure that the Property File **"severinfo.json"** exists in the Same Directory as **"DesktopCentral_LinuxAgent.bin**". Agent will be installed by default in "**/usr/local/desktopcentralagent**" directory.
- If you wanted to change the installation location of the agent, use this command "**./DesktopCentral_LinuxAgent.bin -d <new_location>**" .

You have successfully installed the Desktop Central agent on a remote computer using SSH.

Uninstalling Desktop Central Agents

If you do not want to manage a computer, you can follow the steps mentioned below to uninstall the Desktop Central agent. Once Desktop Central agent is uninstalled, all the details related to the computer will be removed from Desktop Central server. If you wanted to manage this computer again, then you will have to re-install Desktop Central agent in it. However the previous details related to the computer will not be available. To uninstall the agents from the computers, follow the steps mentioned below:

- Go to the terminal as a root user. If you do not login as root user, open the terminal and use sudo command to perform each operation mentioned below and enter password whenever prompted. This provides you the root privilege.

- Navigate to the location, where the agent is installed, (**default Location : /usr/local/desktopcentralagent**) execute this command to "**chmod +x RemoveDCAgent.sh**" to initiate the uninstaller. You need to have root privilege to uninstall the agent. If you do not remember the installation location, you can locate it here, **Agent Installed Directory : "/etc/desktopcentralagent/dcagentsettings.json"**

- Execute this command "**./RemoveDCAgent.sh**" to uninstall the agent.

You can see that the Desktop Central agent has been uninstalled successfully from the computer.

Supported Features:

Desktop Central currently supports the following features for Linux computers.

Features supported in the Inventory Module

- Managing Software License
- Managing Software Categories
- Hardware & Software Inventory Reports
- Alerting by email for every Hardware & Software Changes.

Features supported in the Patch Module

- Automate patch deployment to Linux OS and thirdy party applications
- Patch compliance audits and reports

Features supported in the Software Deployment Module

- Supports installing/uninstalling of DEB based applications
- Customize and schedule software deployment during non business hours

Feature supported in the Configurations Module

- Execution of custom scripts

Features supported in Remote Control

- Remotely access computers on LAN and WAN using Active X and HTML5 Viewer
- Prompts user confirmation before providing access to a remote desktop
- Multi-monitor support with easy switching options

Defining Scope of Management

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

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

- Adding Domain/Workgroup
- Managing computers in LAN
- Managing computers in WAN
- Configuring Modern Management
- Managing Computers running Mac Operating System
- Managing Computers running Linux Operating System

Adding Domain/Workgroup

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

Discovering Domains / Workgroups

To view the discovered domains/ workgroups or to initiate the discovery, select **Admin tab -> Scope of Management (SoM) -> Computers tab -> Add Computers**. This will list all the computers belonging to a domain.

Adding Domains

Domain can be added in Desktop Central in three ways:

1. From the list of computers available in the **SoM --> Add Computers** page select the computers that need to be managed using Desktop Central.
2. Domains can be added manually but, if for some reason, one or more domains are not discovered, you can use the **Add Domain** icon available in the same page to add domains manually.
3. Navigate to **Admin tab -> Global Settings -> Domain -> Add Domain**

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

Parameter	Description	Type
Domain Name	Name of the domain. This is usually the netbios or the pre-2000 name of the domain	Mandatory
Network Type	Select "Active Directory" option	Mandatory

Domain User Name	This should be the domain user name that has administrative privileges in all the computers of that domain. It is recommended to have a dedicated domain admin user account for Desktop Central whose password policy is set to "Never Expire"	Mandatory
Password	Password of the domain admin user	Mandatory
AD Domain Name	The DNS name of the Active Directory Domain	Mandatory
Domain Controller Name	The name of the domain controller. If you have multiple domain controllers, provide the name of the domain controller that is nearest to the computer where Desktop Central Server is installed	Mandatory
Enable the checkbox to use LDAP SSL	By enabling this checkbox, the communication between Desktop Central server and Active Directory will be secured. The default port used is 636.	Optional

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

Adding Workgroups

Similar to domains, workgroups can be added in Desktop Central in three ways:

1. From the list of computers available in the **SoM -> Add Computers** page select the computers that need to be managed using Desktop Central.
2. Workgroups can be added manually but, if for some reason, one or more workgroups are not discovered, you can use the **Add Domain** icon available in the same page to add workgroups manually.
3. Navigate to **Admin tab -> Global Settings -> Domain -> Add Domain**

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

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

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

ℹ Computers in Novell eDirectory based network are managed as Workgroups in Desktop Central.

Changing the Domain or Workgroup Credentials

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

tab -> Global Settings -> Domain -> to avoid getting "Access Denied" errors while performing any remote operations.

To update the credentials, choose to **Modify** against the corresponding domain/workgroup under Actions column. Edit the credentials and click **Update Domain Details**.

SoM Policy - How to add/remove computers from Desktop Central

You can automate the process of adding and removing computers that are managed by Desktop Central by configuring the SoM policy. This helps you to synchronize computers from Active Directory. So you will find the computers that are newly added in the Active Directory, but are not managed in Desktop Central and the computers that have been deleted from the Active Directory. This helps you to quickly add or remove computers from the list of computers managed using Desktop Central.

The synchronization will happen at a specified time everyday and can be configured to notify you whenever a change is detected. You can also initiate the sync option as and when required with sync only modified data and sync all option. Sync only modified data will list only the changes that has happened after the previous sync. So the computers which are added or removed after the previous sync will be listed here. Sync all option can be used to get the complete list of all the computers that has been added or removed in the active directory.

To enable synchronization follow the steps below:

- Select **SoM -> SoM Policy** tab
- Enable the checkbox to **Detect and Add New Computers**
- Specify the action that needs to be performed when a new computer is added to the Active Directory; Whether to notify me and install an agent automatically or just notify me.
- Enable the checkbox to **Delete Inactive Computers**
- Specify the action that needs to be performed when a new computer is removed from the Active Directory or it has been inactive for a long time; Whether to remove the computer from the SoM automatically and notify me or to just notify me.
- Specify the number of days allowed for the computers to be inactive and the action to be performed.
- Specify the notification mail message that needs to be displayed while a computer is inactive for a long time.
- Specify the time at which the sync should happen. The time should be specified in 24 hour format and the sync will happen at the same time everyday.
- Click **Choose Domains/OUs** to select the domains and OUs that you would like to sync.

This will only list the domains and OUs for which the credentials have been specified.

Note: If you do not see all the domains, you should check and specify the credentials first from SoM -> Computers -> Edit Credential.

- If you wish to be notified on any change, select "**Enable Email Notification**" and specify the "To Address", subject and message.
- Click **Save**

ℹ You can choose to exclude computers for management purpose, within Desktop Central. Excluding here, refers to removing the computers, which need not be managed by Desktop Central. You can select them, click on "Exclude Computers", button by navigating here : Desktop Central web console -> SoM ->, SoM Policy -> Exclude Computers. You can view all the excluded computers, and choose to install agents anytime in the future.

ℹ From the SoM summary page, you can manually troubleshoot computers in which the agent upgrade has failed. Upon clicking the troubleshooting page, several agent versions along with the computer count will be displayed in the drop down. Depending on the version that has failed, you can choose to troubleshoot. SoM troubleshooting page will shed light on the status in Active Directory, Distribution Server status, and the agent status.

Next Steps

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

- Managing Computers in LAN - To add and install the agent in the client computers from the same LAN where Desktop Central Server is installed

- Managing Computers in WAN - To add and install the agent in the client computers from remote locations like branch offices and mobile users.

Modern Management

With the wide rage of trend and technological changes, organizations are taking a big leap towards enterprise mobility and security. To cope-up with such trends, Desktop Central adopts the approach of Modern Management. To unleash the Modern Management capabilities of Desktop Central, ensure you are using the Desktop Central - UEM Edition.

Benefits of using UEM edition

1. Manage Windows 10 desktops, laptops, mobile devices and surface pro tablets from a single suite.
2. Uncomplicate your Desktop Central license management. Mobile Device Management is no more an add-on. Puchase licenses to manage computers and mobile devices as endpoints and unify your license management.
3. Read the full set of benefits here.

How UEM works?

Desktop Central's UEM Edition is exclusively packaged to cater the needs of enterprises looking for one solution for all the system management needs. UEM edition serves as a centralized expertise, that could help system administrators manage everything right from desktops to modern mobile devices from a single console.

1. The first step to manage endpoints using Desktop Central is to include all the network computers under Desktop Central's Scope of Management.
2. Once you are done with this, all the computers running in Windows 10 OS will be listed under Mobile Device Management tab -> Enrollment -> Laptop and Surface pro enrollment from where you will have to assign a user to that particular machine.
3. Now, enroll all the Windows 10 mobile devices by referring this page.

After completing the enrollment process, you can leverage the following Modern Management capabilities in Desktop Central.

- Geo-tracking

  Know how to locate all the managed Windows 10 laptops, desktops and mobile devices.

- Corporate or Selective Wipe

  All the configurations and applications that were installed using Desktop Central will be wiped out. This will not disturb any personal data other than the corporate data which has been distributed through Desktop Central. This endpoint will no longer be managed by Desktop Central. In case of Windows device, this action will be performed only when the device contacts the Desktop Central server.

- Complete Wipe

All the data in the endpoint will be completely wiped out. The endpoint will become as good as new. You can also wipe all the data from the SD card, for SAFE and KNOX devices. In case of Windows devices, the enrollment is retained (OS version 1803) even after the data is wiped. If PPKG enrollment is used for other devices, the provisioning package is retained. The endpoint can be used again by just assigning new users.

- KIOSK mode

Read and find how to distribute applications in KIOSK mode.

- Windows store app distribution

Distribute Windows store apps to Windows 10 laptops, desktops, surface pro tablets by adding the software packages.

- Distribute Profiles (restrictions and configurations)

Impose policies and restrictions to the managed Windows 10 computers, tablets and mobile devices.

- Distribute Certificates with SCEP

Read and understand how certificates can be distributed using SCEP.

Configuring Desktop Central Settings

Configure a bunch of settings to make the best of Desktop Central. Desktop Central is a standout from the clichè enpoint management software, as it segregates the settings to be configured.

1. ***General Settings***: Experience hassle-free endpoint management by configuring these settings, irrespective of the feature utilized
2. ***Feature-specific Settings***: Draw a clear line between various features offered by Desktop Central by configuring settings pertaining to specific features
3. ***Value-added Settings***: Enjoy the additional perks of using Desktop Central by configuring settings that augment the value of endpoint management.

General Settings

Here's the list of feature-independent settings that need to be configured -

1. *Administration*
    - User administration
    - Credential Manager
2. *Scope of Management*
    - Adding domain/workgroup
    - Agent Settings
    - Replication Policy
3. *Server*
    - Mail Server Settings
    - Server Settings
    - Server Migration
    - NAT Settings
4. *Security*
    - Export Settings
    - Import SSL Certificates
5. *Database*
    - Remote DB Access
    - MSSQL migration
    - Schedule DB Backup

User Role and Permission

This document will explain the various roles and permissions which can be mapped for users. The below table explains in detail about the roles, that are created by Desktop Central by default. You can create roles and customize it based on your requirement.

Action	Administrator	Full Control	Write	Read
Configuration				
Create Configurations (Users and Computers)	✓	✓	✓	✗
Create Configurations from templates	✓	✓	✓	✗
Create Configurations from Collections (Users and Computers)	✓	✓	✓	✗
Install software	✓	✓	✓	✗
Install patches	✓	✓	✓	✗
View Configurations	✓	✓	✓	✗

Edit Configurations	✓	✓	✓	✗
Delete Configurations	✓	✓	✓	✗
'Save as New' from Configurations	✓	✓	✓	✗
Power Management Configuration	✓	✓	✓	✗
Patch Mgmt.				
Install Patches	✓	✓	✓	✗
Automate Patch Deployment (APD)	✓	✓	✓	✗
APD Task List View	✓	✓	✓	✗
Edit or Delete APD	✓	✓	✓	✗
View Configurations	✓	✓	✓	✗

View Deployment Templates & Add Templates	✓	✓	✓	✗
Edit or Delete Deployment Templates	✓	✓	✓	✗
Approve/Decline/Un Approve - Applicable Patches	✓	✓	✗	✗
Download / Re-download /Delete Patches	✓	✓	✗	✗
Deploy Missing Patches to All Managed Systems	✓	✓	✓	✗
Scan/Scan All	✓	✓	✓	✓
Patch Report	✓	✓	✓	✓
Patch Settings (Except Proxy)	✓	✓	✗	✗
Update Vulnerability Database	✓	✓	✓	✗
Software Deployment				

Create Software Package	✓	✓	✓	✗
Install/uninstall Software (Computer)	✓	✓	✓	✗
Install/uninstall Software (User)	✓	✓	✓	✗
Create Package from Templates	✓	✓	✓	✗
View Configurations	✓	✓	✓	✗
Deployment Templates	✓	✓	✓	✗
Software Repository Settings	✓	✓	✓	✗
Sync Application Details	✓	✓	✓	✗
Self Service Portal	✓	✓	✓	✗

Self Service Portal Settings	✓	✓	✓	✗
'Save as New' from Packages	✓	✓	✓	✗
Inventory				
Computers View (Bulk Update/ Import CSV)	✓	✓	✓	✗
Computers View - Import CSV	✓	✓	✓	✓
Add / Modify Computer Details	✓	✓	✓	✗
Hardware's View	✓	✓	✓	✓
Software View	✓	✓	✓	✓
Move Software To	✓	✓	✗	✗
Alerts settings	✓	✓	✓	✗

Inventory Reports	✓	✓	✓	✓
Scan/Scan all Systems	✓	✓	✓	✓
Software Metering (Add/Delete/Enable/Disable Rule)	✓	✓	✗	✗
Manage License	✓	✓	✗	✓
Group software	✓	✓	✗	✓
Configure Prohibited Software	✓	✓	✗	✓
Block executables	✓	✓	✗	✗
File scan rules	✓	✓	✗	✓
Add Global Exclusions	✓	✓	✗	✗

Manage Software Category	✓	✓	✓	✓
Configure Alerts	✓	✓	✓	✗
Schedule Inventory Scan	✓	✓	✓	✗
Feed Custom Data for Computers	✓	✓	✓	✗
Tools				
Remote Control Computer view	✓	✓	✓	✓
Remote Control History view	✓	✓	✓	✓
Settings	✓	✓	✗	✗
User Confirmation & Exclude Computers	✓	✗	✗	✗
Screen Recording	✓	✓	✗	✗

Performance	✓	✓	✗	✗
Wake On LAN - Wake up & schedule wake up	✓	✓	✓	✗
Remote Shutdown - Shutdown now & schedule shutdown	✓	✓	✓	✗
System Tools - Action & Functionality	✓	✓	✓	✗
Announcement	✓	✓	✓	✗
Chat	✓	✓	✓	✓
System Manager tools (Except Command Prompt, Registry & File Manager)	✓	✓	✓	✓
System Manager Tools - Command Prompt, Registry & File Manager	✓	✓	✓	✗
Reports				
Schedule Reports	✓	✓	✓	✗

Custom Reports	✓	✓	✓	✗
Active Directory Reports	✓	✓	✓	✗
Reports from Other Modules	✓	✓	✓	✗
SoM				
Add/Remove computers	✓	✓	✓	✗
Edit credential	✓	✓	✗	✗
Install/uninstall agent	✓	✓	✓	✗
Remote Offices	✓	✗	✗	✗
IP Scope	✓	✗	✗	✗
SOM Policy	✓	✗	✗	✗

Agent settings	✓	✗	✗	✗
Global Settings				
User Administration	✓	✗	✗	✗
Help Desk Settings	✓	✗	✗	✗
ServiceDesk Plus Settings	✓	✗	✗	✗
Server Settings	✓	✗	✗	✗
Mail Server Settings	✓	✗	✗	✗
Custom Groups	✓	✗	✗	✗
Re-branding	✓	✗	✗	✗
PgSQL Remote DB Access	✓	✗	✗	✗

DC Server Migration	✓	✗	✗	✗
Configuration Settings	✓	✗	✗	✗
Security Settings	✓	✗	✗	✗
Import SSL Certificates	✓	✗	✗	✗
Privacy Settings	✓	✗	✗	✗
Forwarding Server	✓	✗	✗	✗
DPO Dashboard	✓	✗	✗	✗
Export Settings	✓	✗	✗	✗
Server Maintenance	✓	✗	✗	✗

Failover Server	✓	✗	✗	✗
NAT Settings	✓	✗	✗	✗
MSSQL Migration	✓	✗	✗	✗
DB Optimization	✓	✗	✗	✗
Report Settings				
AD Report Settings	✓	✗	✗	✗
User Logon Settings	✓	✗	✗	✗
Admin Tools				
Action Log Viewer	✓	✗	✗	✗
Alerts	✓	✗	✗	✗

Credential Manager

Overview

Desktop Central requires credentials like user name and password to perform various desktop management activities inside the product, say for adding a domain or workgroup, for accessing a network share to deploy software, for deploying certain configurations etc., These credentials details are collected at different places dependent on where they are required, and managing them across the product is tedious and time consuming. Credential Manager provides a unified solution to store and manage all these credentials globally from a centralized location.

Understanding Credential manager

Credential manager validates the domain credentials while you add them and the invalid credentials are not accepted. Any changes related to the user name or password of domain credentials are notified to you in the form of alerts. Thus you can incorporate these changes globally using credential manager, instead of changing them in all the areas across the product. Other workgroup and user credentials are not validated using credential manager, so ensure that you provide the correct details. The workgroup and domain credentials added under the scope of management are considered as root account credentials and are automatically stored in the credential manager. You are not allowed to delete these root account credentials, if needed you can edit or modify them. Similarly you are not allowed to delete a credential, if it is used inside the product, say for executing a software.

Who can add credentials?

Users other than administrators with write privileges can also add the credentials, by finding credential manager under the settings tab. These users do not have the privileges to view or edit the credentials added by the administrator and other users. The privilege to view all the credentials is given only to the administrator.

Configuring Agent Settings

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

Agent General Settings

- Navigate to Admin -> SoM Settings -> Agent Settings.
- The **General Settings** tab is selected by default. You can specify the following from here:
    - **Server IP Address -** The IP Address of the computer where Desktop Central server is installed is displayed here. The agents residing in the client computers communicate to the Desktop Central server using this IP Address. Desktop Central automatically detects the server IP Address whenever Desktop Central Server is started. If you wish to automatically detect and save the IP Address, select the**Automatically detect and save the IP Address change** option. **You can also enter the DNS name of the Server.**
    - **Enable Secured Communication** - Select this option, if the communication between the Agent and the Desktop Central Server should be secured (HTTPS)
    - **Enable Checksum Validation** - Select this option, to verify if the patch/software binaries that are downloaded from Desktop Central server are verified for integrity using "Checksum Validataion (md5 algorithm)". If the checksum fails, then the installation will be aborted.
    - **Restrict Users from Uninstalling Agents from Control Panel** - Selecting this option will ensure that users do not uninstall the Desktop Central Agents from their computer.
    - **Restricting Users from Stopping Desktop Central Agent service -** Choosing this option will restrict the users from manually stopping the Desktop Central agent service. However, administrator can stop the Desktop Central agent service by following the steps mentioned below:
        - Click Tools on Desktop Central server
        - Choose System Manager
        - Select the computer, on which you wanted to stop the service and click Manage
        - Select the service "**ManageEngine Desktop Central - Agent**", under Services tab
        - Under Actions, click stop to stop the service.
    - **Perform Patch Scanning** - Select this option if Patch Scanning has to be initiated immediately after the agent installation. If this option is not selected, Patch

    Scanning will only happen when it is scheduled or when On Demand scanning is initiated.
    - **Perform Inventory Scanning** - Select this option if Inventory Scanning has to be initiated immediately after the agent installation. If this option is not selected, Inventory Scanning will only happen when it is scheduled or when On Demand scanning is initiated.
    - **Enable Firewall Settings** - Desktop Central requires the Windows Firewall running in the client computers to be configured for using all its features. Select this option to configure the firewall for enabling Remote Administration, DCOM, File and Printer Sharing, and Simple File Sharing in Windows XP.
    - **Enable Wake On LAN Settings** Select this option to enable wake on LAN feature in client computers to turn the computer on before deploying important configurations.
- Click **Save Changes**.

Agent Tray Icon Settings

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

- Initiate Patch Scanning
- Initiate Inventory Scanning
- Pull and apply configurations that are available to them
- Self-Service Portal
- Launch ServiceDesk Plus
- Send requests to Help Desk for specific needs.
- When User Logon Reports is enabled, the user will be able to view his/her login history.

Follow the steps below to configure the Tray icon settings:

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

Configuring Mail Server

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

- Navigate to **Admin** tab -> **Server settings -> Mail server settings**.
- Specify the name and port of the mail server.
- Provide the name of the sender, along with the sender's mail address and a test mail address.
- **Email Type :** Indicates whether the connection to mail server will be encrypted or will not be encrypted. (For example: SMTP, SMTPS).
- **TLS Enabled :** Option to enable Transport Layer Security (TLS).
- If it requires authentication, select the Requires Authentication check box and specify the user name and password.
- Click **Save** to save the mail server settings.

Configuring Server Settings

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

To configure server settings

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

- Click on the check box to enable the below listed features:
  - Select the "**Start 'Desktop Central' automatically on machine bootup**" check box if you wish to start Desktop Central whenever the system is started.
  - Select the "**Launch the client upon successful server startup**" check box if you wish to open the client whenever the Desktop Central Server is started.
  - Select the "**Send Desktop Central Usage Statistics**" check box if you wish to allow Desktop Central to collect and share information about the usage of the product. This will used as a feedback to enhance the product.
  - Select the "**Share Commercial Software details to the community**" check box if you wish to update Desktop Central the list of software that you have marked as commercial.
  - Select the "**Automatically mark software as commercial with shared community details**" check box if you wish to share the commercial software details to the Desktop Central Community.
  - Select the "Enable Secure Login (Https)" option to enable https in the client.
  - Select the "**Trim Column Values in Report**" check box if you wish to trim the unwanted space in the column values of report.
  - **Data Sharing :** Enabling this will allow users to see tasks/configurations that are created by all users. If this is disabled, user will be able to see only the tasks/configurations that are created by themselves.
- Specify the **Notification server port number**
- From the Drop down select the current level for **Log Settings** as normal and debug.
- Click the **Save Changes** button.

Migrating Desktop Central Server

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

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

Refer migration document for detailed steps on migrating a Desktop Central server installation from one computer to another without losing any data.

How to secure communication of mobile/roaming users using Secure Gateway Server?

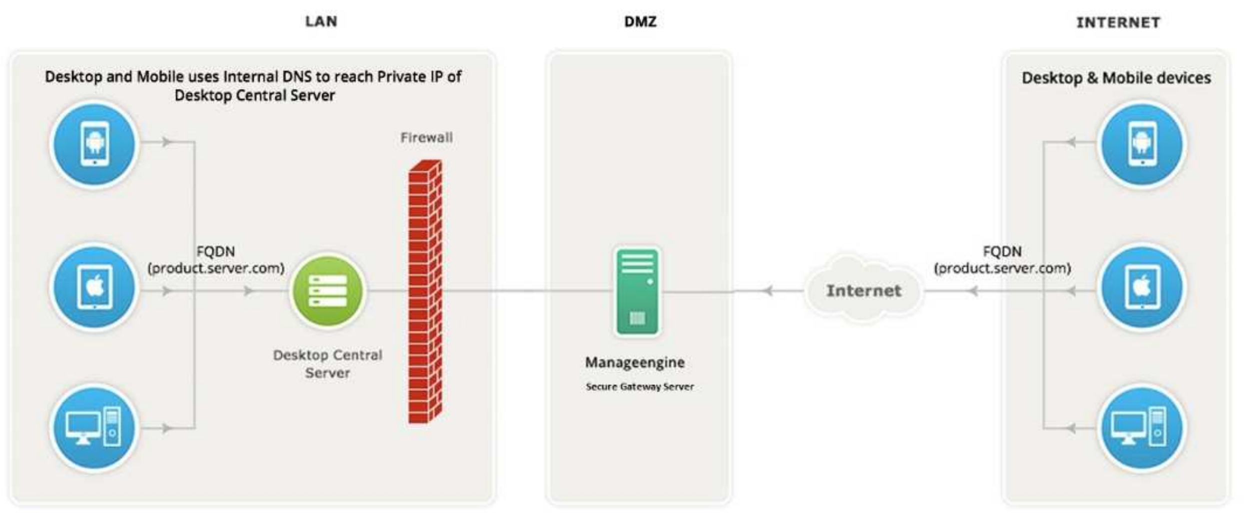
Description

This document will explain you the steps involved in securing the communication of roaming users using Secure Gateway Server component. Secure Gateway Server can be used when roaming agents (on the mobile devices and desktops) access the server through internet. It prevents the exposure of Desktop Central Server directly to the internet by serving as an intermediate server between the Desktop Central server and roaming agents. This ensures that the Desktop Central Server is secure from risks and threats of vulnerable attacks.

How Secure Gateway Server works?

Desktop Central Secure Gateway Server is a component that will be exposed to the internet. This Secure Gateway Server acts as an intermediate server between the managed roaming agents and the Desktop Central server. All communications from the roaming agents will be navigated through the Secure Gateway Server. When the agent tries to contact the Desktop Central server, Secure Gateway Server receives all the communications and redirects to the Desktop Central Server.

Secure Communication using Secure Gateway Server



Note: Map your Secure Gateway Server's public IP adress and Desktop Central server's private IP address to a common FQDN in your respective DNS. For example, if your FQDN is "product.server.com", map this to both your Secure Gateway Server and Desktop Central server IP address. By this mapping, the WAN agents of roaming users will access Desktop Central server via Secure Gateway Server (using internet) and the agents within the LAN network will directly reach Desktop Central server, hence leading to quicker resolution.

Hardware requirements for secure gateway server

The hardware requirements for secure gateway server include the following :

Processor : Intel Core i5(4 core/8 thread) 2.3 GHz. 6 MB cache
RAM size : 4 GB

Steps

To introduce Secure Gateway Server based communication to Desktop Central, follow the steps given below:

- Modify Desktop Central Settings
- Install and configure Secure Gateway
- Copy the certificates
- Infrastructure recommendations

Modify Desktop Central Settings

- Enter Secure Gateway Server IP address instead of Desktop Central server IP address under Desktop Central server details while adding remote office. This is to ensure the WAN agents and DS communication to Secure Gateway Server.
- Enable secured communication(HTTPS) under DS/WAN agent to Desktop central server communication.
- Configure NAT settings using the Secure Gateway Server's public FQDN/IP address.

Install and configure Secure Gateway Server

- Download and install Secure Gateway Server on a machine in Demilitarized zone.
- Enter the following details under **Setting up the Secure Gateway Server** window, which will open after the installation process.
  - DC Server Name: Specify the FQDN/DNS/IP address of the DC server
  - DC Http Port: Specify the port number that the Secure Gateway Server uses to contact the DC server (eg: 8020)
  - DC Https Port: Specify the port number that the mobile devices use to contact the DC server (eg: 8383 - it is recommended to use the same port 8383(HTTPS) for Desktop Central Server in secured mode)
  - DC Notification Server port: 8027 (to perform on-demand operations), this will be pre-filled automatically
  - Web Socket Port : 8443(HTTPS), this will be pre-filled automatically.

Copy the certificates

If the build number is below 90056 and if you are using self signed certificate, follow the steps given below. For build 90056 and above, this is done automatically.

- Copy the **server.crt** and **server.key** files located in Desktop Central Server under ManageEngine\DesktopCentral_Server\apache\conf directory, to the location where Secure Gateway Server is installed - ManageEngine\MEForwardingServer\nginx\conf

If you are using third party certificate, follow the steps given below:

- Rename the third party certificate as **server.crt**
- Rename the private key as **server.key**
- If you are using an intermediate certificate, modify the file name as **intermediate.crt**

- Copy the **server.crt**, **server.key** and **intermediate.crt** files to the location where Secure Gateway Server is installed - ManageEngine\MEForwardingServer\nginx\conf\
- Navigate to ManageEngine\MEForwardingServer\conf\websetting.conf file and add the line: intermediate.certificate=intermediate.crt

After copying the certificates, click install to complete the installation process.

Infrastructure recommendations

Ensure that you follow the steps given below

- Configure Secure Gateway Server in such a way, that it should be reachable via public IP/FQDN address configured in NAT settings. You can also configure the Edge Device/Router in such a way that all the request that are sent to the Public IP/FQDN address gets redirected to the Desktop Central Secure Gateway Server.
- It is mandatory to use HTTPS communication
- You will have to ensure that the following port is open on the firewall for the WAN agents to communicate the Desktop Central Secure Gateway Server.

Port	**Type**	**Purpose**	**Connection**
8383	HTTPS	For communication between the WAN agent/Distribution Server and the Desktop Central server using Desktop Central Secure Gateway Server.	Inbound to Server
8027	TCP	To perform on-demand operations	Inbound to Server
8443	HTTPS	Web socket port used for remote control, chat, system manager etc.	Inbound to Server

You have now secured communication between Desktop central server, WAN agents and roaming users.

Securing Communication using 3rd Party Certificates

Every Enterprise has the necessity to encrypt the data which traverses the internet. Using secured communication has not proved to be the most secure way to transmit corporate data, so enterprises have gone a step ahead to get specific third party certificates like SSL, PFX etc. These third party certificates ensures that the corporate data is encrypted in such a way, that only the recipient who owns the certificate can decrypt it. Desktop Central supports using SSL and PFX certificates. Adding these certificates to Desktop Central will secure the communication between the Desktop Central server, managed computers and mobile devices.

ⓘ This certificate is valid for a specified term. If the certificate expires, then the communication between the Desktop Central agent and the server will no longer be secure. **You will not be able to manage any mobile devices, till you renew the certificates and upload it in the Desktop Central server.**

Follow the steps mentioned below to create/renew and upload 3rd Party Certificates:

1. Create CSR and Key Files
2. Submit the CSR to a Certificate Authority (CA) to Obtain a CA Signed Certificate
3. Upload the 3rd party Certificates to Desktop Central

1. Create CSR and Key Files

To create CSR and Key files, follow the steps mentioned below:

- Open a command prompt and change directory to <Desktop_Central_Home>/apache/bin
- Execute following command:
  openssl req -new -newkey rsa:2048 -nodes -sha256 -out server.csr -keyout server.key -config ..\conf\openssl.cnf
- Once prompted, enter the information required to generate a CSR. A sample key generation section is as follows:

```
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....++++++
......++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN. There are quite
a few fields, but you can leave some blank. For some fields there will be a default value, If
you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: IN
State or Province Name (full name) [Some-State]: tamilnadu
Locality Name (eg, city) []: chennai
Organization Name (eg, company) []: manageengine
Organizational Unit Name (eg, section) []: desktopcentral
Common Name (eg, YOUR name) []: symphony.yourdomain.com. This should be the
same as you use to connect to the client. For example, if you use FQDN
(https://symphony.yourdomain.com) to access this computer via browser, you should
specify it the same way here as symphony.yourdomain.com.
Email Address []: Leave as empty
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []: Leave as empty
An optional company name []: Leave as empty
```

This operation creates a Key file named **server.key** and CSR file named as **server.csr** in the current working directory **Desktop_Central_Home>/apache/bin**.

2.Submit the CSR to a Certificate Authority (CA) to Obtain a CA Signed Certificate

- Submit created **server.csr** to CAs. Check their documentation / website for details on submitting CSRs and this will involve a cost to be paid to the CA
- This process usually takes a few days time and you will be returned your signed SSL certificate and the CA's chain/intermediate certificate as .cer files
- Save these files and rename your signed SSL certificate file to **server.crt**

3.Upload the 3rd party Certificates to Desktop Central

- Click **Admin** tab on Desktop Central console
- Under **Security Settings**, click **Import SSL Certificates**

- Browse to upload the certificate that you have received from the vendor (CA). The certificate will be **.crt** format for SSL and in **.pfx** format for PFX certificates
    - If you upload a .crt file, then you will be prompted to upload the server.key file. After uploading the sever.key, you will be prompted to upload the intermediate certificate. If you choose **Automatic,** then the intermediate certificate will be detected automatically. However when the intermediate certificate is detected automatically , only one certificate will be detected. If you wanted to use your own intermediate certificate, or upload more than one intermediate certificate, then you need to choose **Manual,** and upload them manually.
    - If you choose to upload a .pfx file, then you will be prompted to enter the password provided by the vendor.
- Click Save to import the certificate.

You have successfully imported the third party certificates to Desktop Central server. These certificates will be used only when "HTTPS" mode is enabled for communication. Click **Admin** tab and choose **Server Settings**, to enable **Https** mode under **General Settings**. You can now see that the communication between the Desktop Central Server and the agents is secure.

ⓘ Ensure that the pfx file or .cert file should match the NAT address specified in the Desktop Central server. If Desktop Central and ServiceDesk Plus server are installed in the same computer, then the same pfx file will work. In the above listed case, if ServiceDesk Plus server is moved to a different computer, then the pfx needs to be modified to specify the appropriate host name.

Configuring Remote Access to the Database in Desktop Central

Desktop Central stores all the information in a database. For example, it comprises information pertaining to IT assets such as hardware and software details, configuration details, etc.

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

The database located in Desktop Central server can be accessed remotely. However, not everyone has permission to access the database. Only administrators can grant/revoke access to computers to connect to the database remotely.

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

Granting Access

This section is applicable only to administrators.

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

- Navigate to the **Admin** tab.
- Under **Database Settings**, click on **Remote DB Access.**
- Select **Grant Access** and enter the **Remote Computer name** to which you want to grant access.

When you grant access, it is highly recommended that you check the usage status periodically and revoke the access to the database from users who:

- Are not required to access the database
- Have access to the database but are not using it

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

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

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

- Navigate to the **Admin** tab.
- Under **Database Settings**, click on **Remote DB Access.**
- The list of computers that have been granted access would be displayed. Under **Actions column** , select **Revoke Access** to revoke the access granted to that particular computer.

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

Connecting Remotely to the Database

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

Checking for Computers With Access

To view the list of the computers which have been granted access, follow the steps given below:

- Navigate to the **Admin** tab
- Under **Database Settings**, click on **Remote DB Access**
- You can now see the list of computers that have been granted access.

Details Required to Connect Remotely

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

- PGSQL Host Address: The host address will be the same as that of the computer where the Desktop Central server is installed and running.
- Username: This refers to the username that you are required to enter for connecting remotely to the database. The username for connecting to the PGSQL database is **medc**.

Password for PGSQL database : Enter **medc** as the password. This default password needs to be changed before granting or revoking access for computer(s).

- Port for : This refers to the port number that is required to connect to the database. PGSQL port details - This refers to the port number that is required to connect to the database. By default, the port number is **8028**.
- Database(s): This refers to the name of the database that you want to connect to remotely. You should enter **desktopcentral** in this field.

Data Back up and Restore

Desktop Central stores information like configuration details, status of deployed configurations, and details about reports, like User Logon reports and Active Directory reports, in a database. Creating a backup of this database and certain important files like configuration files is necessary to prevent loss of data.

You can back up data automatically, by scheduling a back up using Desktop Central, or taking a back up manually. You can also restore this data when required. For example, assume that your hard disk crashes and you have to re-install Desktop Central. You can use the last back up you took to restore all the required information. Note that this is possible only if the backup file is stored in a computer other than yours.

Best Practices for Back up and restore

These are the few best practices recommended for Back Up and Restore option.

- Make sure that you add the exclusion list for Anti Virus. When directories containing the MySQL / PGSQL data are scanned by anti virus software, they misidentify the files content as spam and does not allow to back up that data. Refer the following links which will guide you, how to exclude the Anti Virus.
  McAffe : https://kc.mcafee.com/corporate/index?page=content&id=KB50998
  Symantec :
  http://www.symantec.com/business/support/index?page=content&id=TECH99955
  Kaspersky : http://support.kaspersky.com/us/faq/?qid=208284276
- It is always recommended to Schedule the back up during non-office hours.
- Make sure that you have a minimum of 5GB space to store the back up data.
- Make sure that you specify a Valid destination folder.
- Make sure that the remote database if configured, should be running during back up.

Scheduling Data Backup

You can use Desktop Central to take a back up of the database regularly. For example, if you want to take a back up of the database every Friday at 5 p.m., you can schedule the same using Desktop Central.

To schedule back up of data, follow the steps given below:

1. Select the **Admin** tab
2. Under **Database settings** click **Database Backup**
3. Specify the time at which you want the back up to be taken, in hour:minute:second (hh:mm:ss) format

The time should be specified in the 24-hour format. For example, if you want the database back up to be taken at 6 p.m., the time should be specified as 18:00:00.

- Select the number of backup files that you want Desktop Central to save

Using this option you can select how many database backup files should be saved. The older backup files will be deleted. For example, if you want only 7 backup files saved, select 7. This will ensure that at all times only 7 backup files are saved.

- Specify the location where you want the backup files to be stored
- Check the **Notify when the database backup fails** checkbox
- Specify the email address (es) to which you want an e-mail message sent, if the database back up failslease note that you should have configured your mail server settings to get notified.

Ensure that you have configured your mail server settings to receive notifications.

- Click **Save Changes**

You have scheduled an automatic data backup to take place automatically at a specified time.

Manual Data Backup and Restore

You can manually back up and restore the database. You can do this using the Backup-Restore Utility GUI.

Opening the Backup-Restore Utility Graphical User Interface (GUI)

To open the Backup-Restore Utility GUI, follow the steps given below:

- Right click **start -->Explore --> directory where DC server folder is present -->bin**
- For example, right click **start -->Explore -->Local Disk (C:) -->Program Files -->DesktopCentral_Server -->bin**

- Double-click backuprestore.bat

You've opened the Backup-Restore Utility GUI.

Creating a backup file

- On the Backup-Restore Utility GUI, click the **Backup** tab
- Select the location where you want to save the backup file

If you're using a network share, the directory should have write permission for everyone in the network.

- Click **Backup**
- You can choose to encrypt the backup file by providing a password.

A backup file is created and saved in the specified location. The file will be named using the buildnumber-date-time.zip format. For example, 70120-Oct-25-2010-13-26.zip where 70120 is the build number, Oct 25th 2010 is the date and 13:26 is the time.

Restoring a backup file

Ensure that you have shut down the Desktop Central server before restoring a backup file.

- On the Backup-Restore Utility GUI, click the **Restore** tab
- Browse and select the required backup file.
- Click **Restore**
- In case you have opted for encrypting the backup file, you will have to provide the password for restoring the backup.

The build number of the Desktop Central server should match the build number of the backup file you are restoring. Ensure that you choose the correct architecture of the Desktop Central installation, such as 32-bit or 64-bit. You can verify the details by viewing the Support tab, on the Desktop Central web console.

- This will restore the specified data to Desktop Central server.

If remote database is configured with the Desktop Central server, ensure that it is running on a remote machine. After restoration, changes made after the backup date will not be available.

Feature-specific Settings

Here's the list of settings that are feature-specific :

- *Patch Management*
    - Proxy settings
    - Configuring System Health Policy
    - Approval Settings
    - Patch Database Settings
    - Patch cleanup Settings
- *Software Deployment*
    - Proxy settings
    - Self Service Portal settings
- *Asset Management*
    - Scan settings
    - Configure E-mail alerts
- *Configurations*
    - Configuration settings
- *Tools*
    - Port settings
    - System Manager settings
- *Reports*
    - Active Directory report settings
    - Report settings
- *Integrations*
    - Help desk settings

Value-added Settings

When the below-mentioned settings are configured, the whole process of endpoint management steps up -

- Rebranding
- Role-based access approach
- Two factor authentication
- Custom groups
- Mobile app
- Automatic server maintenance
- Database optimization
- Failover server
- Secure gateway server

Rebranding Desktop Central

You can choose to rebrand Desktop Central server and agent components. This feature will allow you to use your company logo and name, instead of Desktop Central's logo and name. Rebranding the Desktop Central Server, will allow Administrators and Technicians, to view the product as their own.

Benefits of Rebranding

- Reports that are exported, will contain the rebranded logo and company name
- Alerts and messages displayed on the managed computers will contain the rebranded logo and company name
- Users on the managed computers, will understand that the desktop management activity is being performed by their IT team and will not feel insecure

Rebranding Desktop Central Server

You can rebrand the Desktop Central server component by providing a product logo and the company name. You can also choose the web link, and the copyright details which can be modified. These changes will impact the users, when they login the subsequent time. Whenever a report is being generated from Desktop Server, the details on the report will also contain the rebranded details of the company. When the Desktop Central Server is rebranded, the user will not be able to identify the product as Desktop Central, on the server UI, however the text within the product would contain the name of the product as Desktop Central. For example, the installation wizard, product name in the installation directory and messages within the product, if any where the product name is specified as Desktop Central will remain the same.

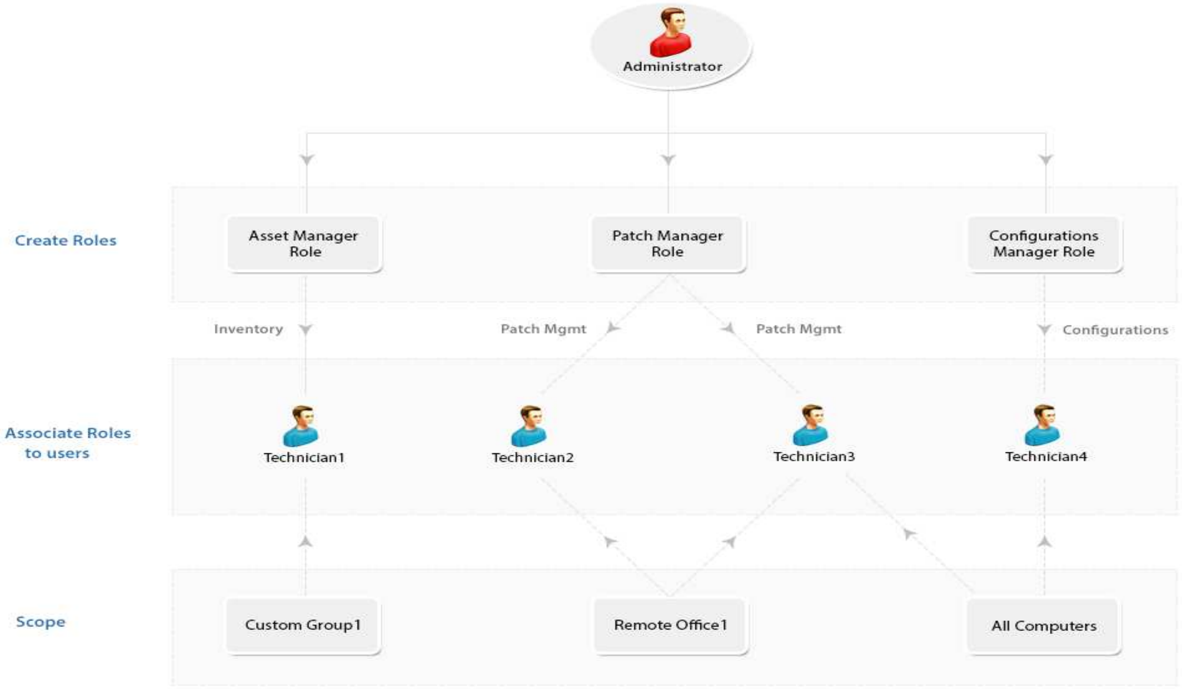
Rebranding Desktop Central Agent

You can choose to rebrand the Desktop Central agent on the managed computer. You will have to provide a logo and the name that should appear on the managed computer's agent. However unlike Desktop Central server, rebranding agent will not modify the image of the Desktop Central icon on the managed computers. Rebranded image and product name will be used while displaying notifications on the managed computer. For example, when a patch/software application is deployed via Desktop Central, user will receive a notifications on the computer where the product name will contain the rebranded company name and logo.

Role Management

Overview

As an administrator, many a time you would have felt mundane routines spill over crucial attention-seeking jobs of your network. Desktop Central answers this concern through its User & Role Management module; delegating routine activities to chosen users with well-defined permission levels. You can easily administer the users, and define their scope to manage a specific set of computers.



Role Management

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

User-defined Role

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

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

1. Select the **Admin** tab and click **User Administration, under Global Settings**. This opens the User Administration page.
2. Select the **Role** tab and click the Add Role button.
3. Specify the **Role Name** and a small description about it.
4. You can define module-wise permission level for the Role in the Select Control Section.

The permission levels are broadly classified into:
Full Control - To perform all operations like an administrator, for the specific module
Write - To perform all the operations, except few restrictions as explained below in the table
Read - To only view the details in that module
No Access - To hide the module from the User (For more details, refer to the table below)

5. Click **Add** button.

You have successfully created a new role.

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

Pre-defined Roles

You will find the following roles in the Pre-defined category:

- Administrator
- Guest
- Technician
- Auditor
- Remote Desktop Viewer
- IT Asset Manager
- Patch Manager
- Mobile Device Manager
- OS Deployer

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

- Defining or modifying Scope of Management
- Adding Inactive Users
- Changing mail server settings
- Changing proxy settings
- Personalizing options like changing themes, setting session expiry, etc.
- Scheduling vulnerability database update
- Scheduling scan settings for Patch Management
- Editing MSI or Script repository
- Viewing Actions Logs of Desktop Central
- Has write permission for the following, Inventory, Reports, Profiles and Apps in Mobile Device Management.

Guest Role: The Guest Role retains the Read Only permission to all modules. A user who is associated to the Guest Role, will have the privileges to scan and view various information about different modules, although making changes is strictly prohibited. Guest Role also has Read Only permission for viewing, MDM inventory details, reports, profiles and Apps of the mobile devices.

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

- Can define and deploy all types of configurations and collections.
- Can view all the configurations including those created by other users, reports, etc.
- Can suspend, modify, or re-deploy the configurations defined by them.
- Can update the Vulnerability Database.
- Can perform Scan operations on all modules.
- Has write permission for the following, Inventory, Reports, Profiles and Apps in Mobile Device Management.

Auditor: The Auditor role is specially crafted for Auditing Purposes. This role will help you grant permissions to auditors view the details of software inventory, check for license compliance, etc. Users with "Auditor Role" can also have read permission for MDM Reports.

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

IT Asset Manager: The IT Asset Manager has complete access to the Asset Management module and all the other features are inaccessible. IT Asset Manager can also view the Inventory details of all the Mobile Devices.

Patch Manager: The Patch Manager role has complete access to the Patch Management. Patch Manager will also have privilege to access to use "Tools", like Wake On LAN, Remote Shutdown, System Manager and ability to schedule Patch Reports. All the other modules/features are inaccessible.

Mobile Device Manager: Mobile Device Manager role has write permission for the following, Inventory, Reports, Profiles and Apps in Mobile Device Management.

OS Deployer: The OS deployer role provides the associated user the privilege to capture images of Windows OS and deploy it across the network computers.

Defining a Scope

Desktop Central provides you the privilege of defining a scope for the users, which means you can define the target computers, which can be mapped to every user. By limiting the user's permission to specific set of computers, you can feel assured that the user has enough permission to perform their roles and not excess permission to take unduly advantage.

The target that you define as the scope, can be one of the following:

- All Computers
- Unique Custom Groups
- Remote Office

All Computers

When the target is defined as 'All Computers', user will have permission to execute all the privileges defined in the role, to all the computers. Though the scope is all computers, the permission level is determined only by the role, to which the user is mapped.

Static Unique Groups

You can create specific custom groups for the management purposes and associate it to the users. The custom groups that you create should be Unique, so that no computers can belong to more than one custom group. These are computer based custom groups, which are created for the user management purpose, is defined as "scope" for the user. Refer to this to know more about Creating Custom Groups

Remote Office

You can create specific remote offices or use the existing remote offices to be defined as the scope for the users. More than one user can have manage the same remote offices. Similarly more than one remote office can be mapped to the same user, however you cannot have a combination of remote offices and unique groups as a part of the scope.

Sharing a Scope

More than one user can share the same scope. In such cases, configurations/tasks applied to the scope can be managed by more than one user. To know more, refer to this: Points to be noted

Modifying a Scope

When a scope of the user is modified, user will not be able to manage the configurations/tasks, which were created by him. He will have permission to clone the configurations without the target, so that he can re-use them for his current scope. Modifying the computers within the scope will not be considered as modifying the scope.

3.User Management

Creating a User and Associating a Role

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

- Login to **Desktop Central** client as an **Administrator**
- Click **User Management** link available under the **Global Settings category**
- Specify the Authentication Type as **Active Directory Authentication** or **Local Authentication**
- Specify a **User Name, Password and Confirm the password**
- Specify the **Role,** from the drop down. You can see find all the pre-defined roles, and the roles that you have created will be listed here
- Specify the **Email address** and the **Phone number** of the user, this is optional
- Define the **Scope** for the user, you can specify the computers, which needs to be managed by the user. You can choose to provide the user access to manage all computers, remote offices or specific unique custom groups. If you do not have a unique custom group, you can create one. If the custom group is not unique, it will not be listed here. Refer to this, to know more about : Unique Custom groups

You have successfully create a user and associated a role to the user with the scope of the computers that need to be managed.

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

Modifying User details

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

Deleting a User

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

Enabling Two Factor Authentication

Enabling Two Factor Authentication will secure the access to Desktop Central web console. Users will be prompted to enter the One Time Password (OTP) along with their default password. You can configure the settings to save the OTP for the specific browser. If this option is enabled, user will not be prompted for OTP for the number of days, specified here : Admin -> User Administration -> Two Factor Authentication. You can choose the mode for two factor authentication, which could be via email or Google Authenticator.

Email

One Time password will be sent to the each user via email. You can not enable Two Factor Authentication, if one or more users do not have email address mapped with Desktop Central server. You will have to ensure that email address of all the users are registered in Desktop Central server.

When two factor authentication is enabled, users will receive an email with the details of the OTP. Every OTP is valid for 15 minutes from the time of generation. OTP will be an auto-generated 6 digit number. You can also allow the users to save the OTP on their web browsers. You will have to specify the number of days allowed, for the OTP to be saved on the web browser. Users will not be prompted for OTP, if they choose to save the OTP on the browser. If you specify the number of days as 0, then users will not be allowed to save the OTP on the web browser. OTP will be generated every time the user tries to login into Desktop Central web console.

Google Authenticator

You can choose Google Authenticator, to generate OTP. You will have to install Google authenticator on your smart phone. Google authenticator can be downloaded based on the mobile device's operating system as mentioned below:

- iOS devices - App Store
- Android devices - Google Play
- Windows - Windows Store

Download and install the authenticator on the mobile device. When you can login to Desktop Central web console for the first time, a QR code will be displayed. You will have to open the Google authenticator app and scan the QR code to create an account for Desktop Central. You can see Desktop Central is now added to the Google authenticator app and OTP will be generated automatically.

You can use the OTP generated in the google authenticator as the secondary authentication and login to Desktop Central.

ℹ 1. If the user has deleted the Desktop Central account on the Google authenticator, then the user should contact the administrator to restore Two Factor Authentication using Google authenticator. Administrator can re-send the QR Code to restore the Google Authenticator from here : Admin -> User Management -> Actions (Under the appropriate user) -> Re-send QR Code.

2. If the Desktop Central administrator is not able to access Google authenticator, he/she can contact other administrators to send the QR code via e-mail. If there are no other administrators available, then follow the steps given in the document to disable two-factor authentication and then access the server.

Password Policy

You can impose the following restrictions on passwords for user accounts:

- **Minimum Password Length:** Define the minimum length a password should have.
- **Using Previous Passwords:** Specify the number of previous passwords that can't be reused.
- **Define Password Complexity:** Two options are available:-
  - **Simple:** Users will be prompted to enter a password that meets the specified password length. There are no enforcements for any characters/numbers to be used.
  - **Complex:** Users will be prompted to enter a password with minimum one

special character(! ~ @ # $ % ^ & + = _ *), upper case and lower case character.

- **Enable User Account Lockout:** You can specify the maximum number of invalid login attempts that are allowed before the account gets locked for a customizable 'Lockout duration'. Once a user account has been locked, login is possible only after the lockout duration is over.

Points to be Noted

- A Unique Custom group can be managed by more than one user.
- A same computer cannot be a part of more than one Unique Custom Group
- Only Administrators will have permission to modify the scope for users
- Scope defined for a user cannot be a combination of custom groups and remote offices, it can only be all computers or specific unique group or remote office
- When the scope of the user is modified, the user will not be notified about the changes made to his scope
- Adding or removing computers from the unique custom groups would not affect the scope of the user
- Refer to the following scenarios and behaviors:
  User A's scope : **Static Unique Group 1**
  User B's scope : **Static Unique Group 2**
  User C's scope : **Static Unique 2 and Static Unique Group 3**
  User D's scope : **Static Unique Group 1, Static Unique Group 2, Static Unique Group 3 and Static Unique Group 4**
    - User A creates and applies the configuration/task to Static Unique Group 1. This configuration will be visible to User A, and User D, since they share the same scope (Static Unique Group 1). This configuration can be modified by User A and User D. When user D modifies this configuration, the target of this configuration will list only the scope that is being shared by User A and User D.
    - User D creates a configuration and applies it to Static Unique Group 2, then this configuration can be viewed by user User B, User C and User D. All the three users will be able to manage the configuration.
    - User D creates a configuration and applies it to Static Unique Group 3, and Static Unique Group 4. In this case, User C and User D will be able to view this configuration. User C cannot make any changes to this configuration.
    - User A creates a configuration and applies it to Static Unique Group 1 and later, user A's scope is modified, then this configuration can only be viewed by him, or cloned as a new configuration without the target.

Creating Custom Groups

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

- You can have any number of custom groups to group computers and users of a specific department. You can create this once and can use these groups as targets for deploying the configurations.
- You can add or remove users/computers from groups at any point of time.
- Groups once created can be used in any number of configurations.
- Creating Unique Custom groups, will leverage user management by defining specific scope (unique Custom Groups) to specific users.

This document will explain you on the three types of custom groups, they are:

- Static Custom Group
- Static Unique Group
- Dynamic Custom Group

The following links will help you in creation of custom groups:

- Create a Custom Group
- List View
- Ignore Prefix
- Add Computers Manually

Static Custom Group

You can define a static group, when you have a definite set of users/computers to be added to this group. If you want to add or remove users/computers in this group, it has to be done manually. A computer can be a part of more than one static custom group. These groups are created as target, for deploying configurations.

Static Unique Group

A Static unique group is a static group, where the computers belonging to this group cannot be added to any other groups. Computers added to a Static Unique group once, will not be listed, when you try to create another group of the same kind. The main purpose of the creating a Static unique group is to associate these groups as Scope for the users. All the privileges to manage this group can be defined only by the administrator.

ℹ You can also import a csv file to add computers to a static or static unique group. The csv should contain the name of the computer followed by the domain name as explained below:

Computer Name,Domain Name
system101,companyorg

Dynamic Custom Group

A Dynamic Group is the one that is created with a set of rules or criteria. Based on the defined criteria, the computers gets automatically added to this group. Any new computer matching the criteria will automatically get added to this group. The computers belonging to this group are generated only during the execution configuration. The defined queries will be applied and the result will be published as the Dynamic Custom Group.

Create a Custom Group

To create a custom group, follow the steps below:

- Select the **Admin** tab
- Click the **Custom Groups** link available under the Global Settings. This will list all the Custom Groups that have been created.
- Click the **Create New Group** button and specify the following values:
  - Specify a name for the custom group. This should be unique.
  - Select the Domain or the Workgroup from the list.
  - Select the **Group Type** as Computers or Users. This will list the available computers/users in the selected domain.
  - **Note**: By default, the users/computers will be displayed in Tree View. Use List View link to view users/computers as a list. Manual entry of computers/users is possible using Manual Input option.

    - Select the computers/users and move them to the Added list.

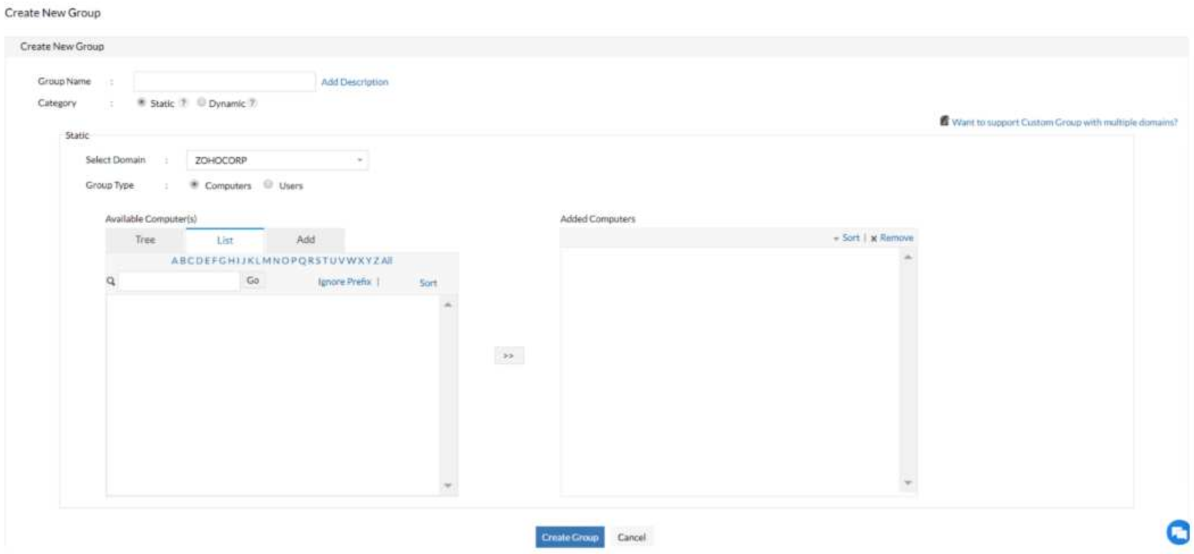
- Click **Submit** to create the group.
- Repeat steps 3 & 4 to create more custom groups.

List View

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

Ignore Prefix

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



Create New Group

Create New Group

Group Name :

Category : ● Static ○ Dynamic

Static

Select Domain : ZOHOCORP

Group Type : ● Computers ○ Users

Add Computers Manually

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

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

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

You have successfully created a custom group, which can be used for management purposes.

Configuring Mobile App

You can now access Desktop Central on the go, by using an app exclusively designed for iOS devices. Desktop Central app is supported from build #91110 and later versions. You can manage computers running Windows, Mac and Linux operating system. You can download the mobile app from the app store. This app is supported for iphone and ipad. After downloading and installing the mobile app, you will have to provide the following information:

Server Name : Specify the Desktop Central server name or IP. This should be reachable from devices outside the enterprise.

Port : 8020 (Specify the port number that you have used)

Mode : HTTP/HTTPS

Two Factor authentication is currently not supported on the mobile app. After providing the above mentioned details, you will be prompted to enter the user name and password. SoM and Inventory are the features currently supported on the mobile app. You can now start performing the below mentioned desktop management activities:

- Scan computers
- Fetch Hardware and Software details
- Add or remove computers from SoM
- Manage Prohibited Software
- Install/uninstall agents

ℹ 1. Mobile App is supported only for customers running Enterprise Edition of Desktop Central, build 91110 or later versions.

2. Two Factor authentication is currently not supported on the mobile app.

3. Access to the contents in the mobile is determined by the role and permissions for every user. For example, if a user has read only role in Desktop Central, his access using the app will remain the same.

DB Optimization

This document explains about optimizing the RAM memory consumption for PostgreSQL database. This is applicable only for customers running Desktop Central on PGSQL database. Performance of PGSQL database, is mainly determined by the amount of RAM memory consumed. Desktop Central requires a minimum of 4GB as the default RAM memory. If you have surplus RAM memory, then you can choose to customize the RAM memory consumption. Increasing the memory consumption, will allow the back end operations to be performed faster, this will impact other services/applications running on the same computer. Assume, you have 12GB as RAM memory and Desktop Central uses only 4GB by default. You can customize this settings on the Desktop Central server. You can increase the memory consumption upto 80%, which means you can increase the RAM memory consumption limit upto 9.6GB in this case. Increasing the RAM memory consumption to 80% does not mean, that the RAM memory will not be shared for any other operation. The consumption will be determined only based on the operations performed on the Desktop Central server. If the back end operations running in the server does not consume the specified memory, it can be utilized by other applications.

You can customize the memory consumption settings by clicking **Admin** tab, and choosing **DB Optimization** under **Database Settings**.

Configuring Failover Server

Downtime is a threat to every enterprise, which would affect productivity. Desktop Central offers **Failover Server**, to overcome these challenges. You can configure a secondary server, which will act as a standby server, whenever the primary server fails. This will ensure that the desktop management system is not aborted due to any hardware surprises. This document will explain the steps involved in configuring the failover server. This feature is supported for computers running Windows XP and later versions.

Prerequisites

You need to ensure that the below listed criteria are met, before configuring the failover server:

- License for Failover Server
- Remote MSSQL Database
- Remote Repositories
  - Patch Store
  - Software Repository
- Static IP Address

Failover is supported only for MSSQL databsae. You should have purchased license for failover and uploaded it in the product. You need to ensure that the database, patch store and the software repository are installed in a remote computer. This will ensure that the database, patch store and software repository are not affected, when one of the server is down. You should also ensure that the IP Address, that you configure for the primary server and the secondary server is static so that the communication will reach the appropriate static IP address.

Ensure that the Desktop Central's primary server, secondary server and the remote database (if any) belongs to a same domain and are located in a same subnet. If you have configured NAT settings to redirect all communications to a local IP, you will have to ensure that the redirected communications reach the virtual IP address.

Configuring Failover Server

You can configure failover server from Desktop Central web console -> Admin - > Failover Server. You will have to specify the Primary and Secondary Server's IP address. You will have to provide a virtual IP address, which could actually be updated to the agents. Every communication from the agent, distribution server will reach the virtual IP. If you have configured NAT settings to redirect all communications to a local IP, you will have to ensure that the redirected communications reach the virtual IP address.

All request that reaches this virtual IP will be redirected to the primary server, whenever the primary server is not reachable, the communication will be taken to the secondary server. The secondary server will periodically sync all the data from the primary server, so that it is up-to-date. You can also configure settings to receive mail notifications, whenever one of the server is down, or not reachable. Follow the steps mentioned below to configure Failover server:

1. Clone Server components to secondary server
2. Configuring Secondary Server
3. Activate Secondary Server

Clone Server components to secondary server

Perform the following steps on the computer, where (Primary) Desktop Central server is installed:

1. Stop Desktop Central server
2. Navigate to **<Installation_Directory>/ManageEngine/DesktopCentral_Server/bin**
3. Execute "Clone_Primary_Server.bat", to clone and create a zip folder which contains the server components.
4. A new zip file "Product.zip", will be created in the **"<Installation_Directory>/ManageEngine/DesktopCentral_Server>"** folder.

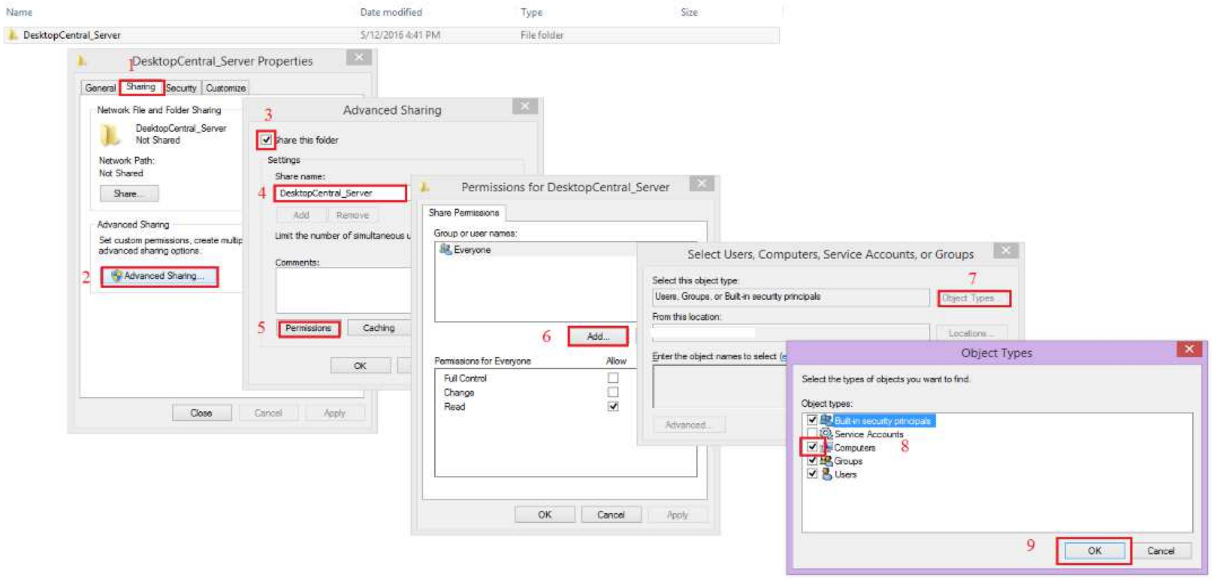
Configure Secondary Server

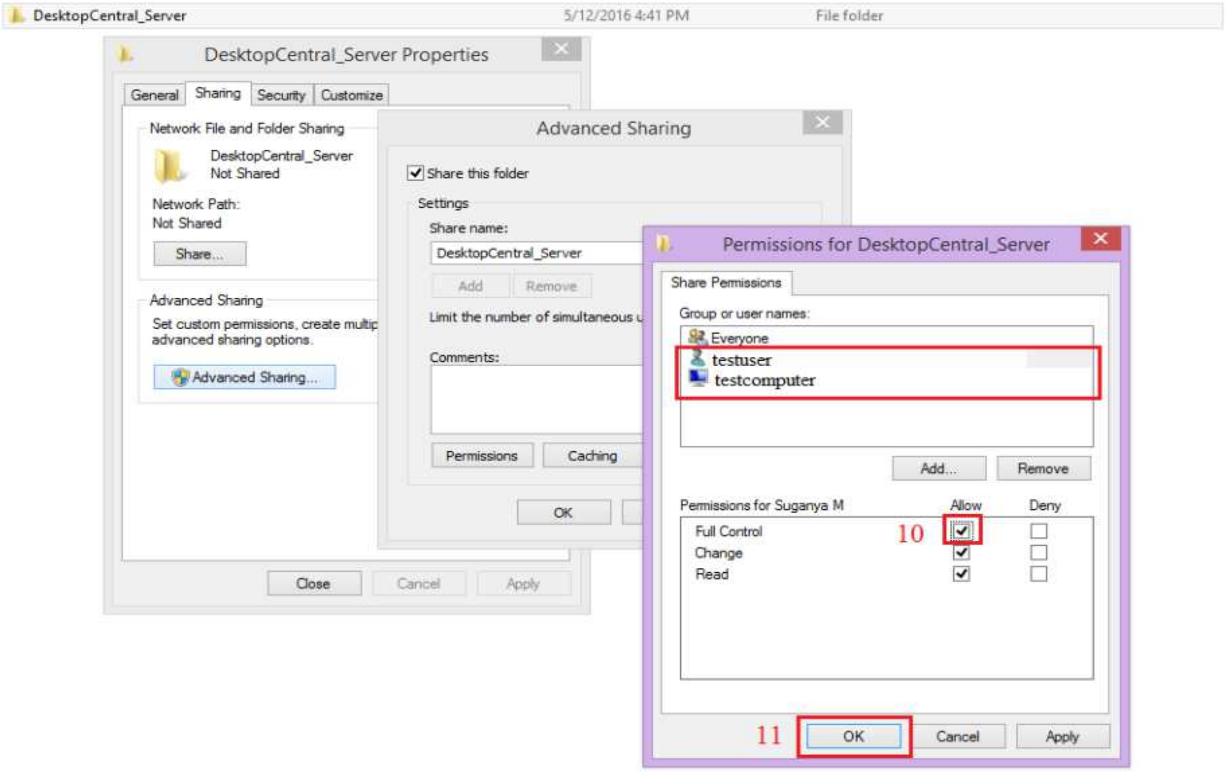
ℹ Ensure that the the secondary server do have permissions to synchronize the data from the primary server and vice versa

You will have to enable the following settings:

- **Access to computer** where Desktop Central Primary & Secondary Server are installed.
- **Permission for the admin** user to manage both the Desktop Central Primary & Secondary Server.

The below mentioned steps should be performed on the primary server first and the same should be performed on the secondary server during activation.





Steps for Sharing:

1. Right click on the folder choose **Sharing** tab
2. Click **Advanced Sharing**
3. **Enable** Share this Folder

4. Specify the name as **DesktopCentral_Server**
5. Click **Permissions**
6. Click **Add**
7. Choose **Object Types**
8. Enable **Computers,**
9. Click **OK**
10. Under Enter Object Name, specify **the secondary server name** and **the user name with Admin privileges**

11. Click share permission and select **user** and **computer** and ensure that **Full Control** is enabled

12. Click **OK**, to complete the process.

If Desktop Central server is installed in Windows 10 or Windows Server 2012 R2, you will have to ensure that the permissions are modified here, (Right click) Desktop Central folder -> Properties -> Security -> Edit Permissions -> Edit -> Add (add the name of the secondary server).

Activate Secondary Server

Perform the below mentioned step on the computer where the Secondary server is installed:

1. Download the ***Configure_Failover_Server.bat*** from the product : Desktop Central web console -> Admin -> Failover Server
2. Open Command Prompt as an administrator and navigate to the location where you have downloaded the .bat file and execute ***Configure_Failover_Server.bat <PrimaryServer_IP>***
3. Repeat the steps for sharing, as mentioned above on the secondary server and ensure that you provide name of the computer, where the primary server is installed, in step 10.

You can now see that the server components are replicated to the secondary server.

Desktop Central Features

Desktop Central offers a wide range of features for holistic endpoint management, namely -

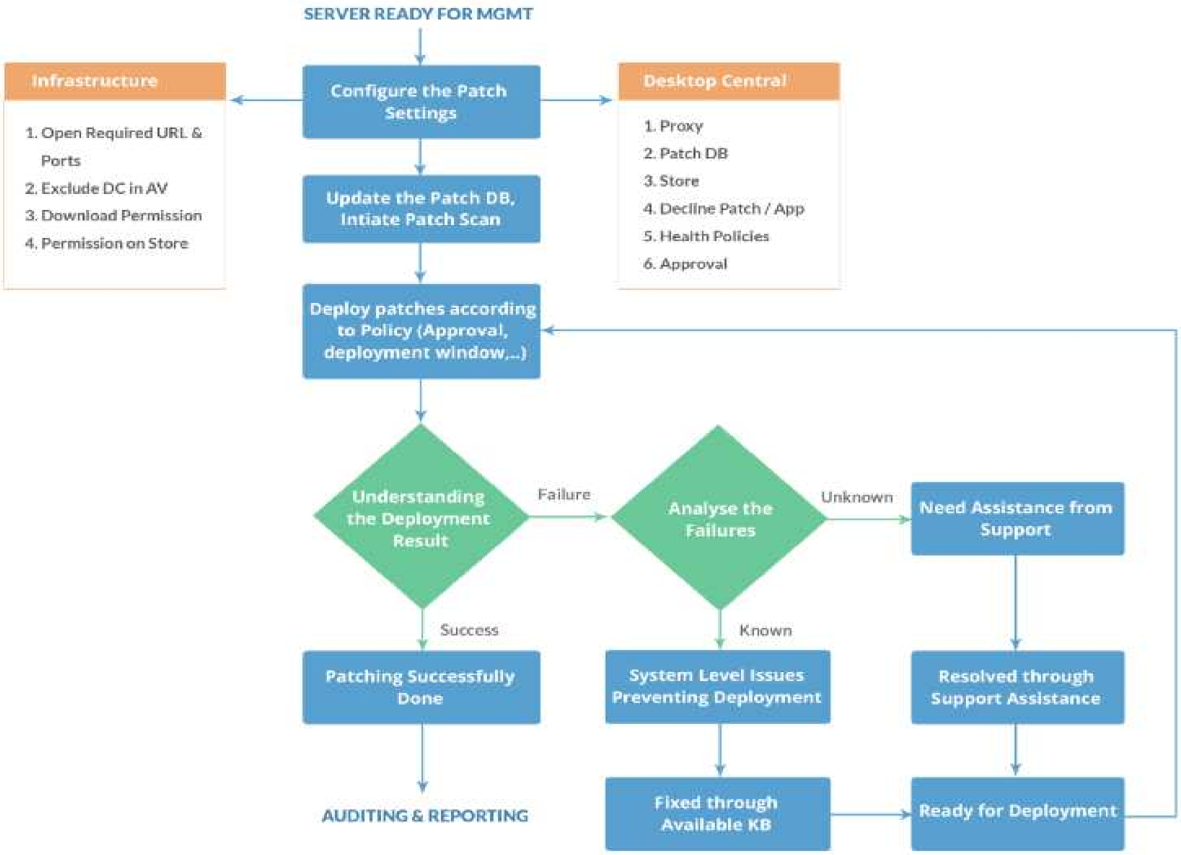
1. Patch Management
2. Software Deployment
3. IT Asset Management
4. Advanced Remote Control
5. Configurations
6. Tools
7. Reports
8. Integrations

Setting Up Patch Management

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

- Configuring Proxy Server
- Configuring Vulnerability DB Synchronization Interval
- Configuring Automated Patch Deployment
- Configuring System Health Policy
- Declining Patches for Scan
- Setting Up Patch Management in a closed network

The below mentioned workflow diagram will explain you an overview on the pre-requisites and how the patch management works. The first thing you will have to do, is to configure Proxy server, to establish connection to the internet. Internet connection is required to download the missing patches. You should also ensure, to add the required domains to the proxy's exceptional list. The second step is to configure the patch DB synchronization, so that the Desktop Central server reaches the online patch repository to update/identify the list of latest patches that are released. All the computers will be scanned to identify the missing patches. You can also configure system health policy to rate the health status of the computers. Patch deployment can be automated, you can also choose to decline patches, for specific groups. Only the approved patches will be deployed using automated patch deployment (APD). You can choose to approve patches manually or automate patch approval process.


SERVER READY FOR MGMT
Configure the Patch Settings
Infrastructure
1. Open Required URL & Ports
2. Exclude DC in AV
3. Download Permission
4. Permission on Store
Desktop Central
1. Proxy
2. Patch DB
3. Store
4. Decline Patch / App
5. Health Policies
6. Approval
Update the Patch DB, Intiate Patch Scan
Deploy patches according to Policy (Approval, deployment window,..)
Understanding the Deployment Result
Failure
Analyse the Failures
Unknown
Need Assistance from Support
Success
Known
Patching Successfully Done
System Level Issues Preventing Deployment
Resolved through Support Assistance
AUDITING & REPORTING
Fixed through Available KB
Ready for Deployment

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

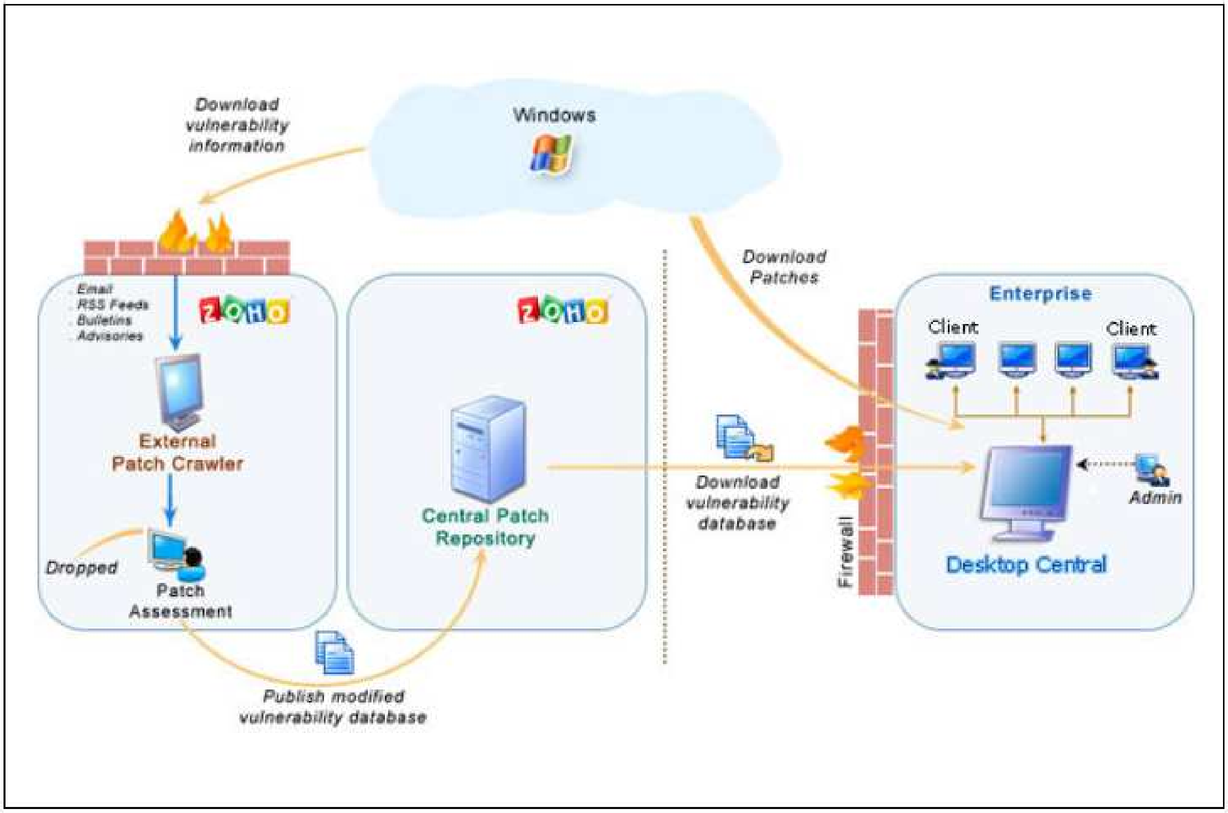


Fig: Patch Management Architecture

The *External Patch Crawler* resides at the Zoho Corp. site and repeatedly probes the internet to draw vulnerability information from the Microsoft website and Apple 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 network to assess the patch needs. Using a comprehensive database consolidated from Microsoft's and other bulletins, the scanning mechanism checks for the existence and state of the patches by performing file version checks, registry checks and checksums. The vulnerability database is periodically updated with the latest information on patches, from the Central Patch Repository. The scanning logic automatically determines which updates are needed on each client system, taking into account the operating system, application, and update dependencies.

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

Patch download and deployment

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

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

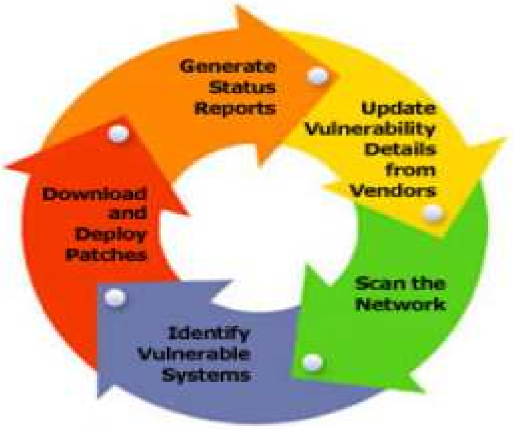

Generate Status Reports
Update Vulnerability Details from Vendors
Scan the Network
Identify Vulnerable Systems
Download and Deploy Patches

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.

Configuring Proxy Server

Desktop Central requires connection to reach the internet in order to perform the following operations:

- Synchronize Latest Patch Details
- Automatically Fetch Computers Warranty
- Manage Mobile Devices

Desktop Central periodically updates the vulnerability database with that of the Central Patch Repository that resides at Zoho Corp.'s site. Desktop Central uses this configuration to connect to the internet to update the vulnerability database. Internet connection is required to fetch the warranty details of the computers that are managed using Desktop Central. If you wanted to manage mobile devices, then you will have to configure proxy to allow connections reaching the internet. You can choose to configure proxy using one of the methods mentioned below:

- Direct Connection to Internet
- HTTP Proxy Configuration
- No connection to the Internet
- Configure Automatically using Script

Direct Connection to Internet

- Click the **Admin** tab to invoke the **Admin** page.
- Under **Patch Settings,** click **Proxy Settings** link. This opens the Proxy Settings page.
- Select the "Direct Connection to the Internet" option and click OK

HTTP Proxy Configuration

- Click the **Admin** tab to invoke the **Admin** page.
- Under **Patch Settings,** click **Proxy Settings** link. This opens the Proxy Settings page.
- Select the "Manual Proxy Configurations" option and specify the Proxy host, port, user name and password of the HTTP Proxy.
- Click OK to save the configuration.

No Connection to Internet

You can choose this option, if your Desktop Central Server does not have connection to internet or the server is located in a closed network like DMZ. By Choosing this option, you can download the missing patches manually using a special tool exclusively designed for patch management. Refer this document to learn more about Patch Management for Closed Network.

Configure Automatically using Script

Using this option, you can automate the proxy configuration using a script. All the required specifications, can be customized in a script and the Proxy PAC URL can be specified. You will have to provide the authentication details for configuring the proxy.

> Ensure that you add the following to the exception list while you configure the Proxy.

Configuring Patch Database Settings

Desktop Central's Patch repository is updated periodically, with the details of the latest patches that are released by Microsoft, Apple, Linux and other 3rd party vendors. Every enterprise has a Patch Database, in order to perform patch management activities using Desktop Central. Enterprises sync their Patch Database with the Desktop Central Patch Repository to ensure that their database is up-to-date. All the machines are scanned for the missing patches, only based on the Patch Database. Configuring the Patch Database Settings, refers to the time interval during which the Patch Database will sync the patch details from the Desktop Central's Patch Repository.

Administrators can choose to use patch management for patching a specific type of Patch like, OS related patches or third party patches etc. Though there could be a lot of patches released frequently, not every enterprise will have a need to update all those patches to all the computers. So, Administrators use the "Decline Patch" feature. Administrators can also choose to scan only the specific type of patches like OS related patches or 3rd party patches. All the computers will be scanned to identify the missing patches, based on the selection. For example administrators can choose to install only patches related to Mac operating system and 3rd party patches related to windows operating system. Then computers will be scanned to identify the missing patches related to "Mac, Linux and 3rd party patches related to windows operating system".

To configure the Patch Database settings, follow the steps below:

- Click the **Admin** tab to invoke the **Admin** page.
- Click the **Patch Settings -> Patch Database Settings** icon
- Select the type of Patches that you wish to manage, like Microsoft, Apple or 3rd Party Patches. If you wanted to update only Microsoft patches or 3rd party patches for Windows Operating System, you can specify it here. This provides you the feasibility to customize Patch Management, based on your requirement. You select only Microsoft Patches, however the patch database will get all the updates from the Desktop Central's Patch Repository. All the computers will be scanned and only the missing patches related to Microsoft will be listed.
- The "**Enable Scheduled Vulnerability Update**" will be selected by default. To disable scheduler, clear this option.
- You need to specify the time for the patch database to be synchronized. This will happen everyday.
- If you wish a mail to be sent upon successful update, select the **Notify when Task Finishes** check box and provide the email address. You can specify multiple email addresses as comma separated values.
- Click **Save Changes** to save the configuration.

Note: It is recommended to schedule the Vulnerability Settings on daily basis. This would ensure that the Patch Database is up-to-date and secure from threats and vulnerabilities.

Configuring System Health Policy

What is System Health Policy?

Desktop Central periodically scans the systems in your network to identify the missing patches. The missing patches include both the operating system and third party application patches pertaining to that system. Generally, patches are released with varying severities ranging from Low to Critical. Based on these patch severities, Desktop Central classifies the system into three categories to quickly identify the health status of the systems in the network. Health policy of the systems are calculated based on the missing security updates and third party updates. It is recommended to deploy all the security and third party updates to maintain the health status of the systems. If you do not want a specific missing patch, to impact the system health status, then you can choose to decline the patch. Patches that are declined will not be considered for the System Health Status calculation.

How are the systems classified?

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

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

The patches that are declined will not be considered for arriving at the system health status.
You can choose to exclude all 3rd party patches from system health calculation.

Customizing Patch Severity

You can customize the criteria to determine the health of a system. You can specify the number of patches, which will be considered as a bench mark to rate a system as highly vulnerable or vulnerable. Refer to the example explained below:

Criteria specified to mark a computer a highly vulnerable:

- 3 or more critical patches are missing
- 3 or more important patches missing
- 0 Moderate Patches are missing
- 0 Low severity patches are missing.

Criteria specified to mark a computer a vulnerable:

- 2 or more critical patches are missing
- 1 or more important patches missing
- 1 Moderate Patches are missing
- 0 Low severity patches are missing.

Based on the above mentioned criteria, if 3 or more critical patches are missing, then a system will be marked as highly vulnerable. If only 2 critical patches are missing, then it will be marked as vulnerable. If 1 critical patch is missing system will be considered as healthy. Assume 5 moderate severity patches are missing, then the system will be marked as Vulnerable. If 10 low severity patches are missing, system will still be considered as healthy, since you have not specified any number in the criteria.

You can configure the above explained settings by following the steps mentioned below:

1. Select the **Admin** tab and choose **Patch Mgmt**.
2. Click the **System Health Policy** link available under **Patch Settings**.
3. Specify the number of missing patches to determine the health status of a system, based on severity and count of missing patches
4. Under Advanced Settings, choose to exclude 3rd party patches from system health calculation
5. Click **Save Changes**.

Excluding 3rd Party Patches from System Heath Calculation

Most of the times, significance of missing 3rd party patches do not precede over the patches related to operating system. This could be because of the vast number of 3rd party applications and its real need towards the business. If you consider that your system's health should not be determined based on the missing 3rd party patches. You can configure your system health in such a way, that even if one or more 3rd party patches are missing in your system, it can still be rated as healthy if all OS related patches are installed on it. You can exclude all the 3rd party patches and choose to include few of those which might be needed.

> ℹ You can choose to calculate the system's health, only based on the approved missing patches. This can be specified only if you have chosen to approve patches manually. If patch approval settings is configured as automatic, then all the patches will be approved by default and considered for system health calculation.

Configuring Automated Patch Deployment

With the steady rise in attack vendors and frequency of attacks, it is mandatory to keep all your enterprise endpoints up to date and round the clock patched. The best way to address this problem, is to have a systematic and automated solution that manages multiple OSs and third party application patches effectively. Desktop Central's Automate Patch Deployment (APD) feature provides system administrators the ability to deploy patches missing in their network computers automatically, without any manual intervention required.The Automate Patch Deployment option is available under Patch Management -> Deployment.

Enhancements in Automate Patch Deployment:

Enhancements to the Automate Patch Deployment (APD) have been made to ensure there are no delays in the detection and deployment of patches to the computers missing them in your network.

Follow the steps to create and configure an Automate Patch Deployment task:

1. Automate patch deployment if you are using Desktop Central build version 10.0.192 and above.
2. Automate patch deployment if you are using a Desktop Central build version below 10.0.192.
3. If you want to migrate APD tasks from old workflow to the new workflow (enhanced Automate Patch Deployment available from build version 10.0.192 onwards).

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:

Applicable and Missing Patches Views

- Navigate to Patch Management tab -> Patches -> Applicable and Missing Patches Views
- 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.

Latest and All Supported Patches Views

Navigate to Patch Management tab -> Patches -> Latest and All Supported Patches Views and select the required patches and click the **Install Patches** button, opens the Installing Patches Configuration with the selected patches added. You can then select the targets and deploy the patches.

All Managed, Vulnerable, and Highly Vulnerable Systems Views

1. Navigate to Patch Management tab -> Systems -> All Managed, Vulnerable, and Highly Vulnerable Systems Views
2. Click **Missing Patches** link to view the missing patches of that system.
3. 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.

Install Patches Configuration

Navigate to Patch Management tab -> Deployment -> Manaual Deployment to select the Install

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

⇧ Top

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

You can view the complete details of the patches that are applicable for your network, patches that are missing in your network and patches that are installed in your network. You can also view the status of the computers in your network based on the system health policy. A system is said to be healthy when it has all the critical patches installed in it. Systems are rated to be vulnerable and highy vulnerable based on the missing patches. . You can also generate reports based on specific criteria.

Desktop Central's Patch management views are broadly classified into the following:

- All Patches View
    - Viewing Applicable Patches
    - Viewing Missing patches
    - Viewing Installed Patches
    - Supported Patches
    - Latest Patches
  - Downloaded Patches
- All Systems View
    - Highly Vulnerable Systems
    - Vulnerable Systems
    - Healthy Systems

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 Applicable Patches, follow the steps mentioned below:

1. Click the **Patch Mgmt** tab
2. Under Views Select **All Patches**
3. Click **Applicable Patches**.

You can view the details of the patches that are applicable for your network. Applicable patches are further listed under specific views like patch view, computer view and detailed view. You can also generate reports by selecting specific options from the pre-defined filters provided. You can filter the patch by Application, service pack, bulletin, patch type, approval status, download time, release time etc.,

The details of the applicable patches shown includes the following:

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

installed. This also includes the systems where the patch has already been installed.

- **Installed Systems**: Refers to the count of the systems where the patch has been installed.
- **Missing Systems**: Refers to the count of the systems that do not have the patches installed yet.
- **Failed Systems**: Refers to the number of systems on which the patch deployment has failed. Clicking the count will list the details of the failed computers, from where you can redeploy.
- **Platform**: Refers to the platform of the Operating System like Windows or Mac.
- **Vendor**: Refers to the vendor of the Operating System like Microsoft or Apple.
- **Reboot**: Refers if the patch requires a reboot or not.
- **Patch Uninstallation**: Refers if uninstallation is supported for the patch or not.

Installing Patches

You can install the patches by selecting the patches to be installed and by clicking the **Install Patches** button. Administrators can view the missing p[atches based on the Windows or MaC operating system. So that clicking on the patches will open the Installing Patches Configuration, with the selected patches added. Select the targets and deploy the configuration.

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

Note: You can choose to uninstall the patch, by selecting the patches and clicking the **Uninstall Patch** button. Uninstallation will be done only if Desktop Central supports uninstallation of the specific patches.

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.

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 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 Missing Patches, follow the steps mentioned below:

1. Click the **Patch Mgmt** tab
2. Under Views Select **All Patches**
3. Click **Missing Patches**.

You can view the details of the patches that are missing in your network. Missing patches are further listed under specific views like patch view, computer view and detailed view. You can also generate reports by selecting specific options from the pre-defined filters provided. You can filter the patch by Application, service pack, bulletin, patch type, approval status, download time, release time etc.,

The severity of the missing patches are depicted in a graph. The details of the missing patches shown includes the following:

1. **Patch ID**: A unique reference ID in Desktop Central for every patch
2. **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
3. **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.
4. **Patch Description**: A brief description about the patch.
5. **Patch Type**: Refers to whether this patch applies to Microsoft OS/Applications or Non-Microsoft Applications like Adobe, Java, etc.
6. **Severity**: Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information.
7. **Approve Status**: This refers to whether the patch has been approved for bulk deployment via Automated Patch Deployment. This is significant only if you have enabled Patch Approval prior to buld deployment. You can also approve or decline a patch by selecting the appropriate option from the "Mark As" menu.
8. **Release Date**: Refers to the date of release of the patch by the vendor.
9. **Download Status**: Refers to the status of the patch download on the Desktop Central Server.
10. **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.

11. **Installed Systems**: Refers to the count of the systems where the patch has been installed.
12. **Missing Systems**: Refers to the count of the systems that do not have the patches installed yet.
13. **Failed Systems**: Refers to the number of systems on which the patch deployment has failed. Clicking the count will list the details of the failed computers, from where you can redeploy.
14. **Platform :** Refers to the Operating System used by the computers. You can choose to filter the patch management based on the Operating System such as Windows and Mac.
15. **Vendor :** Refers to the vendor of the software applications.
16. **Reboot :** Refers whether rebooting is required or not after installation of patches.

Installing Patches

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

This will open the Installing Patches Configuration, with the selected patches added. Select the targets and deploy the configuration. The selected patches will be applied only to the target computers with the corresponding operating system. If the selected patches were applicable for Windows Operating System, then the patches will be distributed only to computers using Windows Operating System and vice versa.

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

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

Viewing Installed Patches

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

To view the list of Installed Patches, follow the steps mentioned below:

1. Click the **Patch Mgmt** tab
2. Under Views Select **All Patches**
3. Click **Installed Patches**.

You can view the details of the patches that are installed in your network. Installed patches are further listed under specific views like patch view, computer view and detailed view. You can also generate reports by selecting specific options from the pre-defined filters provided. You can filter the patch by Application, service pack, bulletin, patch type, approval status, download time, release time etc.,

The severity of the installed patches are depicted in a graph. The details of the missing patches shown includes the following:

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

- **Platform**: Refers to the platform of the Operating System like Windows or Mac.
- **Vendor**: Refers to the vendor of the Operating System like Microsoft or Apple.
- **Reboot**: Refers if the patch requires a reboot or not.
- **Patch Uninstallation**: Refers if uninstallation is supported for the patch or not.

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. The target will be listed based on the selected patches, if the selected patches were applicable for windows operating system, then the target will be computers using Windows operating system.

Note: You can choose to uninstall the patch, by selecting the patches and clicking the **Uninstall Patch** button. Uninstallation will be done only if Desktop Central supports uninstallation of the specific patches.

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

All Supported Patches

The Managed Systems view provides the details of all the patches released by Microsoft Corporation, Apple and third party vendors that are supported by Desktop Central.

To view the details on Supported Patches, follow the steps mentioned below:

1. Click the **Patch Mgmt** tab
2. Under Views Select **All Systems**
3. Click **Managed Systems**.

You can view the details of the all the patches that are applicable for your network which are supported by Desktop Central. You can also see the patches that are missing on those systems and deploy them, you can invoke to restart or shutdown the system from the same view. You can also generate reports by selecting specific options from the pre-defined filters provided. You can filter the system details based on computer name, domain name, remote office, custom group, OS, Service Pack, last scan time, last boot time etc,.

The following details are shown:

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

- **Superceded By**: Indicates that the patch is outdated and have another patch that is more recently released and has taken its place.
- **Platform**: Refers to the platform of the Operating System like Windows or Mac.
- **Vendor**: Refers to the vendor of the Operating System like Microsoft or Apple.
- **Reboot**: Refers if the patch requires a reboot or not.
- **Patch Uninstallation**: Refers if uninstallation is supported for the patch or not.

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 Latest Patches

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

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

The following details of the patches are displayed:

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

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. The selected patches will be applied only to the target computers with the corresponding operating system. If the selected patches were applicable for Windows Operating System, then the patches will be distributed only to computers using Windows Operating System and vice versa.

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 Downloaded Patches

This document will explain you about the following:

- Configuring Patch Download Settings
- Configuring Patch Cleanup Policy

The Downloaded Patches view provides the details of the patches that are downloaded by Desktop Central, along with their Deployment Status.

To view the list of the downloaded patches, click the **Downloaded Patches** link under the **Patch Mgmt** tab. You can filter the view based on the Language(s) that are present in your network.

You can export the Downloaded Patches details in PDF and CSV file formats..

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

- **Patch ID**: A unique reference ID in Desktop Central for every patch
- **Bulletin ID**: A Unique ID, that represents the Patch as per the update
- **Patch Description:** A short description on the Patch
- **Language**: This gives you information about the language in which the patch got downloaded, say English, Japanese, etc.
- **Size (in KB)**: Refers to the size of the Downloaded Patches.
- **Download Status**: The Download Status attribute displays whether the patch download was successful or not.
- **Approve Status:** Status of the Patch, as Approved or Declined for deployment purposes
- **Superseded By:** Latest version of the patch that has been released, which Supersedes the previous versions of the patch
- **Download Time:** Time, when the Patch has been downloaded
- **Remarks:** Remarks/ comments can be specified about the patch
- **Platform:** Specifies the Operating System of the Patch
- **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.
- **Release Date:** Date, when the patch has been released

Configuring Patch Download Settings

Administrators can configure a specific limit of space for Patch Repository. When the Patch

Repository size exceeds the specified limit, a mail notification will be sent to the administrators if required. This provides them a feasibility to verify that the Patch Repository does not run out of free disk space. If a Patch Repository runs out of free space, then the latest patches cannot be downloaded. However, the space limit specified above is used only for notification purposes. Assume, if you have configured the Repository size as 10 GB, where as the available free space in the same drive is 40 GB, then the patch downloads will not be affected even if the size exceeds the specified limit of 10 GB.

In case the existing patch store has limited space available, you can modify the location details using the **Change Patch Store Location** option available on the top right corner of the **Downloaded Patches** page. You should copy the patches from the previous directory to this new location and restart Desktop Central Server for the changes to take effect. The steps to restart the Desktop Central Server are as follows:

1. Go to **Start** menu --> **Control Panel** --> **Administrative Tools.**
2. Click on **Services**..
3. Right-click **ManageEngine Desktop Central 8 Service**, and then click **Restart**.

Configuring Patch Cleanup Settings

Administrators can configure patch cleanup settings to increase the free disk space on the Patch Repository. There are two significant ways to increase the free disk space, they are explained below:

- Removing Superseded Patches
- Removing Patches older than a specific time period

Removing Superseded Patches

Using "Cleanup Settings", you can remove superseded Patches. When a new version of a patch has been released, the older version of the patch is no longer required in the network. So these patches can be removed as and when a latest version is supported. You can automate this process of removing the superseded patches by configuring the cleanup policy. This will result in increasing you free disk space, by removing unwanted patches.

Removing Patches older than a specific time period

Patches once downloaded, are retained in your patch repository. Administrators needs to periodically check for the patches which are not missing on any of the computers and which are old enough to be removed. Though it is a time consuming process, you can remove a lot of unwanted patches and increase your disk space. Desktop Central has now automated this process of removing patches which are older than a specific period of time. You can specify a time interval, after which the patches will be removed if it is not missing in any of the managed computers.

You can follow the steps mentioned below to configure Patch Cleanup Policy:

1. Click **Patch Mgmt** tab
2. Choose **Download Settings** under **Views**
3. Configure cleanup policy.

You have successfully configured the patch cleanup policy. Superseded patches and patches that are older than the specified time limit will be removed from the patch repository, which means the available free disk space in the Desktop Central server will be increased. These changes will also impact the Distribution Server. Distribution server synchronizes the patch details with the Desktop Central server in such a way, that when a patch is removed from the Desktop Central server, it will also be removed from the Distribution Server during the subsequent replication interval. So whenever the patch repository is cleaned up, the unwanted patches will also be removed from the Distribution Server.

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 Healthy Systems

Healthy systems are those that have all the security patches installed.

To view the details on Healthy Systems, follow the steps mentioned below:

1. Click the **Patch Mgmt** tab
2. Under Views Select **All Systems**
3. Click **Healthy Systems**.

You can view the details of the systems that are healthy in your network. You can also see the patches that are missing on those systems and deploy them, you can invoke to restart or shutdown the system from the same view. You can also generate reports by selecting specific options from the pre-defined filters provided. You can filter the system details based on computer name, domain name, remote office, custom group, OS, Service Pack, last scan time, last boot time etc,.

The following details about the healthy systems are shown here:

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

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

Viewing Vulnerable Systems

Vulnerable systems are those that do not have one or more Moderate/Low rated patches installed.

To view the details on Vulnerable Systems, follow the steps mentioned below:

1. Click the **Patch Mgmt** tab
2. Under Views Select **All Systems**
3. Click **Vulnerable Systems**.

You can view the details of the all the systems that are vulnerable in network. You can also see the patches that are missing on those systems and deploy them, you can invoke to restart or shutdown the system from the same view. You can also generate reports by selecting specific options from the pre-defined filters provided. You can filter the system details based on computer name, domain name, remote office, custom group, OS, Service Pack, last scan time, last boot time etc,.

The following details about the vulnerable systems are shown here:

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

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

Viewing Highly Vulnerable Systems

Highly Vulnerable systems are those that do not have one or more Critical/Important rated patches installed.

To view the details on Highly Vulnerable Systems, follow the steps mentioned below:

1. Click the **Patch Mgmt** tab
2. Under Views Select **All Systems**
3. Click **Highly Vulnerable Systems**.

You can view the details of the all the highly vulnerable in your network. You can also see the patches that are missing on those systems and deploy them, you can invoke to restart or shutdown the system from the same view. You can also generate reports by selecting specific options from the pre-defined filters provided. You can filter the system details based on computer name, domain name, remote office, custom group, OS, Service Pack, last scan time, last boot time etc,.

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

Patch Approval Settings

Desktop Central allows you to automate patch deployment process, from identifying the missing patches, to deploying them to the required computers. There might be cases where you would like to test a critical patch in few computers before rolling it out to the entire network. Desktop Central allows you to create test groups to test those patches before approving them. This feature is available only for customer running Desktop Central build # 92092 and later versions and Enterprise Edition.

If you are using Desktop Central professional edition or build # lower than 92092, follow these steps.

For Enterprise Edition and build # 92092 & later versions

Patch approval process can be performed from, **Desktop Central web console -> Patch Mgmt -> Deployment -> Test and approve settings.** You can choose one of the below mentioned mode:

- ○ Automatically approve all patches
- ○ Test and approve patches
    - Manually approve tested patches
    - Approve tested patches automatically
    - Change "automatic approval" to "test & approve"
    - Change "test & approve" to "automatic approval"

Automatically approve all patches

All the patches will be approved automatically, which means all the approved patches will be deployed using Automated Patch Deployment. If you want to ignore deploying a specific patch, then you will have to decline the patch manually.

Test and approve patches

This feature allows you to create test groups to test the patches before approving them. You will have to create test groups for each platform separately. It is recommended to create a test group, which contains all the major versions of the OSs, so that the testing could be effective. Once the patches are successfully deployed to the test groups, then you can choose to approve them either manually or automate the approval process. If the patch deployment has failed, then the patches will not be approved. When a patch is not approved, those patches will not be deployed using Automated Patch Deployment tasks. You can either deploy them manually or approve it, for the deployment to happen.

Manually approve tested patches

After testing the patches, you can choose to approve the tested patches manually. You can click the test group to view the details on the patches which are successfully tested and are waiting for approval, those patches will be marked as "Not Approved". You will have to choose them manually and approve it, if the deployment need to be automated. If they are not approved, then you will have to deploy them manually.

Approve tested patches automatically

Once the patches are successfully deployed to the test group, you can configure a time interval for the patches to be approved. This will allow you to identify the stability of the patches once they are deployed. Assume a patch is tested successfully and it has no adverse effects for 7 days after deployment, then you can choose to approve those patches. When those patches are approved, they become available for Automated Patch Task and are deployed to the complete network. This time delay for approval is completely optional and provides you an extra buffer time before approving the patches.

Change "automatic approval" to "test and approve"

If you change the approval settings from automatic approval to test and approve, you will have to create a test group for testing the patches and the testing process remains the same as explained above. Once the patches are tested, you can choose to approve the patches either manually or automatically.

Change "test and approve" to "automatic approval"

All the test groups that you have created will be removed. All the patches will be approved by default.

For Professional Edition and build # lower than 92092

Desktop Central allows you to automate patch deployment from identifying the missing patches and to deploy them on to the required computers. The automation is done irrespective of the patches and applications. There might be cases where you would like to test a critical patch in few computers before rolling it out to the entire network. In such cases, you can choose to approve the patches manually. Only the patches that are approved will be deployed via Automated Patch Management. Patch Approval process can be automated or patches can be approved manually. Patch approval process can be performed from, **Desktop Central web console -> Patch Mgmt -> Settings -> Approval Settings.** This section explains you on the following:

- Automatic Patch Approval process
- Manual Patch Approval process
- Change Patch Approval Settings from Automatic to Manual

        - Change Patch Approval Settings from Manual to Automatic

Automatic Patch Approval process

All the patches will be approved by default, which means all the patches will be deployed through "Automated Patch Deployment Tasks". If you want to restrict a specific patch from being deployed, then you will have to decline it manually.

Manual Patch Approval process

By enabling this option, you will have to choose the specific patch/application to be marked as Approved. Only the patches that are approved, can be deployed via Automated Patch Management. When you choose "manual approval", all the patches will be marked as "Not Approved" by default and you will have to choose to decline or approve patches.

Change Patch Approval Settings from "Automatic" to "Manual"

When the Patch Approval settings is changed from "Automatic" to Manual mode, users will be provided with the following options:

- Retain the Approval status of the Existing Patches
- Mark all the patches except "Declined Patches" as "Not Approved"

Retain the Approval status of the Existing Patches

- You can choose to retain the existing Approval status of the patches, which means the patches that are marked as "Approved" will be retained as Approved. Patches that were marked as "Declined" will be retained as "Declined". All the patches that are discovered henceforth will be marked as "Not Approved".

Mark the Existing patches as "Not Approved"

- By choosing this option, all the patches other than "Declined Patches" will be marked as "Not Approved". All the patches that are discovered henceforth will be marked as "Not Approved", you can choose to decline the patches manually.

Change Patch Approval Settings from "Manual" to "Automatic"

When the Patch Approval settings is changed from "Manual" to "Automatic" mode, all the patches except "Declined" patches will be marked as Approved. Patches that are discovered henceforth will be marked as "Approved" automatically.

Decline Patches

Overview

Declining Patch, is an important part of patch deployment. When we automate patch management, all the missing patches are downloaded and deployed to the target computers. This results in deploying patches even though, they might not be business critical. So, you will have to choose to ignore patches which are not critical. Ignoring to install some of missing patches will reflect on the system's health status. Computers in your network might be rated as highly vulnerable, or Vulnerable.

In order to avoid this, you can decline patches. Declining a patch results in the following:

- When a patch is declined, it will not be considered as missing patch
- It will not be calculated for the system health status
- Patches that are declined will not be deployed via automated patch deployment.

Declining Patches to All Computers or Specific Group

You can choose to decline specific patches or all patches pertaining to a specific application. Patches can be declined to all computers or specific group of computers. A default group named, **"All Computers Group"** is created by Desktop Central. If you wanted to decline a specific patch to all computers, then you can choose this group and decline the required patches. If you want some of the patches to be declined to a specific group of computers, then you can create separate custom groups like, groups based on OS, or Remote Office, etc. and decline the patches.

Here are few examples for of how decline patch works:

1. Assume a specific patch **"Adobe 1.1"** has been declined for a **All computers Group**, then the patch **"Adobe 1.1"**, will not be considered as missing patch and will not be downloaded in the network. Computers will not be considered as vulnerable, even if this patch is not installed.
2. If a critical Patch **"Chrome 23.1"** is declined for specific custom groups, like custom

group "**Remote_Office1 & Remote_Office2"** then the patch will be downloaded and deployed to all the missing computers, except for those computers in custom group **"Remote_Office1 & Remote_Office2"**. If this patch **"Chrome 23.1"** is missing in any computer other than the specified custom groups, then those computers might be rated as vulnerable, since a critical patch is missing.

3. When a computer is added to a custom group "**Remote_Office1",** all the patches that are declined to the custom group will be considered as declined to the newly added computer.

Follow the steps mentioned below to decline know the steps involved in declining patches and applications:

1. Click the **Patch Mgmt** tab to on the Desktop Central console
2. Click **Decline Patch** link available under **Settings**
3. Click on Select **Group and Decline Patches**
4. Select **All computers Group,** if you wanted the patch to be declined for all the managed computers, else **choose/create a specific group**which contains the required target.
5. Add **Description** if required
6. Choose patches based on **KB Number, Bulletin, Patch ID, Application or Platform**.
7. Select the **patches/application** that needs to be declined
8. Click **Save** to save the changes.

If you wanted to revoke, the declined patches then you can edit it by selecting **Actions** against the **custom group name**.

You have successfully declined patches for group. You can now see that Patches that are declined will not be reflecting the system health status or not been calculated as missing patches.

See Also: Patch Management Architecture, Patch Management Life Cycle, Scan Systems for Vulnerability, 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 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 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.
- **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 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

Setting Up Software Deployment

The Software Deployment feature in Desktop Central enables you to deploy software remotely as well as distribute software applications to users and computers in a Windows network. Here are the to-be-followed steps to reap the benefits of software deployment:

1. Creating a software package
2. Software templates
3. Software repository
4. Software installation
5. Software uninstallation
6. Self-Service Portal

Creating Software Packages

Package creation is the fundamental step in software deployment. Desktop Central enables you to store the commonly used applications which can be installed on to the client machines as required. The common applications that include MSI, EXE, APPX and MSU files are stored in the Software Repository. The software packages that are added to the repository can then be used while defining the Software Installation Configuration.

The following packages can be created using Desktop Central -

1. MSI Package
2. EXE Package

Here's how you create packages for Mac computers.

Configuring Software Repositories

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

- Network-share repository
- HTTP repository

Network-share Repository

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

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

Advantages

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

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

Required Permissions

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

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

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

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

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

Creating a Network-share Repository

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

1. Navigate to **Software Repository** from Software Deployment tab.
2. Click the **Create a Network Share** option
3. Enter the path for the network share
4. If you do not enter a path for the network share, it will automatically be created in the computer where Desktop Central server is installed.
5. Check the **Accessing the Share using Credentials** checkbox
6. Enter a username and password
7. If you are creating the network share on a domain computer, prefix the domain name to the username. For example, ZohoCorp\Administrator. If you are creating the network share on a workgroup computer, prefix the computer name to the username. For example, \DCAdmin.
8. Click **Save**

You have created a network-share repository.

HTTP Repository

An HTTP repository is used to store executable files before you install them in computers in your network. You can use this repository when you want to deploy software packages to computers using the HTTP path. You can also change the location of the HTTP repository if required.

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

Advantages

Using an HTTP repository enables you to do the following:

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

Changing the Location of the HTTP Repository

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

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

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

Network Share VS. HTTP Upload

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

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

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

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

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

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

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. The Software Installation configuration helps you to install MSI and EXE packages remotely to specific users of several computers of the Windows network from a central location.

The four steps of creating and deploying the configuration are -

1. Name the Configuration
2. Define Configuration
3. Define Targets
4. Deploy Configuration

Software Distribution Features

1. 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
2. Ability to schedule software installations
    - Install Software at a specified time
    - Install Software either during or after startup of the computer
3. Option to install the application as a specific-user using the **Run As** option.
4. Supports execution of pre-deployment/post-deployment scripts/commands prior to installation/uninstallation and abort if not successful.
5. Option to copy the installables to the client computers before installing the software.
6. Ability to create package repository. The packages created once can be reused any number of times to install or uninstall the software.

Adding MSI Packages

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

- Navigate to Software Deployment tab and click **Add Packages**.
- Select the Package type as **MSI** and specify the following details:

Parameter	**Description**
	Package
Package Name	Name of the Software Package
License Type	Specify if the software is commercial or non-commercial
Locate installable	The installable needs to located - ○ From Shared Folder : If the software has to be installed in computers in the same LAN, select this option ○ From Local Computer : If the software has to be installed in computers in branch offices over the VPN tunnel or internet, select this option
Add Files to Upload	When you choose to locate the installable from local computer, you need to browse and select the installables, which will be uploaded to the Desktop Central Server
MSI File Name with network path	● When you select to choose the installable from shared computer, specify the name of the MSI file with its complete network path. This path should have all the related files and should have necessary read & execute permissions. ● Example: \\MyServer\MSIApps\Skype\skype.msi.

MSI Properties for installation	● Specify the MSI properties for installation. ● Example: REBOOT=ReallySuppress
Disable Uninstall option in Add/Remove Programs	Select this option, if you do not want the users to remove the software from Add/Remove Programs.
Pre-Deployment Activities before Installation	
Check if Software Exists	Specify the Software Name and version, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Registry Key/Value	Specify the Header Key, Sub Key and Value Name, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Data on Registry Value	Specify the Header Key, Sub Key, Value Name, Data Type, Comparator and Register value, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check File Folder	Specify the File Name or Folder Name based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Free Disk Space	Specify the required free space and the drive, so that installation will be initiated only if there is sufficient space.
Check Running Process	Specify the Process Name, so that you can choose to proceed with the installation when the process is stopped or kill the process and proceed with the installation.
Configurations	Configurations such as Create/Append Path, Create/Delete Shortcut, Executing custom scripts, Managing Files and Folders , Configuring Registry Settings and Configuring Windows Services, Setting Environment Variables can be deployed as a pre-deployment activity.
Pre-Deployment Activities before Uninstallation	
Check if Software Exists	Specify the Software Name and version, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Registry Key/Value	Specify the Header Key, Sub Key and Value Name, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.

Check Data on Registry Value	Specify the Header Key, Sub Key, Value Name, Data Type, Comparator and Register value, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check File Folder	Specify the File Name or Folder Name based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Running Process	Specify the Process Name, so that you can choose to proceed with the installation when the process is stopped or kill the process and proceed with the installation.
Configurations	Configurations such as Create/Append Path, Create/Delete Shortcut, Executing custom scripts, Managing Files and Folders , Configuring Registry Settings and Configuring Windows Services, Setting Environment Variables can be deployed as a pre-deployment activity.
Post-Deployment Activities after Installation	
Configurations	Configurations such as Create/Append Path, Create/Delete Shortcut, Executing custom scripts, Managing Files and Folders , Configuring Registry Settings and Configuring Windows Services, Setting Environment Variables can be deployed as a post-deployment activity.
Post-Deployment Activities after Uninstallation	
Configurations	Configurations such as Create/Append Path, Create/Delete Shortcut, Executing custom scripts, Managing Files and Folders , Configuring Registry Settings and Configuring Windows Services, Setting Environment Variables can be deployed as a post-deployment activity.
Advanced Options	
MSI Root Path	When you choose to copy the installables to individual computers before installing the software, you need to specify the directory to be copied.
Architecture	Specify the Package architecture as 62 bit or 32 bit. If the software architecture is chosen as 32 bit , then it will be installed on all the computers (32 bit and 64 bit). If the software architecture chosen is 64 bit, then Desktop Central will not try to install the software on 32 bit computers.
Maximum Time Limit for Installation	Specify the time limit allowed for the installation to happen. If the time to install the software application exceeds the time limit specified here, installation process will be aborted.

Enable Logging for troubleshooting	Select this option to enhance the logging to troubleshooting the deployment errors.
Package Properties	
Manufacturer	Name of the software vendor
Version	The software version
Language	The software language version
Package Description	Description of the software package

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

Modifying MSI Packages

To modify the MSI packages, follow these steps:

1. Click **Software Deployment** tab.
2. The list of **managed packages** , will be displayed.
3. Click the **Actions** column next to corresponding package.
4. Select **Modify** to modify the package.

Removing MSI Packages

To remove the MSI packages, follow these steps:

1. Click **Software Deployment** tab.
2. The list of **managed packages** , will be displayed.
3. Click the **Actions** column next to corresponding package.
4. Select **Delete** to remove the package.

The package details will be deleted from the table.

Adding an MSIEXEC/EXE/ISS/Command Package

- Navigate to Software Deployment tab and click **Add Packages**.
- Select the Package type as **MSIEXEC /EXE/ISS/Command** and specify the following details:

Parameter	**Description**
Package	
Package Name	Name of the Software Package
License Type	Specify if the software is commercial or non-commercial
Locate installable	The installable needs to located - ○ From Shared Folder : If the software has to be installed in computers in the same LAN, select this option ○ From Local Computer : If the software has to be installed in computers in branch offices over the VPN tunnel or internet, select this option
Add Files to Upload	When you choose to locate the installable from local computer, you need to browse and select the installables, which will be uploaded to the Desktop Central Server
Installation Command with switches/arguments	Specify the command to be executed in the client computers for installing the application. The command specified here will be "as such" executed in all the client computers. Make sure that the path to the executables specified in the command is relative to the EXE Root Directory specified above. Examples: 1. msiexec.exe \Skype\skype.msi /qn 2. googlesetup.exe /S

Uninstallation Command with switches/arguments	Specify the command to be executed in the client computers for uninstalling the application. The command specified here will be "as such" executed in all the client computers. Make sure that the path to the executables specified in the command is relative to the EXE Root Directory specified above. Example:Skype\uninstall.exe If the uninstaller in the individual computers has to be invoked, you can specify the complete path to the uninstaller. please note that the uninstaller has to be in the same location in all the client computers. You can use environment variables in the path. Examples: C:\WINDOWS\ie7\spuninst\spuninst.exe /q %SystemRoot%\ie7\spuninst\spuninst.exe /q
Pre-Deployment Activities before Installation	
Check if Software Exists	Specify the Software Name and version, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Registry Key/Value	Specify the Header Key, Sub Key and Value Name, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Data on Registry Value	Specify the Header Key, Sub Key, Value Name, Data Type, Comparator and Register value, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check File Folder	Specify the File Name or Folder Name based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Running Process	Specify the Process Name, so that you can choose to proceed with the installation when the process is stopped or kill the process and proceed with the installation.
Configurations	Configurations such as Create/Append Path, Create/Delete Shortcut, Executing custom scripts, Managing Files and Folders , Configuring Registry Settings and Configuring Windows Services, Setting Environment Variables can be deployed as a pre-deployment activity.
Post-Deployment Activities after Installation	

Configurations	Configurations such as Create/Append Path, Create/Delete Shortcut, Executing custom scripts, Managing Files and Folders , Configuring Registry Settings and Configuring Windows Services, Setting Environment Variables can be deployed as a post-deployment activity.
Pre-Deployment Activities before Uninstallation	
Check if Software Exists	Specify the Software Name and version, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Registry Key/Value	Specify the Header Key, Sub Key and Value Name, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Data on Registry Value	Specify the Header Key, Sub Key, Value Name, Data Type, Comparator and Register value, based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check File Folder	Specify the File Name or Folder Name based on the search result you can choose to proceed with the installation, uninstall the existing version or skip installation.
Check Running Process	Specify the Process Name, so that you can choose to proceed with the installation when the process is stopped or kill the process and proceed with the installation.
Configurations	Configurations such as Create/Append Path, Create/Delete Shortcut, Executing custom scripts, Managing Files and Folders , Configuring Registry Settings and Configuring Windows Services, Setting Environment Variables can be deployed as a pre-deployment activity.
Post-Deployment Activities after Uninstallation	
Configurations	Configurations such as Create/Append Path, Create/Delete Shortcut, Executing custom scripts, Managing Files and Folders , Configuring Registry Settings and Configuring Windows Services, Setting Environment Variables can be deployed as a post-deployment activity.
Advanced Options	
EXE Root Path	When you select the Network Path option, specify the shared directory from where all the commands will be executed. This directory should have access to all the executables that are required to install the application.

Exit Code	Specify the exit code, which should be returned when the installation has been succeeded.
Architecture	Specify the Package architecture as 62 bit or 32 bit. If the software architecture is chosen as 32 bit , then it will be installed on all the computers (32 bit and 64 bit). If the software architecture chosen is 64 bit, then Desktop Central will not try to install the software on 32 bit computers.
Maximum Time Limit for Installation	Specify the time limit allowed for the installation to happen. If the time to install the software application exceeds the time limit specified here, installation process will be aborted.
Package Properties	
Manufacturer	Name of the software vendor
Version	The software version
Language	The software language version
Package Description	Description of the software package

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

Modifying EXE Packages

To modify the EXE packages, follow these steps:

1. Click **Software Deployment** tab.
2. The list of **managed packages** , will be displayed.
3. Click the **Actions** column next to corresponding package.
4. Select **Modify** to modify the package.

Removing EXE Packages

To remove the EXE packages, follow these steps:

1. Click **Software Deployment** tab.
2. The list of **managed packages** , will be displayed.

3. Click the **Actions** column next to corresponding package.
4. Select **Delete** to remove the package.

The package details will be deleted from the table.

Software uninstallation

The Software Uninstallation configuration helps you to uninstall MSI and EXE packages remotely from specific users of several computers of the Windows network from a central location.

The four steps of creating and deploying the configuration are -

1. Name the Configuration
2. Define Configuration
3. Define Targets
4. Deploy Configuration

Here's how MSI and EXE software can be uninstalled from computers/users:

1. Uninstallation of MSI software
2. Uninstallation of EXE software

Uninstalling MSI Software

Desktop Central provides an option to uninstall MSI software packages to users and computers of the Windows network. It provides an option to schedule the uninstallation and also the status of the uninstallation is made available. You can also re-install the applications installed using Desktop Central.

- Uninstall MSI Software from Windows Users: The software will be uninstalled from the specified users.
- Uninstall MSI Software in Windows Computers: The software will be uninstalled from all the computers.

Uninstalling MSI-based Applications for Users

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

1. Navigate to **Software Deployment -> Install/Uninstall Software Configuration -> User configuration**.
2. Provide a name and description for the configuration
3. Select the **Package**.
4. Select the **Operation Type** as **Uninstall**.
5. Specify the user account as which the software needs to be uninstalled: As a system user or any specific user.
6. If you wish to involve user interaction while uninstalling the software, enable the appropriate check box.
7. Configure the scheduler settings and choose the deployment policy.
8. Upon defining the target, click **Deploy**.

Uninstalling MSI-based Applications for Computers

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

1. Navigate to **Software Deployment -> Install/Uninstall Software Configuration -> Computer configuration**.
2. Provide a name and description for the configuration
3. Select the **Package**.
4. Select the **Operation Type** as **Uninstall**.
5. Specify the user account as which the software needs to be uninstalled: As a system user or any specific user.
6. If you wish to involve user interaction while uninstalling the software, enable the appropriate check box.
7. Configure the scheduler settings and choose the deployment policy.
8. Upon defining the target, click **Deploy**.

Uninstalling EXE Software

Desktop Central provides an option to uninstall EXE software packages to users and computers of Windows network. It provides an option to schedule the uninstallation and also the status of uninstallation is made available. You can also re-install the applications installed using Desktop Central.

- Uninstall EXE Software from Windows Users: The software will be uninstalled from specified users.
- Uninstall EXE Software from Windows Computers: The software will be uninstalled from the specified computers.

Uninstalling EXE-based Applications for Users

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

1. Navigate to **Software Deployment -> Install/Uninstall Software Configuration -> User configuration**.
2. Provide a name and description for the configuration
3. Select the **Package**.
4. Select the **Operation Type** as **Uninstall**.
5. Specify the user account as which the software needs to be uninstalled: As a system user or any specific user.
6. If you wish to involve user interaction while uninstalling the software, enable the appropriate check box.
7. Configure the scheduler settings and choose the deployment policy.
8. Upon defining the target, click **Deploy**.

Uninstalling EXE-based Applications for Computers

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

1. Navigate to **Software Deployment -> Install/Uninstall Software Configuration -> Computer configuration**.
2. Provide a name and description for the configuration
3. Select the **Package**.
4. Select the **Operation Type** as **Uninstall**.
5. Specify the user account as which the software needs to be uninstalled: As a system user or any specific user.
6. If you wish to involve user interaction while uninstalling the software, enable the appropriate check box.
7. Configure the scheduler settings and choose the deployment policy.
8. Upon defining the target, click **Deploy**.

Software Deployment Templates

What is a template?

A template is a predefined format that can be applied. Desktop Central offers over 4000 software templates that can be used to create packages automatically. This functionality downloads software binaries from the respective vendors' web sites and aid in package creation of that particular software. The benefits of creating packages using template are as follows -

1. Pre-filled fields such as installation/uninstallation commands
2. Save time by just defining the targets and the package is good to be deployed

Prerequisites

Ensure that you **define valid proxy credentials** and **provide access rights** for automating the package creation process from the Templates section of Software Deployment.

Creating a package

A package once created, can be used several times for deploying a software. This package will be stored in the software repository. You can create a single package or multiple packages from the Templates tab by following the steps given below:

1. Navigate to **Software Deployment -->Templates**.

2. Select the required application. Select multiple applications if you want to create multiple packages.
3. Click the **Create Package** button. If the package creation type is manual, click Learn More to know the steps on how to create the package manually.
4. You are required to confirm if you want to download the binaries related to the package(s) you have chosen. If you do not want to download the binaries, click **Cancel**.
5. The download process of the respective binaries will begin. The download process status will be updated once the package creation is completed.

7. Click **View packages**

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

Accessing the location of a package

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

1. Navigate to **Software Deployment -->Templates** and click on the required application.
2. In the **Application Details** window, click on the link against **Location** for accessing the location of the application.
3. Ensure that the URL of the executable link is added to the exception list in the proxy server.
4. You can now recreate the package and deploy it.
5. These links will redirect you to the location from which the package is being downloaded. The possibility of getting a download error reduces if the link is accessible. However, if you get an error while trying to access the link, then you will get an error while trying to download the required binaries, from the Desktop Central server. You should verify the functionality of the executable links for packages only from the system on which the Desktop Central server is installed. Refer our KB document for error while downloading binaries.

Autoupdate templates

Software templates can be updated automatically, meaning, every time there is a latest version of the software, the corresponding template will be updated automatically. This gives you an edge when it becomes momentous for every software to be updated to the latest version. Autoupdate Templates is applicable only for Windows and will be carried out after every successful sync, once everyday.

The perks of updating your software templates automatically are -

- Save the time and labor invested in manually updating the template to the latest version
- Packages for the latest version of the template will be created automatically
- For the packages published in Self-Service Portal, this update will automatically be reflected which implies that the latest version of the software template will be available to your end users and they can install it at their convenience. Upon launching the Self-Service Portal, a package with the latest version will be available for installation. This will replace the old package.

Steps

- Navigate to Auto-update Templates from Software Deployment tab. This will list all the software templates for which auto-update has been enabled, along with the status of the package and number of packages created using this template.
- If you want to add templates to this list, click Enable auto-update button and choose the templates.
- A package can be created automatically from this list.
- Another way of enabling auto-update for templates will be while creation of a package. From the Templates tab, choose the software for which you want to create a package. You will be asked for enabling auto-update of this template.

Creating Software Packages for Mac Computers

For every software that you wish to deploy using Desktop Central, a package should be created. The package contains the details of the software application, its installation location and the installation/uninstallation commands. The packages once created can be used to deploy software to any number of computers later. The software application, which needs to be deployed to target computers should be uploaded to a particular location. This should be accessible only via 'HTTP share'. "Network Share" is not applicable for Mac, unlike Windows. Administrators should specify the HTTP path while creating a software package.

This document will explain about various steps involved in creating a software package for computers running Mac operating system. Refer the following options, before creating a software package:

- Creating Software Package with Single File
- Creating Software Package with Multiple Files
- Using Installation Commands
- Uninstalling a Software
    - Removing Software for All Users
    - Removing Software for Specific Users
    - Removing Software for the Currently Logged-in User
    - Removing Software with Preferences

Note: Installables can be uploaded only in .dmg format. If you wanted to upload the installable, which is in **.pkg/.mpkg / .app** format or upload more than one installable, then it should be compressed and uploaded in **.zip, .tar, .gz, .bz2, .tgz, .tbz or .dmg** format.

Creating Software Package with Single File

Creating a package to install with a single installable file is very easy. Follow the steps mentioned below:

1. Navigate to **Software Deployment -> Add Packages -> Mac**.
2. Specify a **name for the Package** and provide the details of the package for your personal reference.
3. Click **Installation** tab
4. Click **Browse,** under **Upload Files** upload the installable (software application) that needs to be deployed to the target computers. The installable should be in **.pkg/.mpkg** or **.app** format.

You have successfully created a package with a single installation file.

Creating Software Package with Multiple Files

The steps to create a package with multiple files, is the same like creating a package with single installation file. some software applications like Office, would require more than one installation file, in such cases administrators can upload the installable files in **.zip, .tar, .gz, .bz2, .tgz, .tbz or .dmg** format. These files will be extracted to identify the .pkg/.mpkg or .app files. these files are the same like

Using Installation Commands

Administrators can use installation commands if they want to customize the installation or change the default installation location. If installation command is not specified, then the software application will be installed using the default installation commands. The following are examples, of how commands can be used to change the default installation location:

For pkg: ***installer -pkg "/Volumes/Wireshark/Wireshark 1.10.0 Intel 64.pkg -target "/Volumes/Drive1"***
For app: ***ditto "/Volumes/Appcleaner/appcleaner.app" "/TargetPath/appcleaner.app"***

Note: If you are uploading the installable in compressed format, then you can specify only the installable's name in the installation command.

Uninstalling a Software

A software can be removed by specifying the appropriate installed location. If there is more than one file that needs to be removed, then you can add more than one location or use a script for uninstallation. Uninstallation command can be specified under, "Advanced Options". If you write a script of your own, then it is recommended to test it, before it is added to the software package.

Note: Scripts can be uploaded in .sh (shell script), .scpt(Apple Script), .pl(Perl Script), .py(Phyton Script) formats.

Removing Software for All Users

Remove a software for all users by using the command as mentioned below: "**$allusers**/Library/Application Support/Google/Chrome"

The above is a sample command to remove "Google Chrome" for all users.

Removing Software for Specific Users

Remove a software for a specific users by using the command as mentioned below:
"/Users/user1/Library/Application Support/Google/Chrome"
The above is a sample command to remove "Google Chrome" for a specific user 'user1'.

Removing Software for the Currently Logged-in User

Remove a software for the currently logged on users by using the command as mentioned below:
$currentusers/Library/Application Support/Google/Chrome

Removing Software with Preferences

A software can be removed with its preferences. If there is more than one file that needs to be removed, then you can specify more than one location of the file/folder which needs to be removed or use a script for uninstallation. The shell script below is an example for an uninstallation script, used to remove a software application with its dependent files from multiple computers. Most vendors provide the script for uninstallation, if you write a script of your own, then it is recommended to test it before it is added to the software package.

Sample Script to Remove Office and its dependent files/folders from multiple computers

```
#!/bin/sh
osascript -e 'tell application "Microsoft Database Daemon" to quit'
rm -R '/Applications/Microsoft Communicator.app/'
rm -R '/Applications/Microsoft Messenger.app/'
rm -R '/Applications/Microsoft Office 2011/'
rm -R '/Applications/Remote Desktop Connection.app/'
rm -R '/Library/Application Support/Microsoft/'
rm -R '/Library/Automator/*Excel*'
rm -R '/Library/Automator/*Office*'
rm -R '/Library/Automator/*Outlook*'
rm -R '/Library/Automator/*PowerPoint*'
rm -R '/Library/Automator/*Word*'
rm -R '/Library/Automator/Add New Sheet to Workbooks.action'
rm -R '/Library/Automator/Create List from Data in Workbook.action'
rm -R '/Library/Automator/Create Table from Data in Workbook.action'
rm -R '/Library/Automator/Get Parent Presentations of Slides.action'
rm -R '/Library/Automator/Get Parent Workbooks.action'
rm -R '/Library/Automator/Set Document Settings.action'
rm -R '/Library/Fonts/Microsoft/'
rm -R '/Library/Internet Plug-Ins/*SharePoint*'
rm -R '/Library/LaunchDaemons/*Microsoft*'
rm -R '/Library/Preferences/*Microsoft*'
rm -R '/Library/PrivilegedHelperTools/*Microsoft*'
OFFICERECEIPTS=$(pkgutil --pkgs=com.microsoft.office*)
for ARECEIPT in $OFFICERECEIPTS
do
  pkgutil --forget $ARECEIPT
done
```

Self Service Portal

This feature is available only in the Enterprise Edition of Desktop Central.

As a part of IT administration, you will have the need to deploy various software to various users/computers. This is not only a routine task, but also consumes a lot of your time and effort. You will have to deploy multiple software configurations to the required target. Desktop Central adds another easy approach to accomplish software deployment, by introducing **Self Service Portal**. Self Service Portal allows you to publish software to the target users/computers. Unlike manual software deployment, you can publish the list of software to the group (target users/computers). You can empower the users to install software based on their needs. This helps you to save a lot of time and enhances productivity.

Self Service Portal is currently supported only for Windows and Mac (version 10.8 and above) operating systems.

Publishing Software to Self Service Portal

You will find the self service portal on the Desktop Central server by navigating to this location, **Software Deployment -> Deployment -> Self Service Portal.** You can create a Group which contains the target users/computers and publish the available software. Computer based and User based software can be published via self service portal. You will have to specify the software which needs to be published from the list of available software. When a software is published from the Desktop Central server, the same will be updated on the target computer during the subsequent 90 minutes refresh cycle. You can add/remove software which were published in the self service portal. When multiple versions of a software is being published, you can see multiple entries of the same software on the self service portal with the difference in its version. List of software on the self service portal will be synced once in every 90 minutes. User can also choose to sync it manually by clicking on "Sync Now" icon on the right corner of the Self Service Portal. When a software is successfully published for a computer/user for the first time, you will find self service portal added to the agent tray, start menu and as a desktop shortcut on the target computer.

- Removing a published software will not uninstall the software from the target computer, however the software will not be listed in the self service portal.
- When a commercial/paid software is published, users will have to key in/activate the license manually.
- User-based publishing of software packages is not supported for Mac.

Making Self Service Portal Accessible to Users

To enable users to access the Self Service Portal, follow these steps:

1. Navigate to Admin tab -> SoM Settings -> Agent Settings -> Agent Tray Icon.
2. Enable **Show Agent Icon in the System Tray**. Make sure **Show Self Service Portal Menu** is enabled.
3. Click on **Save Changes**.

Users will now be able to access Self Service Portal by right-clicking the agent tray icon in the **system tray** and selecting "Self Service Portal".

Installing Software from Self Service Portal

Users can access self service portal from any one of the following methods:

- Launching self service portal from Desktop Central agent tray
- Double clicking on the self service portal shortcut, from the user's desktop
- Choosing self service portal from the start menu

On opening the self service portal, users can see the list of software that are published. Users can choose to install any number of software from the self service portal. When they click on "Install" option, the installation will be initiated. When a user chooses to install more than one software at a time, installation will be initiated for the first software and the rest will be queued. Software will be deployed sequentially. When a software is installed from the self service portal, the software status will be marked as installed.

If the user has uninstalled the software manually, then the uninstallation status will not be reflected on the self service portal.

Self Service Portal Settings

Configuring this settings will allow you to customize the way self service portal should be displayed on the managed computers. You can configure the settings from here : **Software Deployment -> Settings -> Self Service Portal Settings.** You can specify the options, based on which self service portal will be displayed on the agent tray, desktop shortcut or start menu. You can also choose to re-brand the icon displayed on the self service portal. You can upload your organization's logo and name, so that the same will be displayed on the managed computers. Re-branding will allow the users to easily recognize that the software is distributed by their IT team and will encourage them to use it. You can also automate the publishing process by grouping the software as commercial or non commercial. You can choose to automatically publish the non commercial software to "All Computers" group. Users can choose to install the software themselves. If you are using Desktop Central integrated with ServiceDesk Plus, then you can choose to automatically publish commercial software to "All Computers" group. However users will have raise to request for approval, before installing the software.

.NET 4 should be installed on the managed computers, for self service portal to work. **.NET 4** will be automatically installed on the managed computers, you can choose to install it on the server machines by enabling the check box, under self service settings.

Request for Approval

This feature is supported only for customers who use Desktop Central (**92080**) integrated with ServiceDesk Plus (**9203**).

You can choose to publish software to all the users, however limit the users from installing software which are not essential. If you are using Desktop Central integrated with ServiceDesk Plus, then you can choose the approval mode while publishing software, as "with approval" or "without approval". If you choose to publish software using "without approval", the users will be allowed to install the software by clicking on it. If you have chosen, to publish a software with approval, then the user will not be allowed to install the software, but can raise a request for approval. A help desk ticket will created and updated in the ServiceDesk plus, once the technician approves the request, users will be allowed to install the software. After the user installs the software, the status will be updated back to ServiceDesk Plus and the help desk ticket will be closed automatically.

This feature is available only for Windows.

Setting Up Asset Management

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

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

Scan Systems for Inventory

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

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

Steps to Enable DCOM

To Enable DCOM in Windows 2000 Computers

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

To Enable DCOM in Windows XP Computers

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

Scan Systems Manually

To Scan the systems manually, follow the steps below:

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

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

Troubleshooting Tips

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

Schedule Scanning

Table of contents

Inventory Scan

Schedule system's inventory scan and track asset data periodically to get up-to-date information about the changes in the hardware and software installed across the systems you manage. You can set the frequency of scan according to your requirement. With the agent-server model of Desktop Central, any changes in the hardware or software in the managed systems would be updated immediately. Thus making your asset data more accurate and comprehensive.

To perform inventory scan go to **Inventory -> Actions/settings -> Schedule Scan -> Inventory**

Scan -> Configure Schedule

File Scan

Schedule system's file scan and get details about the various types of files present in the systems you manage. On performing this scan you can identify audios, movies, photos, office documents and outlook data files. With this scan you can view the count and memory usage of these files. Hence by tracking the details of file types you would be able to perform the following activities:

- Identify copy righted files like music and movies in the organization network
- Analyze system's hardware usage and monitor memory usage of files

To perform file type scan go to **Inventory -> Actions/settings -> Schedule Scan -> File Scan -> Configure Schedule**

ℹ File Scan can be performed only by the Inventory administrator who has access to all managed computers.

To view the details of file type scan go to **Inventory -> Computers -> Computer name -> File details**

Manage Software Licenses

Table of contents

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

- Able to get their software compliant status
- Add the details of their software purchases - both one time and additional purchases of the same software
- Should know the computers using those licenses.

- Should be able to reallocate a license, if it is not used/required, to a different resource that require them
- Help them decide on software renewals and purchases.
- Group different versions of the same software and manage their licenses as a single entity.

Add Software License Details

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

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

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

- **Software Name**: Name of the commercial software.
- **Manufacturer**: The software manufacturer (vendor)
- **Licensed To:** To whom the software is licensed.
- **Purchased**: No. of licenses purchased
- **Installed**: No. of licensed software copies that are installed in the network.

- **Purchased Date**: The date of purchase.
- **Expiry Date**: The date of expiry.
- **License Key**: The Purchase license Key details.
- **License File**: The file containing the license particulars for a particular software.
- **Invoice File**: The file containing the Purchase information for a particular software.

You can filter the view based on the compliant status of the software like Under License, Over license, in compliance and expired software.

Adding Additional Licenses

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

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

Create Software Groups

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

To create a new Software Group:

1. Navigate to **Manage Licenses** from Inventory tab.
2. Click **Group Software** to list all the software groups that have been created. Click **Add Software Group** to create a software group.
3. This opens the Add/Modify Software Groups dialog listing all the commercial software installed in your network.
4. Specify a name for this group.
5. Select the software that you wish to group and move them to the Grouped Software list. The software category and the prohibited status of the first software in the selected list will apply to all the software of that group. You can change the position of the software

in the selected list by selecting the software and clicking the arrow button on the right.

6. After selecting the required software, click **Save**.

To modify a Software Group:

1. Navigate to **Manage Licenses** from Inventory tab.
2. Click **Group Software** to list all the software groups that have been created.
3. Click the **Edit** icon from the Actions column of the group that you want to edit.
4. Add or remove the software from the group and click **Save**.

To delete a Software Group:

1. Navigate to **Manage Licenses** from Inventory tab.
2. Click **Group Software.** This will list all the software groups that have been created.
3. Click the **Delete** icon from the Actions column of the group that you want to delete.

Manage Software Category

Table of contents

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

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

To add a new software category:

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

To modify a software category:

1. Navigate to **Manage Software Category** from Inventory tab. This will list all the software categories that have been added, including the pre-defined categories. Choose to Edit from the Actions column of the category against the corresponding software that you want to edit.
2. Rename the category and/or add/remove software to/from this category and click **Update**.

To delete a software category:

1. Navigate to **Manage Software Category** from Inventory tab. This will list all the software categories that have been added, including the pre-defined categories.
2. Choose to delete from the Actions column to delete individually or select the categories that you wish to delete and click **Delete Category**.

Configure Prohibited Software

Table of contents

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

Adding prohibited software

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

1. Navigate to **Prohibit Software** from the Inventory tab. This will list the details of all the software that are already prohibited.
2. Click **Add Prohibited Software**. This will open the Add Prohibited Software dialog listing all the software detected in the managed computers. You should have scanned the Windows systems at least once to have the details of the software here.
3. Select the software that you wish to prohibit and move them to Prohibited List.
   Note: In case you have grouped certain software and you are adding that Software Group under the Prohibited Software List, then all the software in that group will be added.
4. After adding all the software, click **Update**. The software gets added to the prohibited list.

Removing prohibited software

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

Configuring the Auto-Uninstallation Policy

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

1. Select the **Auto-Uninstall Policy tab**.

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

   Note: Increasing this number will cause high CPU usage during uninstallation. If the detected prohibited software count exceeds the limit (maximum number of software to be uninstalled) in a computer, the exceeding numbers of software will be uninstalled during the subsequent startup.
4. Select **Notify User before Uninstalling** check box and specify any custom message in case you want to prompt to the user before the software uninstallation.

   Note: The user will be notified with an Alert message during logon and whenever the agent detects prohibited software. This functionality will be applicable only if the **Notify User Settings** is configured.
5. Specify the wait-window for the software uninstallation. Say if you want to remove the software three days after it has been detected, then mention 3 in the text box provided.
6. Click on **Save** to save changes.
7. Auto-Uninstallation option is available by default for **.msi** applications and for **.exe** applications & we would require silent switches. The following steps will guide you through the Auto-Uninstallation of **.exe** based software applications.

1. Select the **Prohibited SW tab** and click on **Not Configured link** under **Uninstall command** against the **.exe** application that needs to be uninstalled..
2. The **Add/Edit Uninstall Command** window pops up.
3. Choose Pre-fill Uninstall Command or I will specify myself

   Pre-fill Uninstall Command - Selecting this option will fetch the uninstall command of the application from the Add/Remove programs and will be displayed here. Only the silent switch needs to be specified.

   I will specify Myself - Uninstall command and the silent switch should be entered manually. It is recommended to test the uninstallation command manually to verify its correctness.
4. Click **Save** to save the settings**.**
5. Verify the status in **Auto Uninstallation Status Tab** (This uninstallation will happen based on Auto-Uninstall Policy configured)
6. Under **Auto Uninstallation Status** select **Detailed View** to see the status and remarks.

You can choose to uninstall a software by configuring auto uninstall policy. However, this will not prevent users from installing a software/application. Once this software is installed, it will get uninstalled automatically.

Excluding Computers from Software Uninstallation

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

1. Navigate to **Prohibit Software** from Inventory tab. This will list the details of all the software that are already prohibited.
2. Select the checkbox corresponding to the specified software and click the link under Exclusions column. This opens the **Add Exclusions** dialog.
3. Select whether to exclude custom groups or computers and select the groups/computers and move it to the **Excluded** list.
4. Click on **Save** to save changes.

Approving requests to use prohibited software

This feature is supported only for customers, who use Desktop Central version (10.0.192) or above.

1. From the agent tray icon, users can find the list of prohibited software in their network and choose to rise requests to use specific prohibited software based on their needs.
2. These requests can be handled from Desktop Central web console -> Inventory -> Prohibit Software -> User Requests.
3. **If you have integrated Desktop Central with ServiceDesk Plus (Version 9203 or above),**
   - The requests to use prohibited software can be resolved only from ServiceDesk Plus console. Know how to resolve requests in ServiceDesk Plus here.
   - To associate the requests to use prohibited software to ServiceDesk Plus templates, from Desktop Central navigate to admin tab -> under integration settings, ServiceDesk Plus -> Select the "Send requests for using Prohibited Software as tickets to ServiceDesk Plus for approval" option and provide the ServiceDesk Plus template name.
4. Once the technician approves the request, users will be allowed to install and use the requested software.

Configuring Global Exclusion

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

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

Configure E-Mail Alerts

Desktop Central generates e-mail alerts to notify the following events :

1. When a hardware is detected or removed
2. When a software is installed or uninstalled
3. When a prohibited software is installed
4. When software compliance status is under licensed or when a software is used after the license has been expired
5. When the usage of a licensed software is less than the stipulated limit
6. When a software is being used even after its license has expired
7. When the free disk space falls below the configured value : This includes the overall free disk space as well as partition-wise free space
8. When a certificate is on the verge of expiry : You can configure the time duration prior to expiry of certificates for receiving alerts.

To configure e-mail alerts, follow the steps given below:

1. Navigate to the **Inventory** tab
2. Click on **Configure E-mail Alerts** link from the left pane available under Actions /

Settings.

3. Under **Notifications** specify, when the notifications should be sent. Configure the alerts based on your requirements.
4. Specify the email address(es) to which the notifications need to be sent.
5. Click **Save**

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

Block Executable

One of the most challenging task in system administration is to restrict usage of certain applications. Desktop Central facilitates you to perform this task at ease. You will be able to block the required applications/executable using this feature. You can apply these restrictions for specific computers. Desktop Central's prohibited software helps you in detecting and uninstalling the software applications which are not allowed in the network. Block executable feature, allows you to restrict the executable when it is launched, on the target computers. You can block even executables like, notepad.exe, putty.exe etc which are launched without being installed on the target computer. All the file formats supported under Windows "Software Restriction Policy" can be blocked using Desktop Central. There are two ways to block an application/executable, they are:

- Blocking using Path Rule
- Blocking using Hash Value

The following prerequisites should be met for blocking the executable

- Local Group Policy should be enabled on the target machine
- Local Group Policy Should be enabled on the target computer

- Default security Policy should be set as "Unrestricted"
- Local Group Policy should be enabled for Administrator

Blocking using Path Rule

You can choose this option to create a policy in order to block an executable. Path Rule, is used to block an executable based on the name of the executable and its extension. If the user renames the application then the application will not be recognized, which means the application will not be blocked. This rule can be used to block applications even if they are not available in your network. All you need to know is just the name of the executable and its file extension. With the help of path rule, all the versions of the specified application can be blocked. For example, if you have created a path rule to block Google Chrome browser for a specific version, say version 44.0, this policy will block all the versions of Google Chrome browser, unless the executable is not renamed.

Blocking using Hash Value

Hash is a unique value, that represents the executable. If you choose to block an executable using the hash value, then it will be blocked even if renamed. If you want to block an executable using hash value, you should locate it on the server, for the hash value can be calculated.

Creating a Policy

If you wanted to block an executable to a specific target, then you will have to create a policy. Selecting the target computers is the first step in creating a policy. You will have to select the executable which needs to be blocked, if it exists in the database. If you wanted to block an executable for the first time, then you will have to add the executable and choose to block rule as path or hash. You can create two different policies for a single executable, one using path and the other using hash value. Policy will be applied on the target computer for the first time, after the system restart.

Blocking Executable for All the Computers

Desktop Central by default has a custom group, which contains all the managed computers. If you wanted to block an executable for all the managed computers, then you can choose "All

Managed Computers" group and select the executable, which needs to be blocked. You will have to create a policy by specifying the target and executable which needs to be blocked.

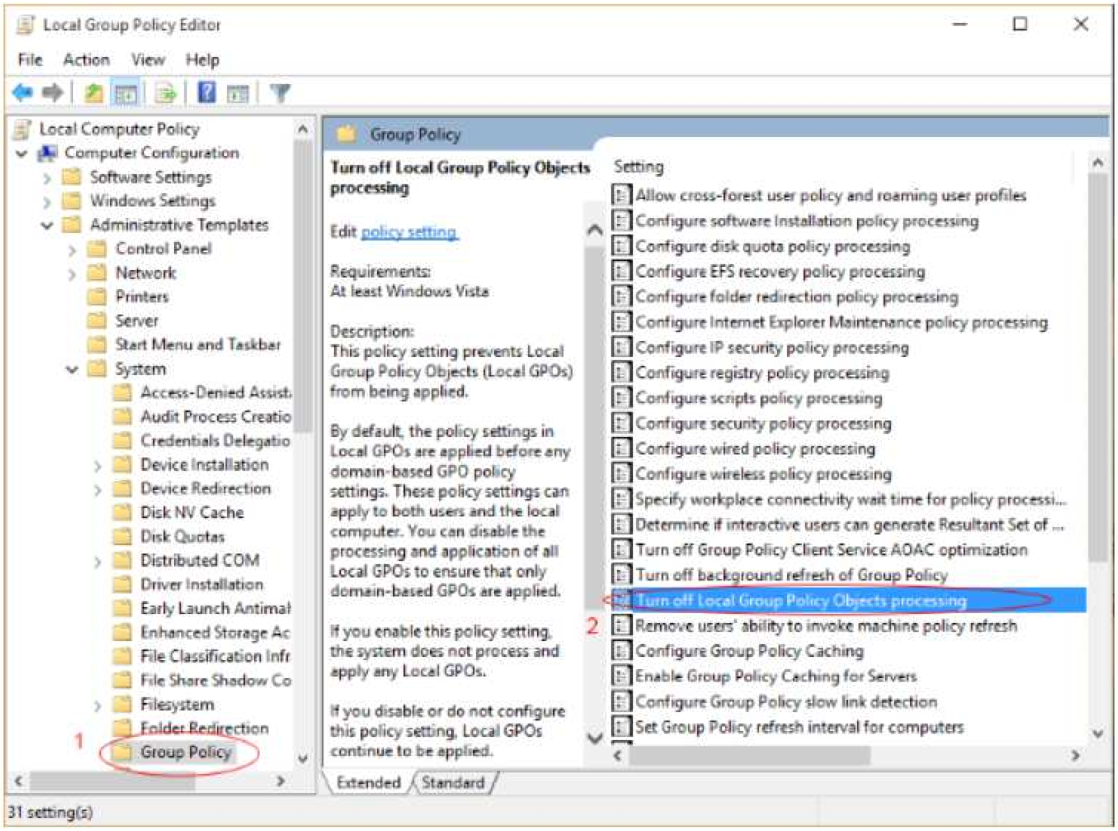
Blocking Executable for Specific Users/Computers

To block an executable for specific target, you will have to create a new custom group or use the existing custom groups. Custom groups can be of any type such as, unique or static. You can block executable by choosing custom group which contains users or computers.

"Block executable" does not support blocking executable which are initiated by the system.

Troubleshooting Tips:

1. How to enable Local Group Policy on the target machine?
   You will have to perform the following steps manually on the target computer:
   a. Go to **Run**
   b. Type **gpedit.msc**
   c. Click Group Policy
   d. Click on "**Turn Off Local Group Policy Objects Processing**" as shown below.



Group Policy

Turn off Local Group Policy Objects processing

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting prevents Local Group Policy Objects (Local GPOs) from being applied.

By default, the policy settings in Local GPOs are applied before any domain-based GPO policy settings. These policy settings can apply to both users and the local computer. You can disable the processing and application of all Local GPOs to ensure that only domain-based GPOs are applied.

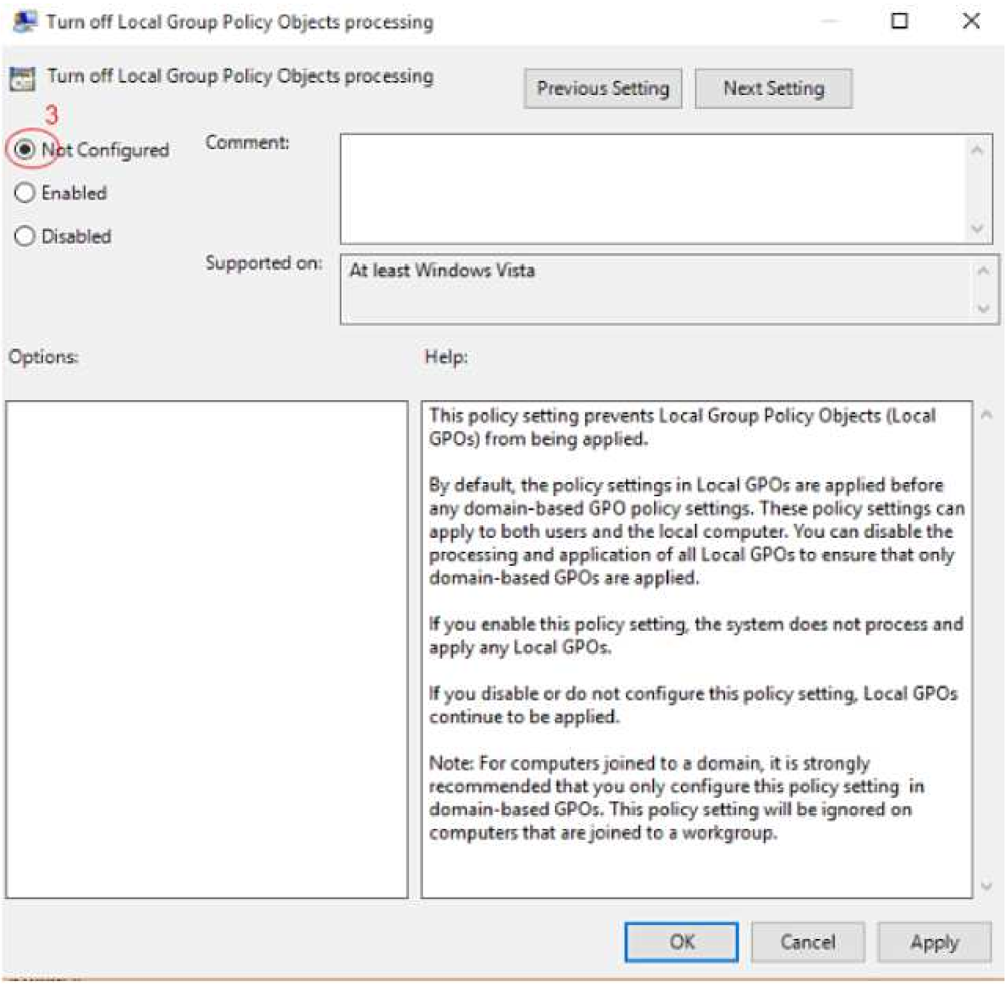
If you enable this policy setting, the system does not process and apply any Local GPOs.

If you disable or do not configure this policy setting, Local GPOs continue to be applied.

Setting
- Allow cross-forest user policy and roaming user profiles
- Configure software Installation policy processing
- Configure disk quota policy processing
- Configure EFS recovery policy processing
- Configure folder redirection policy processing
- Configure Internet Explorer Maintenance policy processing
- Configure IP security policy processing
- Configure registry policy processing
- Configure scripts policy processing
- Configure security policy processing
- Configure wired policy processing
- Configure wireless policy processing
- Specify workplace connectivity wait time for policy processi...
- Determine if interactive users can generate Resultant Set of ...
- Turn off Group Policy Client Service AOAC optimization
- Turn off background refresh of Group Policy
- Turn off Local Group Policy Objects processing
- Remove users' ability to invoke machine policy refresh
- Configure Group Policy Caching
- Enable Group Policy Caching for Servers
- Configure Group Policy slow link detection
- Set Group Policy refresh interval for computers

31 setting(s)

e. Ensure that you have chosen "Not Configured" as shown in the below image.



Turn off Local Group Policy Objects processing

● Not Configured
○ Enabled
○ Disabled

Supported on: At least Windows Vista

This policy setting prevents Local Group Policy Objects (Local GPOs) from being applied.

By default, the policy settings in Local GPOs are applied before any domain-based GPO policy settings. These policy settings can apply to both users and the local computer. You can disable the processing and application of all Local GPOs to ensure that only domain-based GPOs are applied.

If you enable this policy setting, the system does not process and apply any Local GPOs.

If you disable or do not configure this policy setting, Local GPOs continue to be applied.

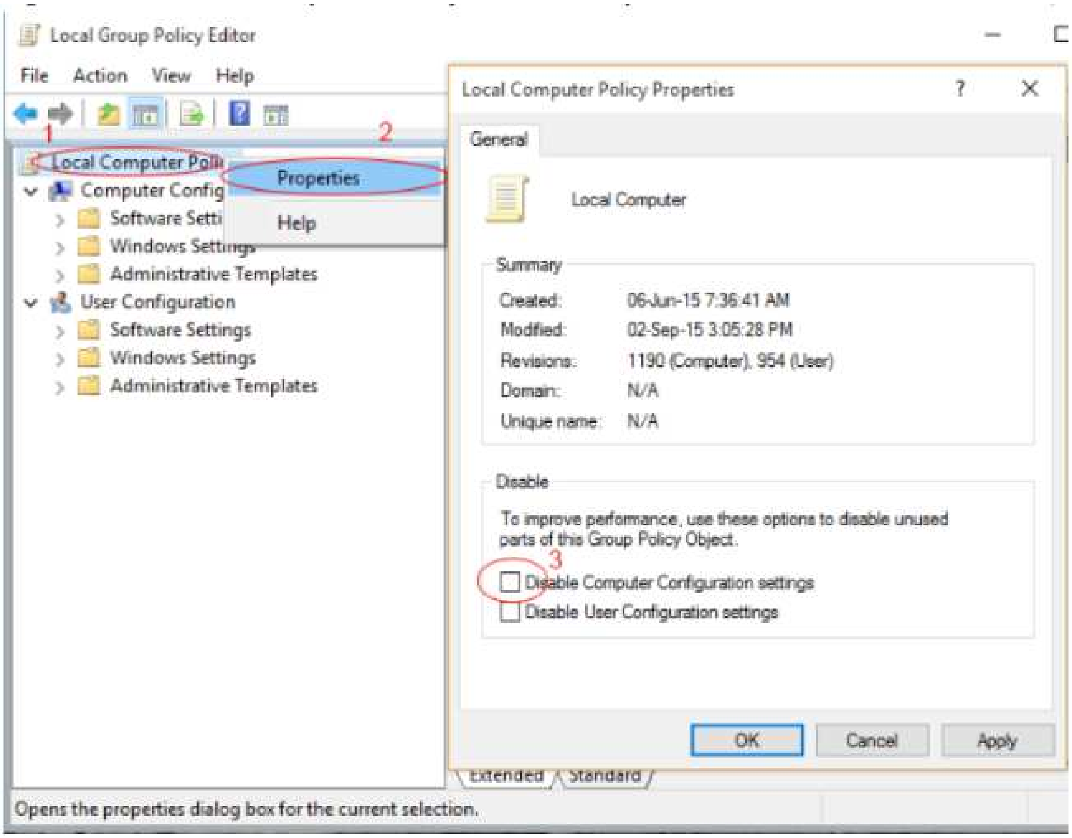
Note: For computers joined to a domain, it is strongly recommended that you only configure this policy setting in domain-based GPOs. This policy setting will be ignored on computers that are joined to a workgroup.

You have now enabled Local Group Policy on the target machine.

2. How to enable Local Group Policy on the target computer?

   You will have to perform the following steps manually on the target computer:

   a. Go to **Run**
   b. Type **gpedit.msc**
   c. Right Click on "**Local Computer Policy**", Choose **Properties** to ensure that "Disable Computer Configuration Settings" is not selected.



Local Computer

Summary

Created: 06-Jun-15 7:36:41 AM

Modified: 02-Sep-15 3:05:28 PM

Revisions: 1190 (Computer), 954 (User)

Domain: N/A

Unique name: N/A

Disable

To improve performance, use these options to disable unused parts of this Group Policy Object.

□ Disable Computer Configuration settings

□ Disable User Configuration settings

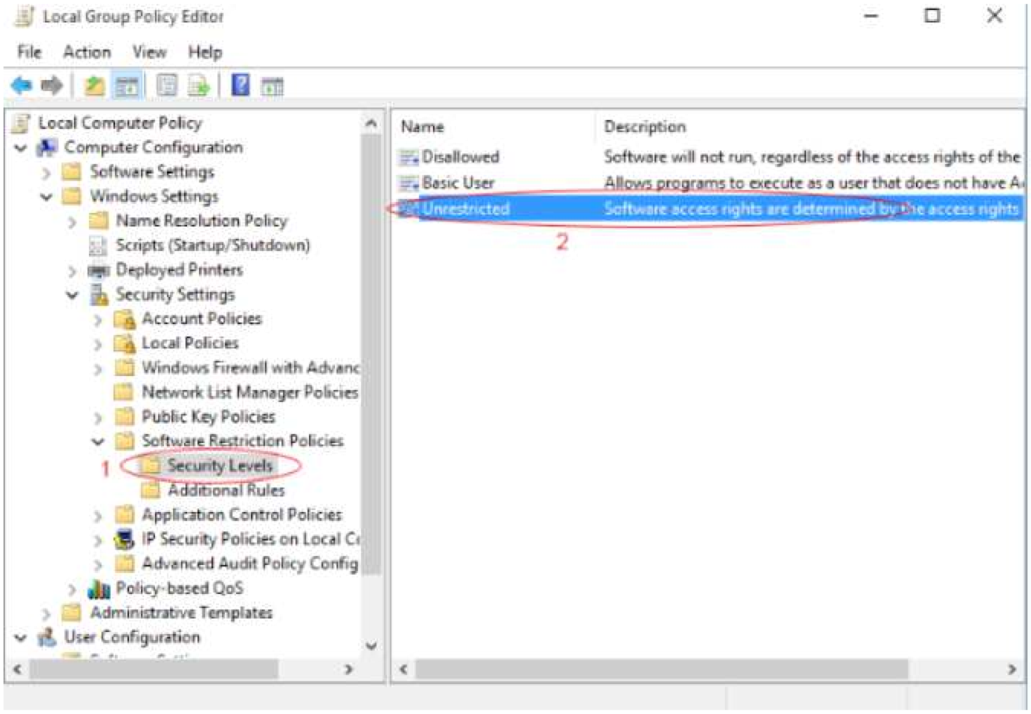
Opens the properties dialog box for the current selection.

You have now enabled Local Group Policy on the target computer.

3. How to set the Default security Policy as "Unrestricted"

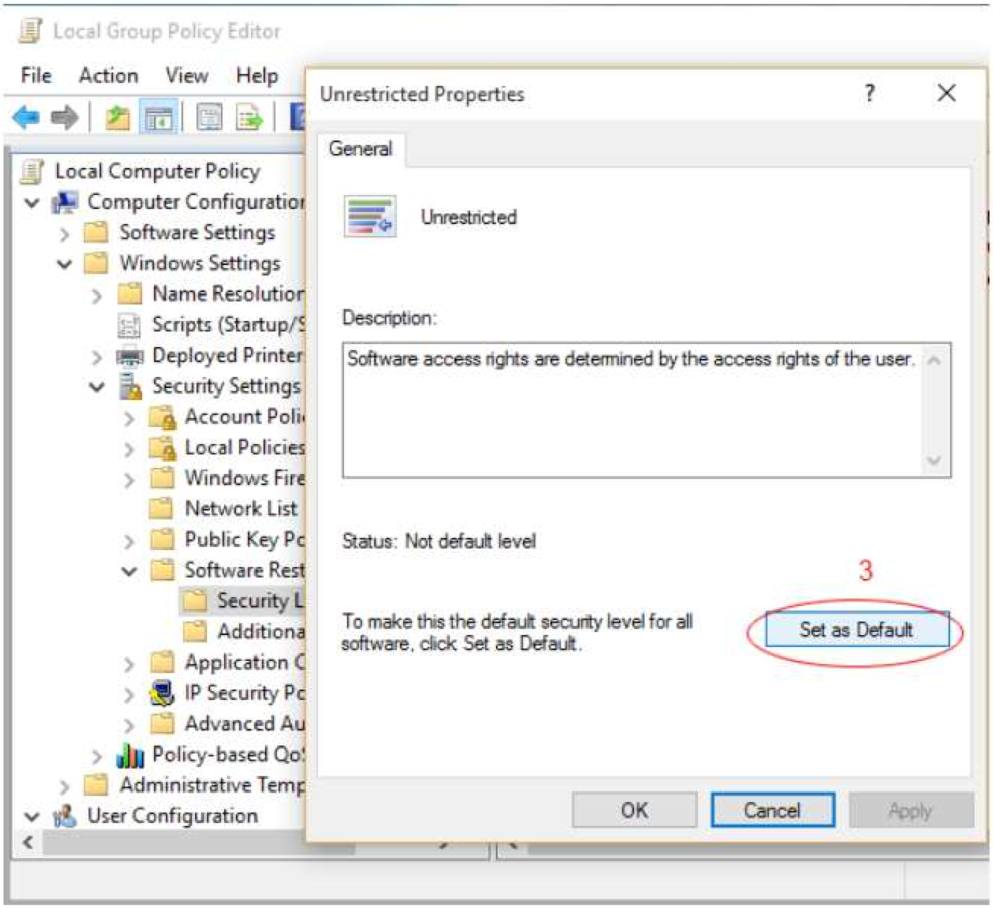
   You will have to perform the following steps manually on the target computer:

   a. Go to **Run**
   b. Type **gpedit.msc**
   c. Click "Security Levels" and double click "Unrestricted" as shown below



Name	Description
Disallowed	Software will not run, regardless of the access rights of the
Basic User	Allows programs to execute as a user that does not have A
Unrestricted	Software access rights are determined by the access rights

d. Ensure that the status is set as "Default" as mentioned in the image below.



Unrestricted

Description:

Software access rights are determined by the access rights of the user.

Status: Not default level

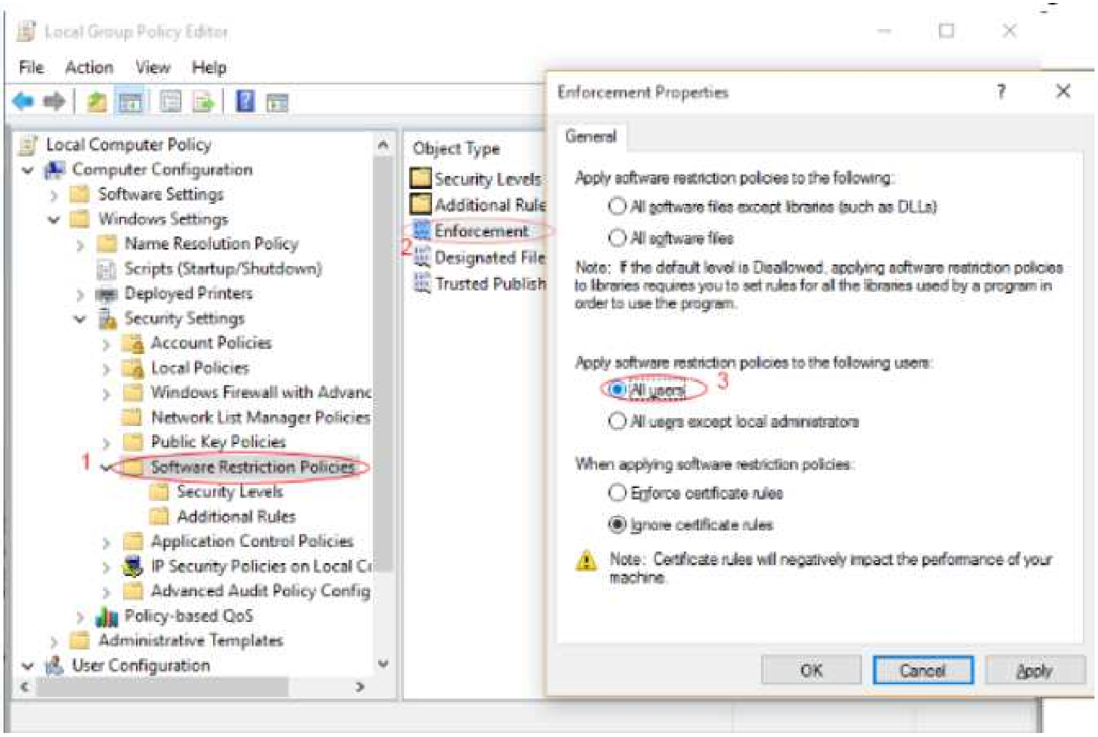
To make this the default security level for all software, click Set as Default.

You have now enabled Local Group Policy on the target computer.

4. How to enable Local Group Policy for the Administrator?

   You will have to perform the following steps manually on the target computer:

   a. Go to **Run**
   b. Type **gpedit.msc**
   c. Click **"Software Restriction Policy"**
   d. Double click **"Enforcement"** to ensure that "**All Users"** is selected as shown in the image below



Enforcement Properties

General

Apply software restriction policies to the following:

○ All software files except libraries (such as DLLs)

○ All software files

Note: If the default level is Disallowed, applying software restriction policies to libraries requires you to set rules for all the libraries used by a program in order to use the program.

Apply software restriction policies to the following users:

● All users

○ All users except local administrators

When applying software restriction policies:

○ Enforce certificate rules

● Ignore certificate rules

Note: Certificate rules will negatively impact the performance of your machine.

OK Cancel Apply

You have now enabled Local Group Policy for Administrators.

Software Metering

Table of contents

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

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

Software metering rules

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

The following details are to be taken into consideration while adding rules:

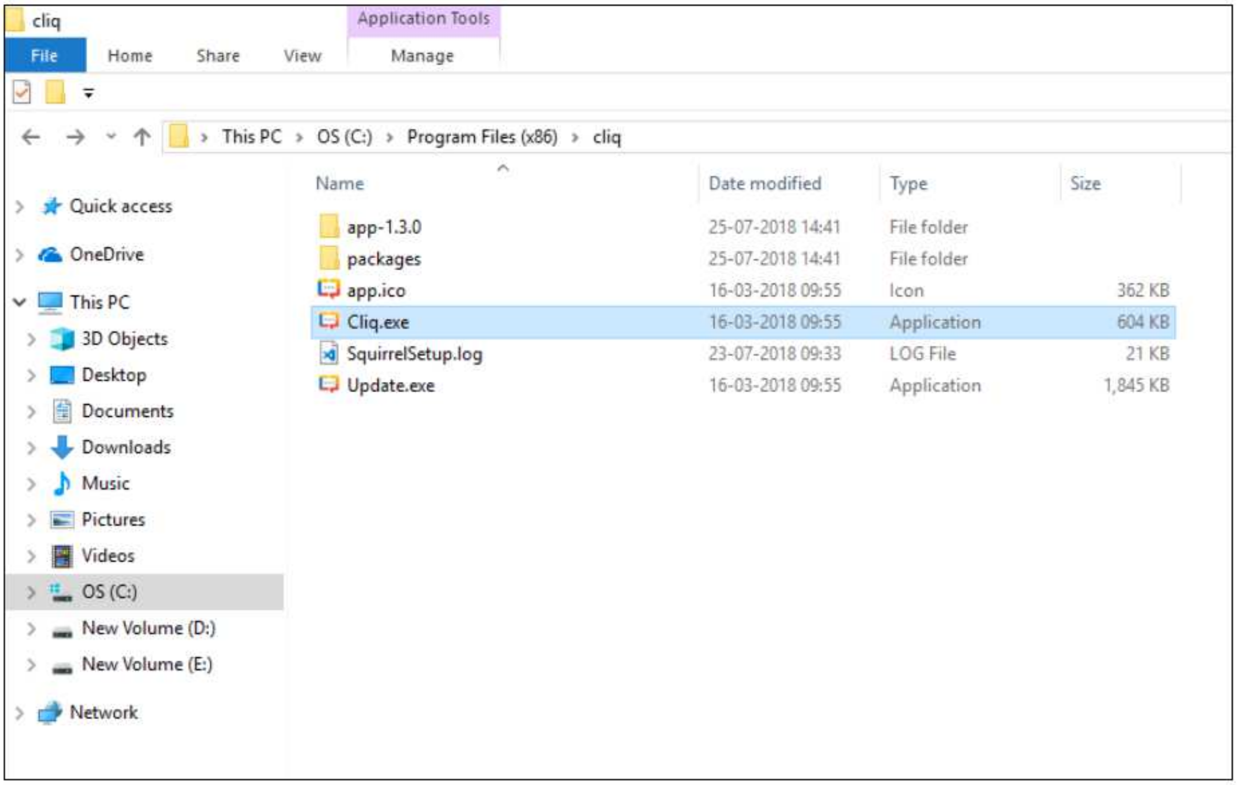
1. File name * : This refers to the executable file name of a software application. You can get this information from the Version/Details tab in the Properties page of the executable file.
2. Original file name : In most cases, the original file name is the same as the name of the executable file. If a user has renamed the executable file of a software application, you can track the usage of that software application, based on its original file name.You can get this information from the Version tab in the Properties page of the executable file. If this information is not available, you can leave the text field blank.
3. Product name : This refers to the name of the product exclusive of the version number.
4. File version : This refers to the version of the executable file of a software application. If

you want the agent to gather details about specific file versions, use an asterisk in the File Version box. For example, if you want the agent to gather details about all file versions beginning with 9, enter 9.* in the File Version box. You can get this information from the Version tab in the Properties page of the executable file. If this information is not available, you can leave the text field blank. If the text field is left blank, the usage details of all the versions of a particular software used in the network will be metered.

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

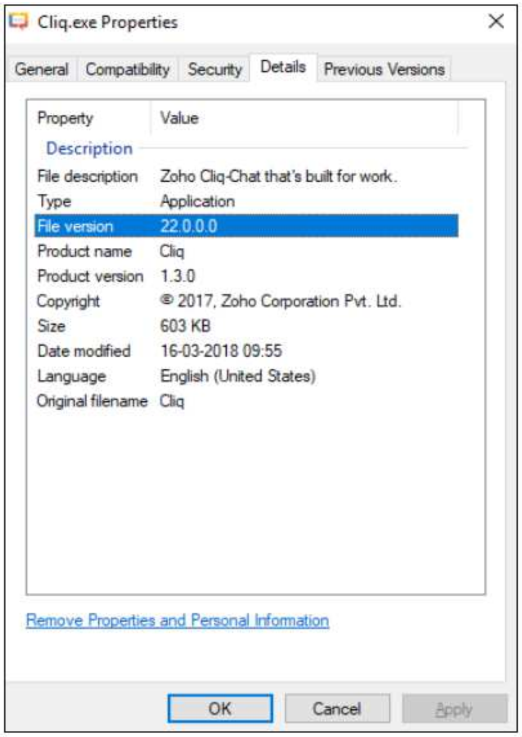
Assume that you want to find information about the details of Cliq software.

1. Open the **exe file location** of the required software in windows explorer.
2. For this, you will have to open the **shortcut location** of the software and right click on properties.
3. Right click on the exe file to obtain details such as file version, original file name and product name.



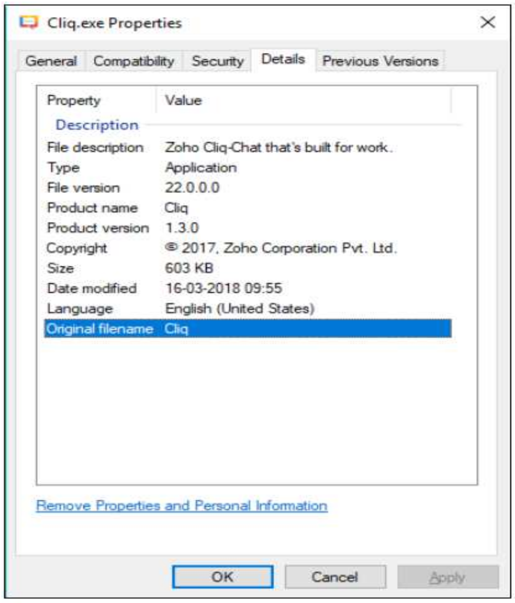
Name	Date modified	Type	Size
app-1.3.0	25-07-2018 14:41	File folder	
packages	25-07-2018 14:41	File folder	
app.ico	16-03-2018 09:55	Icon	362 KB
Cliq.exe	16-03-2018 09:55	Application	604 KB
SquirrelSetup.log	23-07-2018 09:33	LOG File	21 KB
Update.exe	16-03-2018 09:55	Application	1,845 KB

Figure 1: Shortcut in Windows Explorer



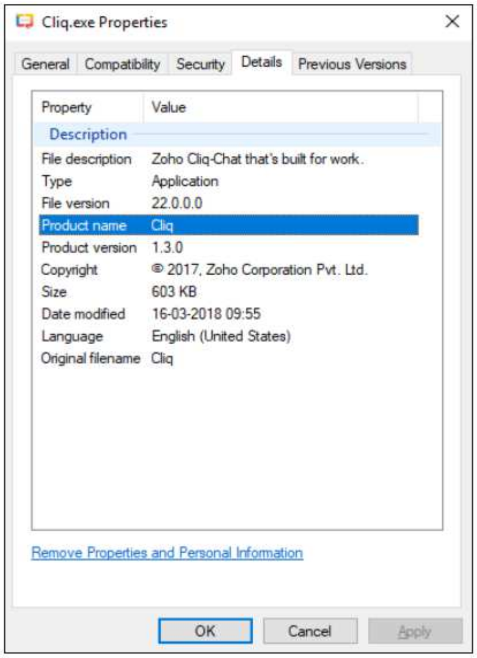
Property	Value
Description	
File description	Zoho Cliq-Chat that's built for work.
Type	Application
File version	22.0.0.0
Product name	Cliq
Product version	1.3.0
Copyright	© 2017, Zoho Corporation Pvt. Ltd.
Size	603 KB
Date modified	16-03-2018 09:55
Language	English (United States)
Original filename	Cliq

Figure 2: File version



Property	Value
Description	
File description	Zoho Cliq-Chat that's built for work.
Type	Application
File version	22.0.0.0
Product name	Cliq
Product version	1.3.0
Copyright	© 2017, Zoho Corporation Pvt. Ltd.
Size	603 KB
Date modified	16-03-2018 09:55
Language	English (United States)
Original filename	Cliq

Figure 3: Original file name



Property	Value
Description	
File description	Zoho Cliq-Chat that's built for work.
Type	Application
File version	22.0.0.0
Product name	Cliq
Product version	1.3.0
Copyright	© 2017, Zoho Corporation Pvt. Ltd.
Size	603 KB
Date modified	16-03-2018 09:55
Language	English (United States)
Original filename	Cliq

Figure 4: Product name

You now have the required information to add rules.

Adding Rules

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

1. Under Inventory tab, click on **Software metering** from the left tree.
2. After clicking on **Add Rules**, provide mandatory details such as Software name, Rule name and File name.

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

You cannot add software metering rules for groups of software.

Software metering reports

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

1. Software metering rules summary
2. Computers with metered software
3. Users with metered software

Software metering rules summary

Based on the rules added for metering of a particular software, this report provides the following details :

1. Discovered count : Number of computers in the network which have the software application installed.
2. Usage count : Number of times a software application is used in all the computers in the network.
3. Usage duration : Information about how long a software application has been used.

Computers with metered software

1. It provides the software usage details such as usage count and usage duration for a particular software application on each computer.
2. In addition to this, the admin can view the reports for each computer during a stipulated time period.
3. With the help of such usage details, the admin can choose to either retain or revoke the license for the software application used on each computer.

Users with metered software

1. The usage details for every user specific software is provided in this report.
2. This is helpful when the users logs into several computer but still the software usage details for that user-specific software needs to be metered.
3. By gauging such usage details, the admin can choose to either retain or revoke the license for user-specific software.

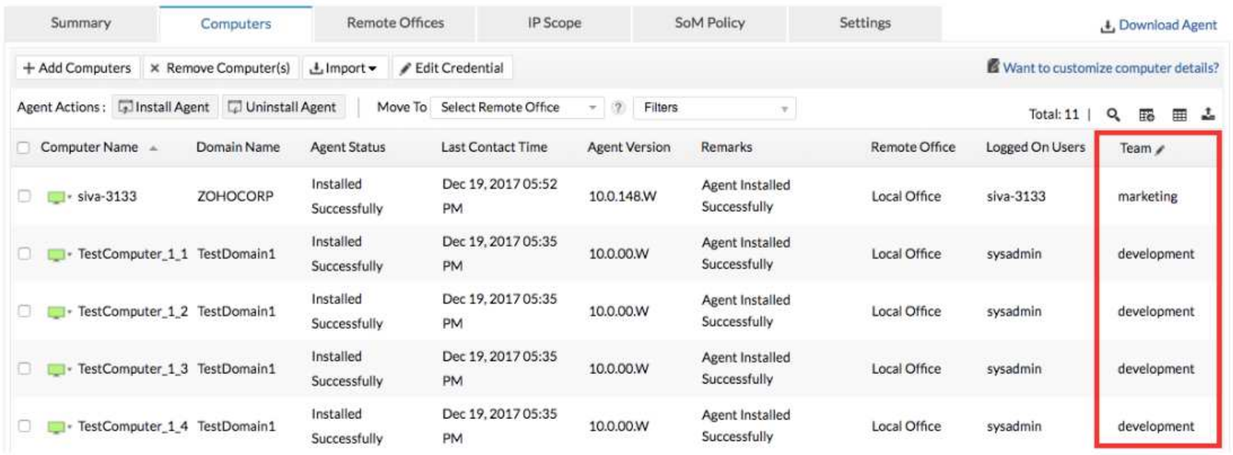
Note : The last **90 days** data from the current date is stored in the Desktop Central report.

Create Custom Fields

Custom Fields allow you to create new columns to display specific views of your data, so that you can quickly see the information that is most important to you. You can gain visibility over insightful data that best aligns with your enterprise specific requirements — column to view user mapping details or asset tag details and many more. These fields can be added only to different Software and Computer views available in Desktop Central.

Here is an example

John, a system administrator has various teams in his enterprise and has to now categorize the computers based on the teams they belong to. Say Devolpment, Marketing or Sales. With Custom Fields, he can create a column **Team** under Admin tab -> Scope of Management -> Computers View so that against each computer name, he will get to know to which team the computer belongs to.



□ Computer Name	Domain Name	Agent Status	Last Contact Time	Agent Version	Remarks	Remote Office	Logged On Users	Team
□ siva-3133	ZOHOCORP	Installed Successfully	Dec 19, 2017 05:52 PM	10.0.148.W	Agent Installed Successfully	Local Office	siva-3133	marketing
□ TestComputer_1_1	TestDomain1	Installed Successfully	Dec 19, 2017 05:35 PM	10.0.0.0.W	Agent Installed Successfully	Local Office	sysadmin	development
□ TestComputer_1_2	TestDomain1	Installed Successfully	Dec 19, 2017 05:35 PM	10.0.0.0.W	Agent Installed Successfully	Local Office	sysadmin	development
□ TestComputer_1_3	TestDomain1	Installed Successfully	Dec 19, 2017 05:35 PM	10.0.0.0.W	Agent Installed Successfully	Local Office	sysadmin	development
□ TestComputer_1_4	TestDomain1	Installed Successfully	Dec 19, 2017 05:35 PM	10.0.0.0.W	Agent Installed Successfully	Local Office	sysadmin	development

Custom Field - Types

You can create custom fields for two types of views. They are,

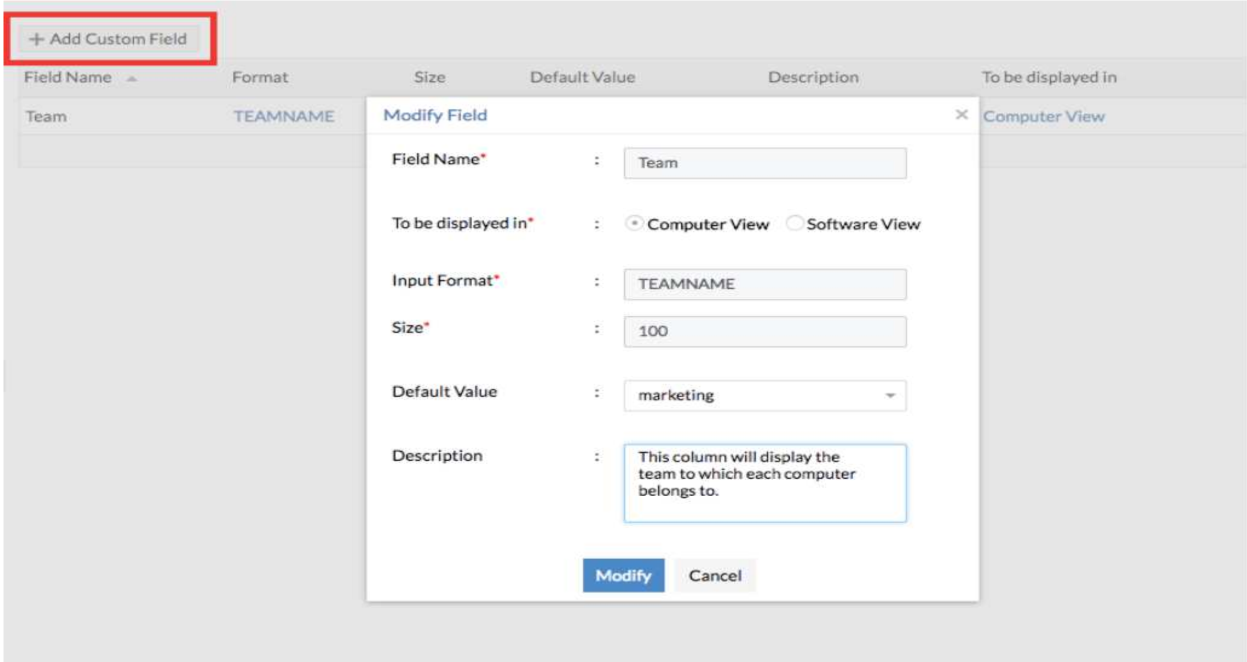
1. **Computer View -** You can view the computers listed under the following,
    - Scope of Management (SoM) -> Computers.
    - Custom Groups
    - Inventory -> Scanned Computers
    - Inventory -> All Computers
2. **Software View -** You can view the software listed under **Inventory -> Software Summary**

Steps to add Custom Fields

1. From your Desktop Central web console, navigate to **Admin tab -> Under Global Settings -> Custom Field -> Add Custom Field.**
2. Furnish the Details such as the name of the custom field, the type of the view in which the field has to be displayed, the data type format for the input value, the size of the value, default value, followed by a small description.

Note: For example, For the custom field **Team** you can choose the alpha-numeric predefined data type as the team name comprises characters.

3. Add the Custom Field.



Field Name	Format	Size	Default Value	Description	To be displayed in
Team	TEAMNAME				Computer View

Modify Field

Field Name* : Team

To be displayed in* : ● Computer View ○ Software View

Input Format* : TEAMNAME

Size* : 100

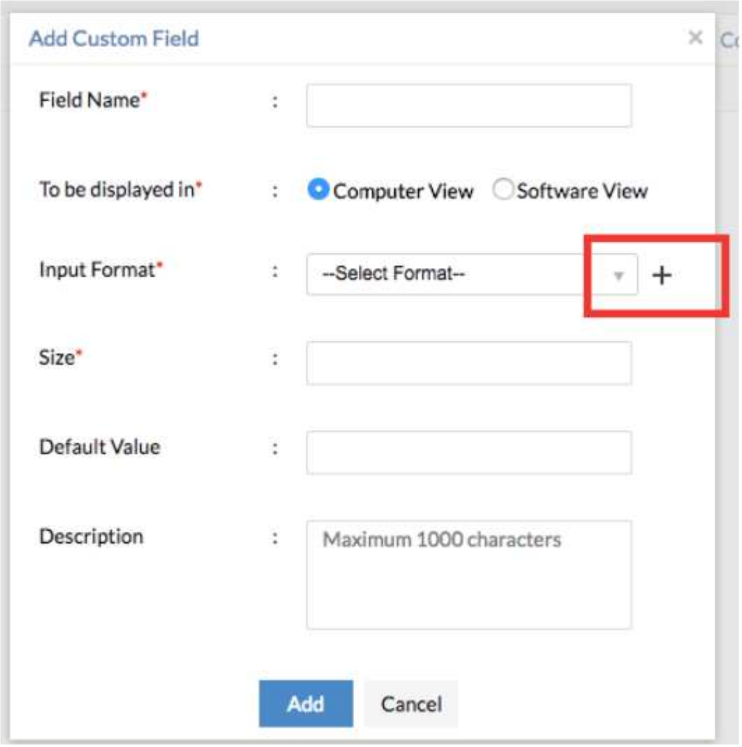
Default Value : marketing

Description : This column will display the team to which each computer belongs to.

4. To modify a Custom Field, Click on actions -> modify across the field name.
5. To delete a Custom Field, Click on actions -> delete across the field name.

To add your own data type format,

1. Navigate to **Admin tab -> Global Settings -> Custom Field**
2. Click on the **Add Custom Field** and press the add button across the input format drop-down list.
3. Name your data format, select a primary format and specify the size.



Add Custom Field

Field Name* :

To be displayed in* : ● Computer View ○ Software View

Input Format* : --Select Format--

Size* :

Default Value :

Description : Maximum 1000 characters

Example: There are only 3 teams in John's enterprise. Now, he can create a custom data type **Team Name** by selecting **alpha-numeric** as the primary data format, specify the size of each input value and the allowed values (value 1, value 2, value 3) as **Development, Marketing and Sales.**

Asset Scan Settings

By configuring asset scan settings, you can choose to either include or exclude components from the inventory scan. This helps in optimization of your inventory data and reports.

The components that can either be enabled or disabled include:

1. Drivers
2. Services
3. Shares

Note:

- Software details, hardware details, antivirus, bitlocker and firewall status along with system details such as users and groups will be scanned during each inventory scan by default.
- Whenever you exclude a component from inventory scan, all the existing data on that particular component will permanently be removed from database.
- Once a component is included to scan, the respective data will be obtained and posted from the subsequent inventory scan.

Viewing Inventory Details

Desktop Central lets you view in-depth inventory details -

- Viewing Hardware Details
- Viewing Computer Details
- Viewing System Details

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 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.
- **Logged on users**: The users who have logged on currently.
- **Last successful scan**:The time at which last scan was carried out successfully

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

When you click on a **specific computer,** the following details will be available :

- Summary
- System details
- Hardware details
- Software details
- Certificates
- File details
- Security details
- USB audit details

Viewing System Details

The System view provides comprehensive details about the services, groups and users in the scanned systems.

To view the system details, follow the steps mentioned below

1. Select the **Inventory** tab.
2. Click the **Computers** link. This lists the computers in your network.
3. Select the computer name for which you want to know the system details. This opens the Computer details page.
4. Select the **System** tab to view the system details. The System tab provides the following details:
    - **Services**: Name of the services running in that system.
    - **Groups**: The groups that are associated with that system.
    - **Users**: The users that are associated with that system.

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

Viewing Inventory Reports

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

1. Hardware Inventory Reports
2. Software Inventory Reports
3. Software Compliance Reports
4. System Details Reports
5. Warranty Reports

Hardware Inventory Reports

Table of contents

Computers by OS

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

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

Computers by Manufacturer

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

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

Computers by Memory

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

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

Computers by Age

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

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

Computers by Device Type

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

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

Computer by Disk Usage

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

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

Mapped Logical Disks

This report provides the details of the drives that are mapped from the computer. Administrators can use this report to identify the logical disks that are mapped to this particular computer. This report plays a vital role for auditing purpose. This report can also be exported in .pdf. xls and .csv format. Administrators can use this report to verify the details of "Mapped Logical Disks" and restrict them, if required. This ensures that the corporate data is secure. To view the report, **Inventory tab --> Inventory Reports --> Mapped Logical Disks**

You can view the list of computers and the details of the drives that are mapped to it. This report will also specify the details of the users, who uses this report, available free space on the disk etc. Select the computer and navigate to the detailed view, to see the report. Clicking a computer account from the report displays the complete information of that account.

Software Inventory Reports

Table of contents

Software by Manufacturer

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

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

Recently Installed Software

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

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

Prohibited Software

Provides the list of prohibited software detected in the network.

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

Software Usage by Computer

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

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

Software Product Keys

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

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

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

Computers with/without a specific Software

Displays the list of Computers that have/do not have a particular software installed on them. You have the flexibility to extract the list based on inputs like, Exact Match of the Software Name specified (or) just a part of the Software Name, etc. Say for example: For an exact match, you specify MS Word and select "Equal" in the Software Name filter. And if you want to identify all the computers that have any of the Microsoft Products, you can simply select the "Like" filter and specify Microsoft in the Software Name field.

To view the report, select the **Inventory** tab and choose the **Computers with/without a specific Software** link available under Software Reports category by hovering the mouse over the **Inventory Reports**

Software Metering

For every Software Metering Rule that you have defined, the Software Metering report will provide the summary of the usage statistics like the number of computers which have this software installed, the usage count of this software and the total usage in hours. You can click on the computers count to get the usage statistics on the individual computers where this software is installed.

To view the report, select **Inventory --> Inventory Reports --> Software Metering**

Software License Compliance Reports

Table of contents

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**

Viewing System Details Reports

- Local Group Members
- Computers by Services
- Share Details

Local Group Members

This reports will give you the list of local user accounts available in the computers of the selected domain. By default, this will list the all the computers with group name as Administrator. You can filter the view by selecting the domain or a custom group and choose the group to view their details.

To view the report, select the **Inventory** tab and choose the **Local Group Members** link available under System Details category by hovering the mouse over the **Inventory Reports**

Computers by Services

This report provides you with the list of computers that has a particular Windows Service running. You can choose the service, its start mode and state and click Generate Report to get the list of computers running that particular service.

To view the report, select **Inventory tab -> Inventory Reports -> Computers by Services**.

Share Details

This report provides the details of the data, that are shared from the computer. Administrators can use this report to identify the drives that are shared from the managed computers. This report plays a vital role for auditing purpose. This report can also be exported in .pdf. xls and .csv format. Administrators can use this report to verify the details of "Shared Drive" and restrict them, if required. This ensures that the corporate data is secure.

To view the report, **Inventory tab -> Inventory Reports -> Share Details**

You can view the list of shares and its details like, users to whom it is shared, permissions provided to the users, shared path, etc. Administrators can use to report to determine, if the share's permission and access need to maintained for all the listed users, or modified for specific users. Select the computer and navigate to the detailed view, to see more details of this report. Clicking a computer account from the report displays the complete information of that account.

Viewing Warranty Reports

Desktop Central automatically retrieves the warranty information of Dell, Toshiba and Lenova computers and provides you the details of the computers whose warranty is about to expire or whose warranty has already expired, etc. While Dell, Toshiba and Lenova computers require no additional information other than their service tag. Desktop Central does not support automatic retrieval of warranty for HP computers, however you can choose to update them yourself manually. For computers other than Toshiba, Dell and Lenova, you can specify the shipping and expiry information manually here to get warranty information in reports. Follow the steps below to manually update the warranty details::

1. Select **Admin ->Inventory Settings ->Add Custom Data for Computers**
2. Choose the computer, to which you wanted to manually add the warranty details
3. Click Bulk Update, to udpate the warranty details manually. However, remember that adding warranty details manually will stop automatic retrieval of warranty details. You can also import the product numbers in bulk using the Import from CSV option
4. Click Save to store the changes

You can see that the warranty details that you have added manually will also be updated in the reports.

Soon-to-expire Warranty

Provides you the details of the computers whose warranty is about to expire soon. You can filter the view to choose the Domain, Custom Group and expiry period.

Expired Warranty

Provides the list of computers whose warranty has already expired

Unidentified Computers

Computers whose warranty information could not be retrieved or for those whose expiry information has not been specified manually will be listed here.

Desktop Central configurations

Table of contents

Introduction to configurations

Desktop Central offers configurations that help administrators manage applications, system settings, desktop settings, and security policies. These are extremely helpful in baselining systems and targets can be selected at user or system level. A group of configurations can also be applied together using the collection feature. The selected settings comes into action either during user logon or computer startup (depending on the type of configuration applied) to minimise the loss of productivity. Status of the applied configurations can also be tracked anytime.

Standardize configurations across your network by applying:

- Windows configurations
- Mac configurations
- Linux configurations

Refer the below-mentioned document for further insights on configurations:

- User configurations: This section provides information about various user-based configurations that you can deploy using Desktop Central and the steps to define them.
- Computer configurations: This section provides information about various computer-based configurations that you can deploy using Desktop Central and the steps to define them.
- Collections: This section provides information about defining a collection of

configurations and steps required to deploy them simultaneously to several users or computers.

- Defining targets: This section provides information about defining targets to which you want to deploy configurations or collections.
- Configuring execution settings: This section provides information about configuring execution settings while defining a configuration. Desktop Central enables you to automate the redeployment process through the Execution Settings option.
- Managing configurations and collections: This section provides information about managing defined configurations. It gives you information about the following:
    - Various configuration statuses displayed on the Desktop Central server
    - Modifying configurations or collections
    - Viewing the status of the defined configurations or collections
    - Suspending deployment
    - Resuming suspended deployments
- Configuration reports: This section provides information about viewing a detailed report about configurations that you define and deploy using Desktop Central. You can also view the status of each configuration in this report.

Defining Configurations

Configurations can be defined for computers or users. You can define a configuration from scratch or use predefined configuration templates. You can also create a group of configurations and deploy them as a collection.

Defining configurations is a four-step process. It comprises of the following steps:

1. Enter a name and description for the configuration
2. Defining the configuration includes the following:
    - Package settings
    - Deployment settings
3. Define a target
4. Configure execution settings

After you define a configuration, you must apply it to specific targets (computers/users) in your network.

Applying Configurations

When you deploy a configuration using Desktop Central, the configuration settings along with the required files will be stored in the Desktop Central server. Desktop Central agents, which are installed in the client computers in your network, will contact the Desktop Central server to collect this information and apply the configurations to specific client computers. The agents will contact the server during the following intervals to collect the required information:

- User-specific configurations: When a user logs on and every 90 minutes thereafter till the user logs out of the domain
- Computer-specific configurations: When a computer is started and every 90 minutes thereafter till the system is shut down

Re-applying Failed Configurations

When you deploy a configuration to client computers, the deployment could fail in a few computers due to various reasons. In such cases, you can re-deploy the configuration. Desktop Central enables you to automate the redeployment process through the Execution Settings option. This option enables you to do the following:

- Specify whether you want the agent to retry applying this configuration in the computers in which the deployment of the configuration failed
- Choose the number of times you want the agent to try deploying a configuration. You can also specify how many times, out of the number of times that you have specified, you want the configuration to be deployed when:
    - Users log on
    - Computers complete the 90-minute refresh cycle

Based on the specified input, configurations will be re-deployed on the computers on which the deployment failed till either of the following takes place:

- Deployment is successful
- Maximum retry count is reached

Reverting Configurations

Desktop Central does not take backup of the settings that you make when you create configurations. Therefore, it is very important that you remember the settings you have made. In most cases, you cannot revert the configuration. However, you can modify the settings that you had made earlier and re-deploy the configuration.

Examples

You can modify configurations and re-deploy them in the following scenarios:

- Assume that you have deployed a configuration to install a software application.

You can revert and change it to enable uninstallation of the software application. You must modify the configuration by changing the following:

  - Operation type from Install to Uninstall
  - Type of package

The package must have an uninstall string.

  - When you want to revert a configuration related to a security policy, you can modify the policy and change the settings as required. For example, assume that you have created a configuration to disable the option to change the wallpaper on the desktop of a computer. You can modify the configuration and change the policy to enable the option to change the wall paper, before re-deploying the policy.

Windows Configurations

Over 30 predefined configurations help administrators manage windows applications, system settings, desktop settings, and security policies. Windows configuration can be applied to user(s) and computer(s) -

- Computer configurations
- User configurations

Desktop Central offers configurations for Mac and Linux as well.

Computer Configurations

This document comprises of the configurations that can applied to computers belonging to Windows domain. These configurations are applied either during system startup or refresh interval. Ensure that you have defined the scope of management before defining the configurations.

Follow the steps mentioned below for choosing a configuration that needs to be created and deployed:

1. Navigate to **Configuration** tab. This will list all the supported configurations for computers and users as well.
2. Choose the required computer configuration.

Desktop Central supports the below mentioned configurations that cover the functionalities of 4 major categories extensively:

Security Configurations

Desktop Central offers a bunch of configurations that when deployed, aids in hardening the security of your endpoints. The security configurations offered by Desktop Central are as follows :

- Certification Distribution
- Firewall
- Install/Uninstall Patch
- Permission Management
- Secure USB Devices
- Security Policies

Productivity Configurations

Amp up the productivity of your network by deploying the following configurations to all the computers in your network.

- Custom Scripts
- Environment Variables
- IP Printer

- Install/Uninstall Software
- Path
- Power Management
- Registry
- Scheduler
- Services
- Shortcut
- WiFi

Desktop Configurations

Deploy the below mentioned desktop configurations & save ample amount of time in managing the desktops.

- Common Folder Redirection
- Display
- File Folder Operation
- Fonts
- General
- Group Management
- Legal Notice
- Message Box
- User Management

Application Configurations

- Launch Application

Certificate Distribution

Description

This document provides the steps required to distribute digital certificates that are used on Windows platform. Using the Certificate Distribution configuration, you can distribute certificates such as SSL Certificates (for web browsers like Chrome) & AD CA Root Certificates (to authenticate users on your WiFi network) to specified targets.

Here are a few scenarios where Certificate Distribution configuration can be used to distribute certificates efficiently:

1. Installing root certificates to authenticate AD users for WiFi access in an organization.
2. Distribute security certificates to browsers like Chrome, Internet Explorer, etc to securely access websites within an organization.

Installing Certificates:

The following are the steps to install certificates to your specified targets:

1. Navigate to Configurations -> Windows -> Certificate Distribution -> Computer.
2. Specify the name and description of the configuration.
3. Select the Install option.
4. Select certificate store(s) to which the certificate should be distributed to.
5. Browse and upload the certificate file from your computer.
6. Specify password for the certificate file if required.
7. You can select multiple certificate files to install using 'Add More Certificates' option.

Deleting Certificates:

The following are the steps to delete certificates from the certificate stores of targets selected:

1. Navigate to Configurations -> Windows -> Certificate Distribution -> Computer.
2. Specify the name and description of the configuration.

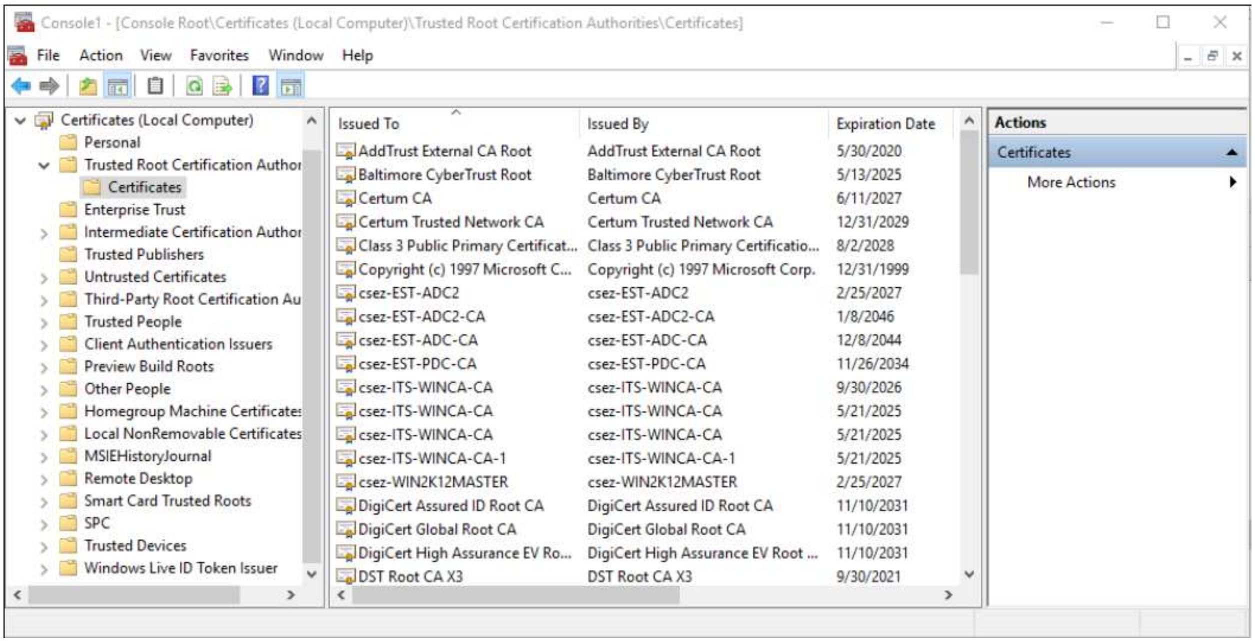
3. Select the Delete option.
4. There are two delete actions that you can perform:
   - Delete specific certificate from the certificate store(s).
   - Delete all expired certificates from the certificate store(s).
5. Select the certificate store(s) from where certificates should be deleted.
6. Specify the Common Name (CN) value of the certificates.
7. All certificates with the given CN value will be deleted from the stores selected above.
8. To delete a specific certificate, specify its unique serial number.
9. You can select multiple certificate files to delete using 'Add More Certificates' option.

How to find the Common Name value (CN) and Serial Number of a certificate ?

To delete a specific certificate, you will have to specify a common name (CN) and its serial number. Find the CN and serial number from the certificate store of the computer where the certificate exists.

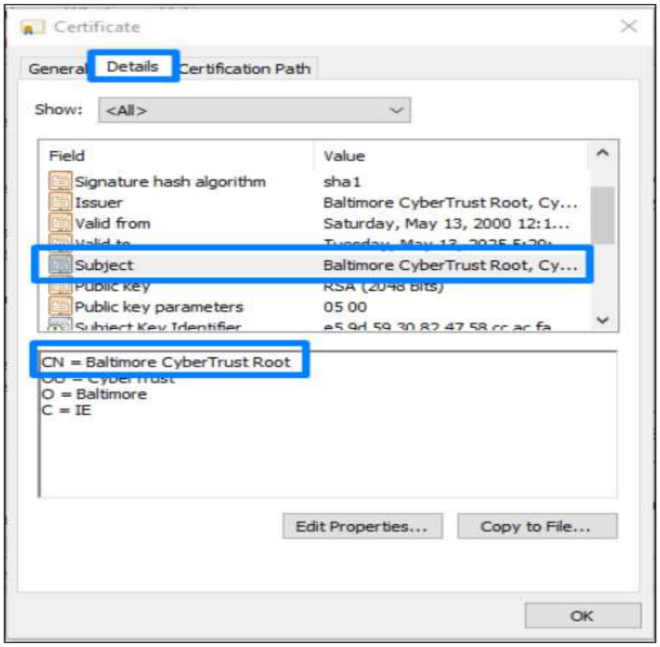
Steps:

1. Navigate to Run prompt window and open Microsoft Management Console (MMC).
2. Select File -> Add/Remove Snap-in.
3. Select 'Certificates' from the available snap-ins.
4. You can select for which account you would like to manage certificates for.
5. Double click on the certificate to be deleted from the certificate store.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Certificates (Local Computer)
Personal
Trusted Root Certification Author
Certificates
Enterprise Trust
Intermediate Certification Author
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Client Authentication Issuers
Preview Build Roots
Other People
Homegroup Machine Certificates
Local NonRemovable Certificates
MSIEHistoryJournal
Remote Desktop
Smart Card Trusted Roots
SPC
Trusted Devices
Windows Live ID Token Issuer
Actions
Certificates
More Actions

Issued To	Issued By	Expiration Date
AddTrust External CA Root	AddTrust External CA Root	5/30/2020
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025
Certum CA	Certum CA	6/11/2027
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999
csez-EST-ADC2	csez-EST-ADC2	2/25/2027
csez-EST-ADC2-CA	csez-EST-ADC2-CA	1/8/2046
csez-EST-ADC-CA	csez-EST-ADC-CA	12/8/2044
csez-EST-PDC-CA	csez-EST-PDC-CA	11/26/2034
csez-ITS-WINCA-CA	csez-ITS-WINCA-CA	9/30/2026
csez-ITS-WINCA-CA	csez-ITS-WINCA-CA	5/21/2025
csez-ITS-WINCA-CA	csez-ITS-WINCA-CA	5/21/2025
csez-ITS-WINCA-CA-1	csez-ITS-WINCA-CA-1	5/21/2025
csez-WIN2K12MASTER	csez-WIN2K12MASTER	2/25/2027
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/10/2031
DST Root CA X3	DST Root CA X3	9/30/2021

6. Select Details tab -> Subject field.
7. Copy the Common Name (CN) value. If CN value is not found, specify the value mentioned in Issued To column.

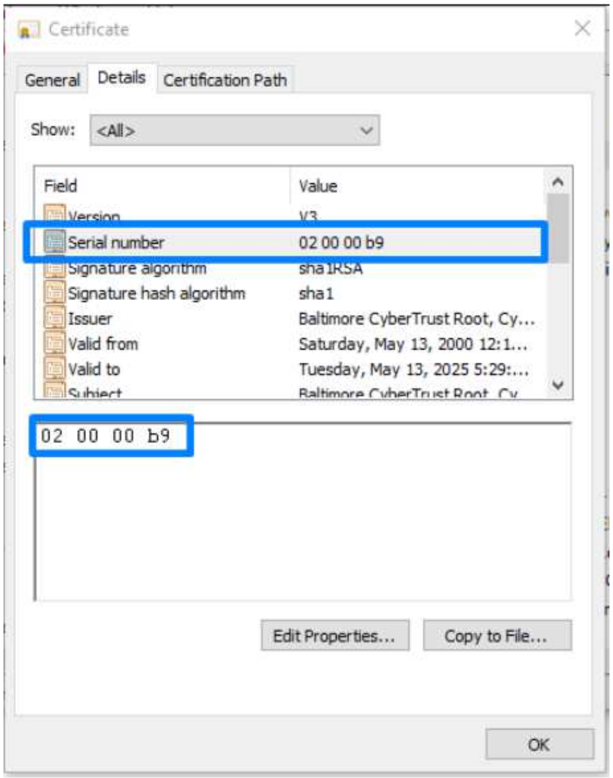


Show: <All>

Field	Value
Signature hash algorithm	sha1
Issuer	Baltimore CyberTrust Root, Cy...
Valid from	Saturday, May 13, 2000 12:1...
Valid to	Tuesday, May 13, 2025 5:29:...
Subject	Baltimore CyberTrust Root, Cy...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Subject Key Identifier	e5 9d 59 30 82 47 58 cc ac fa

CN = Baltimore CyberTrust Root
OU = CyberTrust
O = Baltimore
C = IE

8. Copy Serial number value from Details tab -> Serial number field.



Show: <All>

Field	Value
Version	V3
Serial number	02 00 00 b9
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Baltimore CyberTrust Root, Cy...
Valid from	Saturday, May 13, 2000 12:1...
Valid to	Tuesday, May 13, 2025 5:29:...
Subject	Baltimore CyberTrust Root, Cy...

```
02 00 00 b9
```

You have successfully created a configuration to either distribute or delete certificates from the certificate store of the required computer.

Configuring Firewall

Overview

Configuring firewall is one of the most significant task of a system administrator. Firewall plays a vital role in securing the data from hackers. Desktop Central helps you to deploy customized firewall settings at ease. A firewall configuration in general, can be explained as a collection of Profiles/Rules. These Profiles/Rules, are applied on a computer to determine the permission for all inbound and outbound communication on specified ports. Using Desktop Central, you can create new configurations to deploy specific settings or modify the existing firewall settings, which were not applied using Desktop Central.

Understanding Windows Firewall Profiles

Before we start creating firewall configuration, let us know more about Windows Firewall Profiles. Every computer running Windows operating system, connects to internet/network via profiles. There are three profiles for Windows computers, they are

- **Domain** : This configuration will be applied to computers, which are a part of the domain. Whenever a computer reaches the internet/network the restrictions applied on the firewall of the computer will take effect. This is an ideal example of how computers work in a business environment.
- **Private** : When a computer is connected to a private network, the firewall restrictions will be applied to it. Private Network is the one, which is not connected/exposed directly to the internet. Private networks are configured in such a way, that a security device like NAT (Network Address Translation) or a hardware firewall is precedes the network for security reasons. This creates a layer of security than Domains. This is configured in most enterprises to secure their corporate data.
- **Public** : This profile does not have any security devices or restrictions between the computer and the internet. A good example for public network, is the one you can find in airports, railway stations, coffee shops etc. You need to ensure that you have configured firewall in a most secure way, since these networks in general do not require secured access to reach the internet.

Understanding Rules

Rules are settings which provide advanced control for the system administrator. A rule is a policy, which can be forced over the profiles. Assume you create a profile for Domain and specify to block all inbound communication, you can still create a rule to add exception to the specified profile, and allow inbound communication to a specific port.

Desktop Central supports configuring firewall for computers running Windows XP and later versions.

Follow the steps mentioned below to configure Firewall

1. Windows Vista and later versions
2. Windows XP and 2003 Server

Windows Vista and later versions

You should choose the profile to which you wanted to configure the firewall like Domain/Private/Public. You can also create a generic firewall configuration for all the profiles by selecting all. After specifying the profile, you will have to choose the Action, that needs to be performed on the firewall like,

1. **Do not Modify** : Will not impact the existing firewall settings, if any are configured
2. **ON**: Will turn on the Firewall for the target computer
3. **OFF**: Firewall will be turned off for the target computer

If you have chosen to turn on the firewall, then you will have to specify the action for inbound and outbound communication separately.

Here are few examples for your reference:

1. Profile **All -** Applies to all Domain, Private and Public profiles
   Action on Inbound : Allow
   Action on Outbound : Block
   In this case, all inbound connections will be allowed and all outbound connections will be restricted on the firewall.
2. Profile **Domain -** Applies to computers, only when they are connected to a Domain Network
   Action on Inbound : Allow
   Action on Outbound : Block
   In this case, all inbound connections will be allowed and all outbound connections will be restricted on the firewall.
3. Profile **Public -** Applies to computers, only when they are connected to a Public Network
   Action on Inbound : Block

Action on Outbound : Allow
In this case, all inbound communication will be blocked and outbound connections will be allowed on the firewall, when the computer is connected to a public network.
However, if you have applied any specific rule, to exempt inbound communication for a specific port, then the inbound communication will be allowed only the specified port .

You can create specific rules to exclude specific functions like inbound/outbound communication on specific ports. When you create a rule, you will have to specify a name for the rule, and specify to which profile should this rule be applied, like Domain/Public/Private. You should also specify the port number/ protocol and the action to be performed as exception. You can create one or more rules for the same profile.

You can choose the target, specify the execution settings and deploy the configuration. You have successfully configured the firewall settings on computers running Windows Vista and later versions.

Windows XP and 2003 Server

If you wanted to configure Firewall on the computers running Windows XP, then ensure that Windows XP Service Pack 2 is installed on those computers.

You can choose the Action, that needs to be performed on the firewall like,

1. **Do not Modify** : Will not impact the existing firewall settings, if any are configured
2. **ON**: Will turn on the Firewall for the target computer
3. **OFF**: Firewall will be turned off for the target computer

After specifying the Action on Firewall, you will have to specify the Action that needs to be performed on specific ports. You can choose the action that needs to be performed on the ports like,

1. **Do not Modify** : Will not impact the existing settings, if any are configured
2. **Allow** : All connections inbound/outbound will be allowed for the port, that you choose. You will have to choose/add the port/protocol and specify the dependent services if any.
3. **Block** : All connections inbound/outbound will be blocked for the port, that you choose. You will have to choose/add the port/protocol and specify the dependent services if any.
4. **Port** : Specify the port number. The port number can also be customized by selecting a port from the list of available ports.

You can choose the target, specify the execution settings and deploy the configuration. You have successfully configured the firewall settings on computers running Windows XP.

Installing/Uninstalling Patches and Service Packs

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Install/Uninstall Patch configuration enables you to install or uninstall patches from a central location. Uninstallation of patches is not supported for computers running on Mac operating systems. Below mentioned steps can be followed for installation and uninstallation of patches using Desktop Central.

- Install/Uninstall Patches in Windows Computers
- Install Patches in Mac Computers
- Creating a configuration from All Patches View

Install Patches in Windows Computers

1. Navigate to **Configurations** tab and choose **Install/Uninstall Patch** configuration from the list of Windows Configurations.
2. Follow the steps mentioned below to install/uninstall patches for Windows OS.

Step 1: Name the Configuration

Provide a name and description for the Install/uninstall Patches Configuration.

Step 2: Define Configuration

Note: Specify the operation type as Install or Uninstall for installation and uninstallation of patches respectively and specify the following values.

Parameter	Description
Add the Patches	If you have reached this configuration page from the Patch Management tab by selecting the patches, the selected patches automatically gets added to the List of Patches. Click the Add More Patches button to invoke the Patch Browser. From the patch browser select the patches and service packs that have to be applied. The patch browser has an option to view the missing patches/service packs or all patches/service packs, which can then be filtered based on the application and service pack.
Scheduler Settings	Install After ● Select this option and specify the date and time after which the patches have to be installed. The patches will be installed based on the Install Options selected after the scheduled time. Expiry date ● Set an expiry date for installation/uninstallation of patches.
Deployment Settings	If you have set any Policy as default, then the default policy will be automatically applied to the configuration. You can choose from the policies which are listed under "Apply Deployment Policy". You can see the Policies segregated as My Policies and Created by Others. You can click on View Details to see the policy details and the list of configurations to which the policy is applied. If you do not have an existing policy, you can create one by clicking on create policy Deployment Rule: Deployment can be continued even if some patches cannot be downloaded. If the failed patches are

	successfully redownloaded, they will be installed in the subsequent refresh cycle (within deployment window).

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Install Patches Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Install Patches Configuration in the defined targets. Deployment will be initiated during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Install Patches in Mac Computers

Follow the steps mentioned below to install patches Mac operating systems.

1. Click on Patch Management
2. Under Deployment select Install Patch
3. Choose the operating system as Mac and then create a configuration that needs to be deployed.

Step 1: Name the Configuration

Provide a name and description for the Install Patches Configuration.

Step 2: Define Configuration

specify the following values:

Parameter	Description
Add the Patches	Click the Add More Patches button to invoke the Patch Browser. From the patch browser select the patches that have to be applied. The patch browser has an option to view the missing patches or all patches, which can then be filtered based on the application and service pack. If you have reached this configuration page from the Patch Management tab by selecting the patches, the selected patches automatically gets added to the List of Patches.
Scheduler Settings	Install After ● Select this option and specify the date and time after which the patches have to be installed. The patches will be installed based on the Install Options selected after the scheduled time.

Deployment Settings	Specify the following Deployment Settings: Installation/Uninstallation Option: 1. Install during computer startup: Select this option if the patches have to be deployed during computer startup. 2. Install during 90 minutes refresh interval: Select this option if the patches have to be installed after the computer startup when the next update happens (within 90 minutes) 3. Either of the above, whichever is earlier Install Between ● If you want the installation to happen only between a specified time of a day, you can specify the Start and End time within which the deployment should begin. The Start Time can also be greater than the End time - in such cases the End time is assumed to be on the following day. For example, if you wish the deployment should happen between 10.00 PM and 4.00 AM, you can specify the Start Time as 22:00:00 and End Time as 04:00:00 Allow Users to Skip Deployment 1. Specify whether the use can skip the deployment at a later time by selecting the "Allow Users to Skip Deployment". When you do not select this option, the deployment will be forced and the user will not have any control on the deployment. 2. When you allow users to skip deployment, you can also specify whether they can skip it as long as they wish or force deployment after a specific date. Reboot Policy 1. Do not reboot: Select this option if the client computers should not be rebooted after installing the patches. 2. Force Reboot when the user has logged in: Select this option to force the user to reboot the computer.

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

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Install Patches Configuration

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Install Patches Configuration in the defined targets. Deployment will be initiated during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Note: Patch Uninstallation is currently not supported for Mac Computers

Creating a configuration **from All Patches View**

If you are trying to create a configuration from **Detailed View** under **All Patches,** then the below mentioned scenarios will come into effect. Detailed view will list every missing patch against every single computer in a separate row, which means if a single patch is missing in 5 computers, 5 rows will be listed.
When you have chosen to deploy more than one patch for more than one computer as mentioned below, then you might end up in deploying the patches to the computers which you never intended to deploy. **Creating a configuration based on the above selection will work as follows:**

Selected Patches: Patch 1, Patch 2 and Patch 3.

Defined Target : Computer 1, Computer 2, and Computer 3.

Result of this Deployment:

Patch ID	Included Target	Intended target	Missing Patch	Deployment Initiated	Expected Result
Patch 1	Computer 1	Yes	Yes	Yes	Will be deployed
Patch 1	Computer 2	Yes	Yes	Yes	Will be deployed
Patch 1	Computer 3	No	No	Yes	Will not be deployed
Patch 2	Computer 1	No	Yes	Yes	Will be deployed
Patch 2	Computer 2	Yes	Yes	Yes	Will be deployed
patch 2	Computer 3	No	No	Yes	Will not be deployed
patch 3	Computer 1	No	No	Yes	Will not be deployed
Patch 3	Computer 2	No	No	Yes	Will not be deployed
Patch 3	Computer 3	Yes	Yes	Yes	Will be deployed

As per the above mentioned table, the configuration will be deployed across to all the computers to which the patch is applicable. **Patch 2** is applicable for **computer 1,** but you never intended to deploy it, however the deployment will happen on it, since it is a missing patch.

In order to overcome this, it is recommended to deploy multiple patches to single computer or single patch to multiple computers from "Detailed View". If you want to deploy multiple patches for multiple computers, then it is recommended to create multiple configurations or initiate deployment from Missing Patches View.

> **Note:** When a Patch Management task is initiated, Desktop Central agent residing on the client computer scans the computer for the missing patches and downloads only the applicable patches from the Desktop Central server. If you are managing computers in a remote office using a Distribution Server, then WAN agents will download the applicable patches from the Distribution Server. However the deployed patches will be replicated to the Distribution Server irrespective of whether the patch is applicable for the remote office computers or not.

Managing Permissions

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

The Permission Management allows you to grant or revoke permission on the files, folders and registry. Desktop Central Permission Management Configuration enables you to grant/revoke permissions to multiple computers from a central point.

Step 1: Name the Configuration

Provide a name and description for the Permission Management configuration.

Step 2: Define Configuration

You can grant or revoke permissions for the following objects:

- Files
- Folders
- Registry

Files

To grant or revoke permissions for files, select the *File* tab and specify the following values:

Parameter	Description
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: ● Append - To append to the existing file permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. ● Overwrite - To overwrite the existing file permissions ● Revoke - To revoke the existing file permissions of the specified user/group. All the permissions to the specified user/group on that file will be removed. However, the inherited permissions will not be removed.
File name	Specify the name of the file for which you need to specify permissions.
Settings	Select the required options.

If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Folders

To grant or revoke permissions for folders, select the *Folder* tab and specify the following values:

Parameter	Description

User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: ● Append - To append to the existing folder permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. ● Overwrite - To overwrite the existing folder permissions ● Revoke - To revoke the existing folder permissions. All the permissions to the specified user/group on that folder will be removed. However, the inherited permissions will not be removed.
Folder name	Specify the name of the folder for which you need to specify permissions.
Inheritance	Select the required option to specify how the permission should effect its subfolders and files
Settings	Select the required options.

If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Registry

To grant or revoke permissions for registry, select the *Registry* tab and specify the following values:

Parameter	**Description**
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: ● Append - To append to the existing registry permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. ● Overwrite - To overwrite the existing registry permissions ● Revoke - To revoke the existing registry permissions. All the permissions to the specified user/group on that registry key will be removed. However, the inherited permissions will not be removed.
Hive	Select the registry hive from the given options
Key	Specify the key within that hive for which you need to set the permissions
Inheritance	Select the required options to specify how the permission should effect its subkeys.
Settings	Select the required options.

If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

To modify a permission from the **List of Permission Actions** table, select the appropriate row and click 📝 icon and change the required values.

To delete a permission from the **List of Permission Actions** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Permission Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Permission Management Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Securing USB Devices

This document will explain the following:

- Applying Secure USB Settings to Computers
- Adding Restrictions to secure USB Devices & Excluding Devices
- Revoking All USB Restrictions applied to the User

Description

The Secure USB configuration is used for both users and computers to block or unblock the use of the USB devices.

Using this configuration, you can block or unblock the following devices:

1. Mouse
2. Disk drives (for example, USB drives and external hard-disk drives)
3. CD ROMs
4. Portable devices (for example, mobile phones, digital cameras and portable media players)
5. Floppy disks
6. Bluetooth devices
7. Images (for example, USB cameras and scanners)
8. Printers
9. Modems
10. Apple USB devices (for example: iPhone, iPad and iPod touch)

You can also exclude devices using the Vendor ID or Device Instance ID assigned to each device.

Applying Secure USB Settings to Computers

When you apply the Secure USB configuration to both computers and users, the settings made for computers will be applied before the settings made for users. For example, assume that you have made the following settings:

1. **Settings configured for users**

   a. Administrator: You have unblocked the usage of the disk drive
   b. Other users (excluding the administrator): You have not deployed any configurations
2. **Settings configured for computers :** You have blocked the usage of portable devices and disk drives

The following actions will take place:

1. Computer startup: The Secure USB configuration settings made for the computer are applied when the computer is started. This means that no portable devices and disk drives can be used.
2. Administrator logon: The Secure USB configuration for the computer is applied. However, it is over written by the settings made for the administrator. This means that the administrator can use disk drives.
3. Other users (excluding the administrator) log on: The Secure USB configuration made for the computer is applied.
4. Other users (excluding the administrator)log off: The log off action settings made for users are applied when a user logs off. If the log off-action setting is set to Don't alter device status, then the settings made will apply to the next user who logs on, provided that the user does not have any settings that apply to them.

> **Note**: **Block USB**, represents to block the access to use any USB device.
> **Unblock USB,** represents to re-enable the access to the USB devices that has been blocked.
> **No Change,** represents that no change has been made to the current settings.

Adding Restrictions to secure USB Devices

As an administrator, you can create a configuration block or unblock specific USB devices. You can also exclude specific devices, if required.

To create a configuration to secure USB devices for users, follow the steps given below:

1. Navigate to **Configurations** tab and choose **Secure USB** from the list of Windows configurations.
2. Enter a name and description for the configuration
3. Click **Add** to apply restrictions
4. To add restrictions, select the devices, choose to block or unblock devices. When you have chosen to block devices, you can also specify the devices which needs to be excluded.

5. Define the target
6. Specify the required execution settings
7. Click **Deploy**

You have created configurations to secure USB devices. These configurations will be applied when the user logs in to the computer.

Excluding Devices

When you block a device you can exclude certain devices from being blocked. This can be done, by using Vendor ID or the Device Instance ID assigned to each device. You can exclude devices only when you have blocked a device. To exclude devices, follow the steps given below:

1. Click the **Exclude Devices** link against a device
2. You can also choose to block all the devices, from the specified **vendor**. You will have to specify the Device Instance ID using which, Desktop Central will fetch the vendor instance ID and exclude all devices from the specific vendor.
3. You can choose to exclude **All Encrypted devices/encrypted devices from the list of specified devices.** Devices that are encrypted using BitLocker can be added to the exclusion list.
4. Click **Close**

You have excluded a device from being blocked.

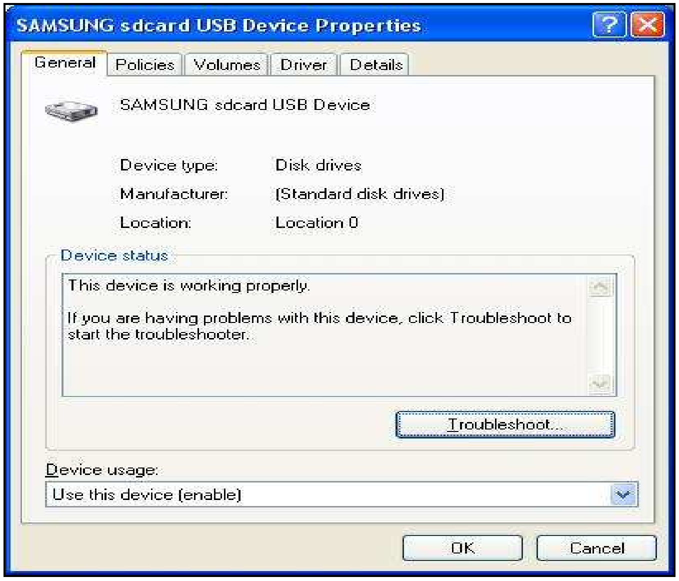
Device Instance ID

Every USB device has a unique ID. This ID is assigned to devices by the system to identify them easily. You can identify the Device Instance ID of a Device by following the steps mentioned below:

a. Right click on **My Computer**
b. Click on **Properties**
c. Click on **Device Manager** (Refer to the figure below)
d. From the list of devices, expand the list of devices for which you want the Device Instance ID.

   (For example : if you want to identify the Device Instance ID of a mobile phone that you have connected to the computer, expand portable devices and follow the next step.)
e. Right-click on the name of a specific device and click **Properties** (Refer to the

figure below)



SAMSUNG sdcard USB Device

Device type: Disk drives

Manufacturer: (Standard disk drives)

Location: Location 0

Device status

This device is working properly.

If you are having problems with this device, click Troubleshoot to start the troubleshooter.

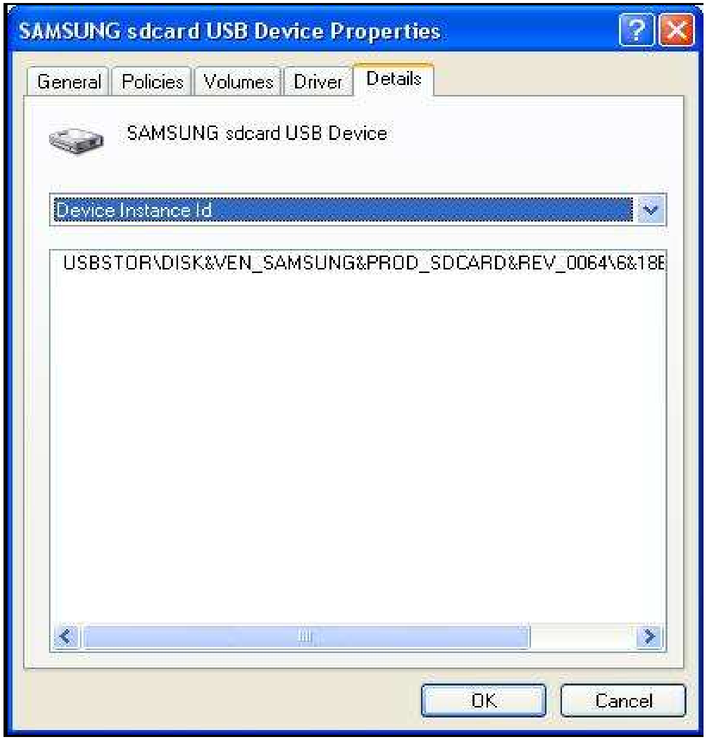
Device usage:

Use this device (enable)

Figure 2: Properties

i. Click the **Details** tab

ii. In the drop-down box, select **Device Instance ID** or Device Instance Path (Refer to the figure below)



SAMSUNG sdcard USB Device

Device Instance Id

USBSTOR\DISK&VEN_SAMSUNG&PROD_SDCARD&REV_0064\6&18E

Figure 3: Device Instance ID

In computers which have the operating system Windows Vista (and later versions), the Device Instance ID is called the **Device Instance Path**. You can copy the Device Instance Path from the Properties property sheet of the Device Manager.

In computers that have older versions of the Windows operating system installed in them, you cannot copy the Device Instance ID directly from the Properties property sheet of the Device Manager.

To copy the Device Instance ID you must open the dcusbaccess log file. This file is located in **<Drive>\<Desktopcentral_Agent Folder>\logs\dcusbaccess.log.** It contains information about the following:Action Time (inserted\removed time)

- Action (inserted\removed)
- Friendly name
- Device Instance ID

You can now view and copy the Device Instance ID for a specific device.

Revoking All USB Restrictions applied to the Computer

Administrators can choose to revoke all USB related restrictions which are applied to the computer.

To create a configuration, in order to revoke all USB related restrictions for users, follow the steps given below:

1. Navigate to **Configurations** tab and choose **Secure USB** configuration from the list of Windows configurations.
2. Enter a name and description for the configuration.
3. Click **Remove** to revoke all restrictions applied to the computer.
4. Define the target
5. Make the required execution settings.
6. Click **Deploy.**

You have created configurations to secure USB devices. These configurations will be applied when the user logs in to the computer.

Configuring Security Policies

Description

The Security Policies Configuration is basically a bunch of security settings to specify the security and restrictions.

Step 1: Name the Configuration

Provide a name and description for the Security Policies Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Choose Policy Category	The specific policy area in which the security policy will be applied. Select the desired category and this would display the relevant security polices. For details on the each policy, refer Security Policies.
Policy Value	To enable, disable, or to leave it unconfigured, select the appropriate option.

1. To modify a security policy from this table, select the appropriate row, click 📝 icon and change the required values.
2. To delete a security policy from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Security Policies Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Security Policies Configuration in the targets defined. The security policies will be applied during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Executing Custom Scripts

Desktop Central provides options for configuring almost all the computer configurations. In addition to the configurations that are supported by Desktop Central, administrators can also write their own scripts that could be run on the machines for accomplishing specific configurations. The scripts could be any of the following formats:

- Batch file (.bat or .cmd)
- In any other language hosted by Windows Script Host (WSH), such as VB Script, JScript, Perl, REXX, and Python.

Note: The script engines for languages like Perl, REXX, and Python, must be registered with Windows. You can also execute single line commands, add dependent files and enable logging, to analyze the output of the script after execution.

Step 1: Name the Configuration

Provide a name and description for the Custom Script Configuration.

Step 2: Define Configuration

The table given below lists the parameters that have to be provided for defining the configuration.

Parameter	Description

Execute Script from	You can execute the script either from repository or as a command line.
Script Name*	The script that has to be added/removed in the machines needs to be chosen from the script repository. It is mandatory to add the script to the script repository for this to work.
Script Arguments	The arguments that have to be provided while executing the scripts.
Dependency files	The required dependency files for execution of the script needs to be added.
Exit Code	Specify the exit code, which should be returned, when the script has been executed successfully
Frequency	Specify the frequency for this script to be executed, like only once, during every system startup, during subsequent system startup for specified number of times or all system startup until a specified time period.
Run As	The script can be executed either as system user or any specific user who holds an account. In the latter case, credentials need to be furnished.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Custom Script Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Custom Script Configuration in the targets.

To save the configuration as draft, click **Save as Draft**.

Setting Environment Variables

- Name the Configuration
- Defining Configuration
- Defining Target
- Deploy Configuration

Environment variables are strings that contain information about the environment for the system, and the currently logged on user. Some software programs use the information to determine where to place files (such as temp, tmp, path etc). Environment variables control the behavior of various programs. Any user can add, modify, or remove a user environment variable. However, only an administrator can add, modify, or remove a system environment variable. Using Desktop Central, the environment variables can be defined and added.

Step 1: Name the Configuration

Provide a name and description for the Environment Variable Configuration.

Step 2: Define Configuration

The following table lists the parameters that have to be specified**:**

Parameter	Description
Variable*	The environment variable name that has to be modified or added.
Value*	The value that has to be stored in the environment variable. Click the ☆ icon to select and assign a dynamic variable to this parameter.

* - denotes mandatory fields

1. To add more environment variables, click **Add More Variables** and repeat Step 2. The defined environment variable gets added to the **List of Environment Variable** table.
2. To modify a environment variable from this table, select the appropriate row, click ✎ icon and change the required values.

3. To delete a environment variable from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Environment Variable Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Environment Variable Configuration in the targets defined. The configurations will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Configuring IP Printer

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

The IP Printer Configuration is for adding or deleting the IP Printer connection in computers. For configuring a shared network printer in the computer for specific users, refer the Configuring Shared Printer.

Step 1: Name the Configuration

Provide a name and description for the IP Printer configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add an IP Printer
- Delete an IP Printer

Add an IP Printer

To add an IP Printer, select the **Action** as *Add* and specify the following values:

Parameter	**Description**
DNS Name/IP	The host name or IP address defined for the printer. *Example*: `192.111.2.32`
Printer Name	The display name for the printer.

Protocol	The printing protocol supported by the printer. Select the printing protocol from the Protocol list box. The default option is "RAW".
Port Number	The port number/queue name in which printing protocol is communicating between the computer and printer. Enter the port number in the Port Number field if the "RAW" Protocol is selected or enter the queue name if the "LPR" Protocol is selected. The default value is 9100.
Port Name	This is an optional field. By default, the port name is IP_<IP_Address/DNS_Name>. You can change the port name if required.
Shared Printer for Driver Installation	Browse to select a shared printer for installing the driver. If the drivers are already installed in the target computers, then Desktop Central will skip the driver installation.
Connect Shared Network Printer using Credentials	To copy Driver Files across Domains or amongst Workgroup computers, you need to specify a credential that has access to domain/workgroup machine where the Shared Printer Driver Files are present.
Add New Driver Package	A Driver Package includes all the software installables required to configure your printer. Add the Driver Package that is bundled along with your printer or download your model specific package from the vendors website and add here.
Use Pre-Installed Driver	If you have already installed a driver in all your target computers, you can use the driver to configure the IP printer.To find the driver name navigate to Devices and Printers -> right click on a Printer -> Advanced option in Printer properties.

Delete an IP Printer

To delete an IP Printer, select the **Action** as *Delete* and specify the following values:

Parameter	**Description**
Printer Name	The display name of the printer.
Delete all existing IP printer connections	To delete all the existing IP printer connections in the computer for the specified user, select this option.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the IP Printer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined IP Printer Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

EXE Packages

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The Software Installation configuration helps you to install MSI and EXE packages remotely to several computers of the Windows network from a central location.

Step 1: Name the Configuration

Provide a name and description for the Software Installation Configuration.

Step 2: Define Configuration

You have an option to install either an EXE or an MSI package

1. Install MSI Package
2. Install EXE Package

Install MSI Package

Select the Installer type as **MSI** and specify the following values:

Parameter	**Description**
MSI Package Name	This will list all the MSI packages that are available in the Software Repository. Select the MSI that has to be installed.

Operation Type	To specify how the installation should happen. Select any of the following options: 1. *Install Completely:* Selecting this option will install the application automatically. 2. *Advertise*: Selecting this option will notify the user about the availability of the software. Thy can choose whether to install the software or not. 3. *Remove*: Selecting this option remove (uninstall) the application from the system
Install as	The user as whom the MSI has to be installed. *System User:* Default system user privilege *Run as User:* User Account with specific privilege
User interaction	You can choose to allow the user to interact with the installation/uninstallation window. This comes handy when a few applications require user intervention and cannot be installed/uninstalled silently.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	**Description**

Schedule time to perform the operation	● Select this option and specify the date and time after which the installation should begin. It is to be noted that the installation/uninstallation will still be based on the Operation Type & Installation / Uninstallation Option selected, but this will begin after the time specified here. ● Set an expiry date: Enable the checkbox if you do not wish to apply this configuration after a specified time period.

Specify the Deployment Settings for the software:

If you have defined Deployment Templates, you can load the Deployment Settings directly from a template by selecting the required template from the list.

Parameter	**Description**
Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after system startup: 1. *During startup*: Select this option if the software has to be installed/uninstalled during computer startup. 2. *After startup*: Select this option if the software has to be installed/uninstalled after the computer startup when the next GP update happens (within 90 minutes) 3. *During or After Startup*: Either of the above, whichever is earlier
Install Between	If you want the installation to happen only between a specified time of a day, you can specify the Start and End time within which the deployment should begin. The Start Time can also be greater than the End time - in such cases the End time is assumed to be on the following day. For example, if you wish the deployment should happen between 10.00 PM and 4.00 AM, you can specify the Start Time as 22:00:00 and End Time as 04:00:00

Allow Users to Skip Deployment	Specify whether the use can skip the deployment at a later time by selecting the "Allow Users to Skip Deployment". When you do not select this option, the deployment will be forced and the user will not have any control on the deployment. When you allow users to skip deployment, you can also specify whether they can skip it as long as they wish or force deployment after a specific date.
Reboot Policy	1. *Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. 2. *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to be displayed in the client machines. This option is applicable if the computer is turned on and even if there is no logged on user, the computer will get restarted after the specified time. 3. *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to be displayed in the client machines. This option is applicable if the computer is turned on and even if there is no logged on user, the computer will get restarted after the specified time. 4. *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to be displayed in the client machines. 5. *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to be displayed in the client machines.

Install EXE Package

Select the Installer type as **EXE** and specify the following values:

Parameter	**Description**
EXE Package Name	This will list all the EXE packages that are available in the Software Repository. Select the EXE that has to be installed.
Operation Type	To specify how the installation should happen. Select any of the following options: 1. *Install Completely:* Selecting this option will install the application automatically. 2. *Advertise*: Selecting this option will notify the user about the availability of the software. Thy can choose whether to install the software or not. 3. *Remove*: Selecting this option remove (uninstall) the application from the system
Install as	The user as whom the EXE has to be installed. *System User:* Default system user privilege *Run as User:* User Account with specific privilege
User interaction	You can choose to allow the user to interact with the installation/uninstallation window. This comes handy when a few applications require user intervention and cannot be installed/uninstalled silently.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Include Hidden Files	

Specify the Scheduler details for installing the software:

Parameter	**Description**
Schedule time to perform the operation	● Select this option and specify the date and time after which the installation should begin. It is to be noted that the installation/uninstallation will still be based on the Operation Type & Installation / Uninstallation Option selected, but this will begin after the time specified here. ● Set an expiry date: Enable the checkbox if you do not wish to apply this configuration after a specified time period.

Specify the Deployment Settings for the software:

If you have defined Deployment Templates, you can load the Deployment Settings directly from a template by selecting the required template from the list.

Parameter	**Description**

Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after system startup: 1. *During startup*: Select this option if the software has to be installed/uninstalled during computer startup. 2. *After startup*: Select this option if the software has to be installed/uninstalled after the computer startup when the next GP update happens (within 90 minutes) 3. *During or After Startup*: Either of the above, whichever is earlier
Install Between	If you want the installation to happen only between a specified time of a day, you can specify the Start and End time within which the deployment should begin. The Start Time can also be greater than the End time - in such cases the End time is assumed to be on the following day. For example, if you wish the deployment should happen between 10.00 PM and 4.00 AM, you can specify the Start Time as 22:00:00 and End Time as 04:00:00
Allow Users to Skip Deployment	Specify whether the use can skip the deployment at a later time by selecting the "Allow Users to Skip Deployment". When you do not select this option, the deployment will be forced and the user will not have any control on the deployment. When you allow users to skip deployment, you can also specify whether they can skip it as long as they wish or force deployment after a specific date.

Reboot Policy	1. *Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. 2. *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to be displayed in the client machines. This option is applicable if the computer is turned on and even if there is no logged on user, the computer will get restarted after the specified time. 3. *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to be displayed in the client machines. This option is applicable if the computer is turned on and even if there is no logged on user, the computer will get restarted after the specified time. 4. *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to be displayed in the client machines. 5. *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to be displayed in the client machines.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Windows Installer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Windows Installer Configuration in the defined targets. The software installation for the selected targets will happen as scheduled.

To save the configuration as draft, click **Save as Draft**.

Setting Path

Path is an environment variable that contains the path prefixes that certain applications, utilities, and functions use for searching an executable file. The Path Configuration enables you to add path prefixes to this variable.

Step 1: Name the Configuration

Provide a name and description for the Path Configuration

Step 2: Define Configuration

Specify the path to be added to the environment variables. Multiple paths can be specified separated by a semi-colon (**;**). Click the ☆ icon to select and assign a dynamic variable to the Path variable.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Path Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Path Configuration in the targets defined. The configurations will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Power Management for Computers

The Power Management Configuration enables you to adjust your power settings to save energy. You can add, modify, and delete power schemes for computers from a central point. You can cut down the cost that is spent on power, when the computers are idle. You can create customized power schemes and apply it to computers via configurations.

Desktop Central supports power management only for computers running Windows Vista and later versions. You can perform the following operations on idle computers by creating power schemes:

Action to be performed	**Impact on the target**
Dim the Display	Only the computer display's brightness will be reduced to save power.
Turn Off the display	Computer's display will be turned off and the power consumption will be reduced reasonably
Turn Off to Sleep	Computer turns to standby mode, all working files/data will be stored on memory. Power consumed will be relative very low
System Hibernate	All working files/data will be stored on the hard disk and turns off the computer. Zero power is consumed
Turn Off Hard disk	Only the hard disk will be turned off, computer will not be shutdown. Power consumption will be cut down considerably
Hybrid Sleep* (applicable for Windows 7 and later versions)	All working files/data will be stored on the hard disk and the computer turns to sleep. Assume a computer has turned off without power, it still restores the working files and resumes back to work, when it is boot up the next time.

The above listed operations can be executed on the computers based on the idle time and mode of power supply such as plugged in and battery mode. After customizing the power schemes, you can choose to apply the power scheme as follows:

- **Overwrite the existing power schemes** with the latest one, that you have created. If more than one power scheme exists with the same name, you can choose to overwrite the previous one with the latest.
- **Set the newly created power scheme as active power scheme**, if you do not set it as

active, then the power scheme will be deployed to the computer. You will have to apply/activate it manually for the power scheme to work.

- You can choose to **enable**, **support for hibernate**. If you do not enable support for hibernate, then the option to hibernate will not work, even if it is specified in the power scheme.
- You can choose to **enable hybrid sleep** for computers, running Windows 7 and later versions. "Hybrid sleep" can be applied for computers, running Windows 7 and later versions. It stores all data and working documents on the hard disk and turns the computer to sleep, which means the power consumed is relatively less. Assume a computer has turned off without power, it still restores the working files and resumes back to work, when it is boot up the next time.

You can create/modify/delete power schemes using Desktop Central. By clicking on configurations tab, on Desktop Central web console, you can choose power management configuration. You can choose to create customized power schemes or modify the default power schemes provided by the operating system. Windows provides, three schemes such as Balanced, High Performance and Power Saver schemes. If you wish to delete a power scheme, you will have to specify the name of the power scheme and deploy it to the target computers.

You can execute advanced options like:

- Prompting for password, when the computer resumes from sleep
- Actions which needs to be performed, when the laptop's lid is closed
- Actions to be performed, when the power button is pressed
- Actions to be performed, when the sleep button is pressed

These actions can be customized, based on the mode of power, like plugged in mode or when it runs on battery.

Modify/Delete power schemes

You can choose to modify either the user defined scheme or default scheme. The remaining setting are the same as that of creating a new scheme. If you wish to delete a scheme, just specify the name of the scheme.

Configuring Registry Settings

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

The Registry Settings allows you to change the values in the registry in the workstations. Desktop Central Registry Settings Configuration enables you to modify the registry values from a central location.

Step 1: Name the Configuration

Provide a name and description for the Registry Settings Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Write Value
- Delete Value
- Add Key
- Delete Key

Write Value

To write a value to the registry, select the **Action** as *Write Value* and specify the following:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value.

Type	The type of the value. This varies with respect to the Header Key selected. Select the appropriate type from the combo box.
Value*	Specify the value to be added.
Data / Expression*	Specify the data or expression. If the new value has to be created without data, enter the word clear inside the parentheses as (clear).

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.
If you wish to write more values, click **Add More Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Value

To delete a value from the registry, select the **Action** as *Delete Value* and specify the following values:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value.
Value	Specify the value to be deleted.

If you wish to delete more values, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Add Key

To add a registry key, select the **Action** as *Add Key* and specify the following:

Parameter	Description
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.

Key	Keys are sub-components of the hives. Specify the key value to be added.

If you wish to add more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Key

To delete a registry key, select the **Action** as *Delete Key* and specify the following values:

Parameter	**Description**
Header Key	Select the header key or hive as HKEY_LOCAL_MACHINE.
Key	Keys are sub-components of the hives. Specify the key value that has to be deleted.

If you wish to delete more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

To modify a registry setting from the **Registry Settings** table, select the appropriate row and click ✎ icon and change the required values.

To delete a registry setting from the **Registry Settings** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Registry Settings Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Registry Settings Configuration in the targets defined. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Scheduling Tasks

The Windows Scheduler Configuration enables you to schedule any program, task or a script to run at a specified time. You can also schedule a task to be executed daily, weekly, monthly , etc. This configuration enables you to add and modify tasks from a central point.

Step 1: Name the Configuration

Provide a name and description for the Scheduler Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create/Modify a Task
- Delete a Task

Create/Modify a Task

To create a new task, select the **Create Task** tab of the Scheduler Configuration. Select the **Modify Task** tab to modify an existing task. Specify the following values:

Parameter	**Description**
Name of the task*	The name of the task that has to be created/modified.
Overwrite if task already exits	Select this option to overwrite the task, if one with the same name exists. This option is only available for create task.

Application Name*	The application or the program that has to be run. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Arguments	The arguments to run the program, if any. Click the ☆ icon to select and assign a dynamic variable to this parameter.
General	● *Enabled*: Select this option to run the task at the specified time. ● ● *Run only when logged on:* Select this option to run the task only when the user has logged on. ●
User Name*	The name of the user as whom the task will be run. Click the ☆ icon to select and assign a dynamic variable to this parameter, for example, $DomainName\$DomainUserName or $ComputerName\$DomainUserName.
Password	The password of the user.
Confirm Password	Confirm the password again.
Run only when the user is logged on	Enable this option to perform the task only when the target user runs the task
Run whether the user is logged on or not	Enable this option to perform the task irrespective of the target user logged on or logged off
Run with highest privileges	Enabling this option allows the target user with highest privileges to run the task

Scheduled Task Completed	● *Delete the task if it is not scheduled to run again:* Select this option to delete the task when it is no longer scheduled. ● *Stop Task:* Select this option and specify the duration after which the task will be stopped.
Trigger	
Perform this task*	Specify the time to perform the task. You can select from the following options: ● *Daily:* To run the task daily. Specify the time and duration to run the task. ● *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run. ● *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months. ● *Once:* To run the task only once. You need to specify the date and time. ● *At System Startup:* To run the task when the system is started. ● *At Logon:* To run the task during the user logon. ● *When Idle:* To run the task when the system is idle for the specified time.
Delay task for	Specify the time duration for which the task needs to be delayed. It can be delayed for a maximum of 31 days.
Repeat the task	Specify the time interval and duration for which the task needs to be executed repeatedly.
Expiry Date	Specify the expiry date of the task

Conditions	
Idle Time	Select the required options: ● Specify the duration,the system has to be idle before starting a task. ● Stop the task if the computer ceases to be idle
Power Management	Select the required options: ● Don't start the task if the computer is running on batteries ● Stop the task if battery mode begins ● Wake the computer to run this task

* - denotes mandatory parameters

If you wish to create/modify more tasks, click **Add More Task** button and repeat step 2. The defined task gets added to the **Task** table.

When a wrong password is provided for tasks scheduled in Win2k / WinXP SP1 machines, the tasks will be successfully created, but will not be executed.

Delete a Task

To delete a task, select the Delete Task tab of the Scheduler Configuration and specify the name of the task that has to be deleted.

Modify a Task

To modify a task select the Modify Task tab of the Scheduler Configuration and specify the name of the task that has to be modified, along with the application name and arguments.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Scheduler Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Scheduler Configuration in the defined targets. The scheduler configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Configuring Windows Services

Applications that have to be run automatically whenever the system starts can be configured to run as a Windows service. However in certain cases, after installing an application as a service, you may wish to change the startup type or delete the service. The Service Configuration enables you to change the settings for the services available in the **Control Panel -> Administrative Tools -> Services**.

Step 1: Name the Configuration

Provide a name and description for the Service Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Service Name	Select the name of the service from the combo box. The combo box contains the list of standard Windows services. If the required service is not listed, click **Add Custom Service** to either select the service from the Additional Services list or add your own by giving the required details.
Action	Specify the action to be performed from the following: ● Don't Modify: To preserve the client settings. This option is selected by default. ● Start: Select this option to start the service. ● Stop: Select this option to stop the service.

	● Restart: Select this option to restart the service.
Service Startup Type	Select how the service should be started from the following options: ● Don't Modify: To preserve the client setting. ● Manual: Select this option if the service has to be manually started after the system startup. ● Disabled: Select this option to disable the service. ● Automatic: Select this option to automatically start the service along with the system. ● Automatic (Delayed) : Select this option to automatically start the service when the system starts, with a delay.

1. To add more services, click **Add More Service** and repeat Step 2. The service gets added to the **Services** table.
2. To modify a service from this table, select the appropriate row, click ✎ icon and change the required values.
3. To delete a service from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Service Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Service Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Managing Shortcuts

1. Name the Configuration
2. Define Configuration
3. Define Target
4. Deploy Configuration

The shortcut is an icon that points to a file, folder or an Internet URL. The Shortcut Configuration enables you to add shortcuts to the computers from a central point.

Step 1: Name the Configuration

Provide a name and description for the Shortcut Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create a Shortcut
- Create an Internet Shortcut
- Delete a Shortcut / Internet Shortcut

Create a Shortcut

To create a shortcut, select the **Action** as *Create Shortcut* and specify the following values:

Parameter	**Description**
Shortcut Name*	Specify the name of the shortcut.

Target Application*	Browse and select the target application from the network for which a shortcut has to be created. The target application can also be in the local machine where the configuration is being deployed.
Arguments*	If the application requires any arguments, specify the arguments. Leave it blank if it does not require any arguments.
Shortcut Location	Select the location to create the shortcut. The shortcut location can be any of the following: ● *All Users Desktop*: Refers to the desktop common for all the users. ● *All Users Start Menu*: Refers to the start menu common for all users. ● *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. ● *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.
Start In Folder*	Some applications may have some references to additional files during execution. In such cases, browse and select the location from where the application has to be started.
Shortcut Comments	Specify the comments for this shortcut.
Icon File*	Browse and select the icon for the shortcut.
Run Window	Select how the application has be started - *Normal*, *Maximized*, or *Minimized*.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note: If you wish to create more shortcuts, click **Add Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

Create an Internet Shortcut

To create an Internet shortcut, select the **Action** as *Create Internet Shortcut* and specify the following values:

Parameter	**Description**
Shortcut Name*	Specify the name of the Internet shortcut.
Target URL*	Specify the URL for which the shortcut needs to be created.
Shortcut Location	Select the location to create the shortcut. The shortcut location can be any of the following: ● *All Users Desktop*: Refers to the desktop common for all the users. ● *All Users Start Menu*: Refers to the start menu common for all users. ● *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. ● *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.
Icon File*	Browse and select the icon for the shortcut.

Delete a Shortcut / Internet Shortcut

To delete a shortcut, select the **Action** as *Delete Shortcut / Delete Internet Shortcut* respectively and specify the following values:

Parameter	Description
Shortcut Name	Specify the name of the shortcut. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Shortcut Location	Select the location from where the shortcuts needs to be deleted. The shortcut location can be any of the following: ● *All Users Desktop*: Refers to the desktop common for all the users. ● *All Users Start Menu*: Refers to the start menu common for all users. ● *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. ● *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.

Note: If you wish to delete more shortcuts, click **Add More Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

To modify a shortcut from the **Shortcut** table, select the appropriate row and click ✎ icon and change the required values.

To delete a shortcut from the **Shortcut** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Shortcut

Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Shortcut Configuration in the defined targets. The shortcut configuration will take effect during the next system start up.

To save the configuration as draft, click **Save as Draft**.

Configuring WiFi

WiFi profiles can be configured for all the managed Windows devices in your network in one-shot using Desktop Central. You can now create, modify or delete WiFi configurations seamlessly. Desktop Central supports WiFi configurations only for computers running Windows Vista or later version. You can choose to remove all the existing WiFi profiles and apply newly created WiFi profiles. You need to ensure that the WiFi adapter is enabled on all the target computers for deploying a WiFi profile. You can turn on the WiFi adapter while creating a new WiFi profile.

- Creating WiFi Profiles
- Modifying WiFi Profies
- Deleting WiFi Profiles

Multiple Profiles can be added in a single configuration, which includes options for creating, modifying and deleting WiFi profiles. Profiles within a configuration will be applied as per the sequence it is specified. If you have chosen to delete all configurations first, then all the existing WiFi profiles will be removed from the computer and then the second profile will be added.

Creating WiFi Profiles

You can create one or more WiFi profiles for the target computer. You can choose to remove all the existing WiFi profiles before deploying the newly created profiles. You will have to follow the steps mentioned below to create a WiFi profile. There are two ways to create a WiFi profile, they are :

- Creating a new profile
- Importing from an existing profile

Creating a new profile:

You will have to provide the following details

- Profile Name : Name for the WiFi configuration

- Security Type : No Authentication / WEP / WEPA2 Personal / WPA Personal / WPA2 Enterprise / WPA Enterprise / 802.1x
- Encryption Type : Specify the encryption type as required
- Security type 802.1x is considered to be more secure than WPA and WEPA2 Personal.
- You can also choose to connect the WiFi that you have configured automatically
- Establish connection even if the network is not broadcasting
- Choose to overwrite if any existing profiles exists with the same name

Importing from an Existing Profile

You can choose to import an existing WiFi profile and deploy the same to the target computers. WiFi profile should be located and uploaded in the Desktop Central server. Desktop Central currently supports WiFi profiles only in xml format.

Modifying the WiFi Profiles

You can choose to modify the existing WiFi profiles by creating a new profile with the required modifications. When a profile is created with a name which already exists on the target computer, then the previous profile will be modified, however the changes will apply only to the computers to which the configuration is applied. Modifying WiFi profiles will not work, if the network adopter is disabled on the device.

Deleting WiFi Profiles

You can choose to delete one or all the WiFi profiles that exists on the target computer. When Delete All profile is applied, all the existing WiFi profiles applied to computers will be removed from the target computer and the newly added profiles will be applied. You can choose to delete a specific profile by specifying the name of the profile which needs to be deleted.

Common Folder Redirection

The Common Folder Redirection Configuration helps to change the location of the All User Shell folders that are shared by all the users. The All User Shell folders contain common Start Menu, Programs Group, Startup Group, Desktop and application data shared by all the users. For the redirection of the user-specific folders in the computer, refer Redirecting User-Specific Folders.

Step 1: Name the Configuration

Provide a name and description for the Common Folder Redirection Configuration.

Step 2: Define Configuration

Select the values for the following fields that require change in settings. For each of the fields in the following table, click the Browse button next to the corresponding field to launch Network Browser window. Select the folder location and click OK button. If this field is left blank, the corresponding folder settings is left unchanged.

The following table provides a brief description about the common folders that can be redirected using Desktop Central.

Field	**Description**
Common Start Menu*	Contains the shortcuts that appear in the start menu that are common for all the users of the computer.
Common Programs Group*	Contains the shortcuts that appear in the Programs group of the start menu that are common for all the users of the computer.

Common Startup Group*	Contains the shortcuts that appear in Start --> Programs --> Startup menu. This specifies the applications that should be started during the startup of the system.
Common Desktop*	Contains the shortcuts and files that appear in the desktop that are common for all the users of the computer.
Common Application Data*	Contains the application data that are shared by all the users (C:/Documents and Settings/All Users/Application Data).

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Common Folder Redirection Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Common Folder Redirection Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click Save as Draft.

Display Configuration for Computer

The Display Configuration is for configuring the display settings of Windows desktops by customizing the primary and secondary display resolution. In addition to this, the DPI settings for font can be set.

Step 1: Name the Configuration

Provide a name and description for the configuration.

Step 2: Define Configuration

The table below lists the display settings that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
Wallpaper	
Primary Display Resolution (this is not supported for virtual machines or when a machine is being accessed from a remote computer)	Specify one of the following action: ● Retain Existing Settings - Will not make any changes to the existing settings ● Specify the resolution from the drop down or choose custom to customize it

Secondary Display Resolution (this is not supported for virtual machines or when a machine is being accessed from a remote computer)	Specify one of the following action: ● Retain Existing Settings - Will not make any changes to the existing settings ● Specify the resolution from the drop down or choose custom to customize it
Font DPI	Specify one of the following action: ● Retain Existing Settings - Will not make any changes to the existing settings ● Specify the font DPI to be displayed as 100 % /125% / 150 % / 200 %
Font Files	Choose the upload type as "Network Share" or "HTTP upload" to upload the font files.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Display Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Display Configuration in the targets defined.

The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Managing Files and Folders

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

The File and Folder Operation allows you to copy, move, rename, delete files and folders in computers. Desktop Central File and Folder Operation Configuration enables you to copy/move/delete files for several computers from central location.

Step 1: Name the Configuration

Provide a name and description for the File and Folder Operation configuration.

Step 2: Define Configuration

You can perform the following actions:

- Copy Files and Folders
- Rename/Move Files and Folders
- Delete Files and Folders

Copy Files and Folder

To copy files and folders, select the *Copy* tab and specify the following values:

Parameter	**Description**

Select Action Type	Select the Action from any of the following for HTTP : ● *Files* ● *Files as archive* Select the Action from any of the following for network share: ○ *Copy a File* - To copy a file from one location to another ○ *Copy a File to a Folder* - To copy a file from one location to a specified folder ○ *Copy Multiple Files* - To copy multiple files to a specified folder ○ *Copy a Folder* - To copy a folder from one location to another
Source File	Specify the file that has to be copied. The file can either be in a shared location or in the specified location in the client machines.
Destination Folder	Specify the destination location to copy the files/folders.
Overwrite Existing Files	Select this option to overwrite the existing files.
Create Destination Directory if doesn't Exist	Select this option to create the destination directory, if it does not exist.
Modified, Created, Accessed	Select this option to specify the modified, created or accessed details of the file/folder.

If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Rename/Move Files and Folders

To rename or move the files and folders, select the *Rename/Move* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: ● Rename/Move a file ● Rename/Move a folder
Source File/Folder	Specify the file or the folder that has to be copied
Destination File/Folder	Specify the destination file or the folder.

If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Delete Files and Folders

To delete the files and folders, select the *Delete* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: ● Delete a File ● Delete Multiple Files ● Delete a Folder
Source File	Specify the files/folders that has to be deleted
Include Read Only Files	Select this option, if you wish to copy the files even if it has only read-only permissions
Include System Files	Select this option if you wish to copy the system files.

Include Hidden Files	Select this option if you wish to copy the hidden files.
Modified, Created, Accessed	Select this option to specify the modified, created or accessed details of the file/folder.

To modify a file action from the **List of File Actions** table, select the appropriate row and click ✎ icon and change the required values.

To delete a file action from the **List of File Actions** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the File and Folder Operation Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined File and Folder Operation Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Installing Fonts

This document will explain the steps involved in installing fonts for computers. Administrators can choose to install specific fonts for specific computers. Applying this configuration will restrict the computers to use specific fonts. Administrators can remotely install the font files to computers which are located in different geographic locations.

Adding Fonts

The following steps will explain on deploying "Fonts" to computers:

1. Navigate to Configurations tab and choose Font Configuration from the list of Windows configurations.
2. Specify the name and description for the configuration.
3. Click on the Add option. Upload font files that need to be deployed to the target computers. You can select multiple font files at a time by pressing ctrl/shift + select the files.

Ensure that the font file is in .ttf, .otf, .fon and .zip format.

4. Define the target computers.
5. Specify retry options if required and deploy the configuration.

You have successfully created a configuration to deploy fonts to computers.

Removing Fonts

The following steps will explain on removing "Fonts" deployed to computers:

1. Navigate to Configurations tab and choose Font Configuration from the list of Windows configurations.
2. Specify the name and description for the configuration.
3. Click on the Remove option. Specify the font files that need to be removed from the target computers. You can choose to remove one or more fonts which were deployed using Desktop Central. You can also remove fonts which were not deployed using Desktop Central.
4. Define the target computers.
5. Specify retry options if required and deploy the configuration.

You have successfully created a configuration to remove fonts from computers.

Configuring General Computer Settings

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

Description

This configuration is for defining the general settings of the computers in your network, such as displaying the last user name & synchronizing the system time with the time zone.

Step 1: Name the Configuration

Provide a name and description for the General Configuration.

Step 2: Define Configuration

The table below lists the general settings that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
Display last User Name	To specify whether to display the previously logged user name or not. This is displayed when a user logs on to the system. To leave it unchanged, select *Preserve client settings* option.
Registered Owner*	The name of the registered owner of the system. This is displayed in the General tab of the My Computer properties window.
Registered Company*	The name of the company. This is displayed in the General tab of the My Computer properties window.

Time Server	Browse and select a time server to synchronize the time of the computer with of the time server. Time synchronization happens when the computer starts.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the General Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined General Configuration in the defined targets. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Managing Windows Local Groups

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

The Group Management allows you to add, modify, or delete local groups from the computers.

Step 1: Name the Configuration

Provide a name and description for the Group Management Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add Group
- Delete Group
- Modify Group

Add Group

To add a group to the computer, select the **Add Group** link from the Choose Group Action table and specify the following:

Parameter	**Description**
Group Name	The name of the group that has to be created.
Description	The description of the group.

Add Member	Select the Member Type as Local, Domain User, or Domain Group and specify/select the users or global groups that have to be added to the local group.
Overwrite if group already exist	Select this option, if you wish to overwrite the group definition, if one with the same name exists.

If you wish to add more groups or to perform another action, click **Add More Actions** button and continue. The values gets added to the **List of Settings** table.

Delete Group

To delete a group from the computer, select the **Delete Group** link from the Choose Group Action table and specify the group name that has to be deleted.

If you wish to delete more groups or to perform another action, click **Add More Actions** button and continue. The values gets added to the **List of Settings** table.

Modify Group

To modify a group of the computer, select the **Modify Group** link from the Choose Group Action table and specify the group name that has to be deleted.

Parameter	**Description**
Group Name	The name of the group that has to be modified.
Description	The description of the group.
Add Member	Select the Member Type as Local, Domain User, or Domain Group and specify/select the users or global groups that have to be added to the local group.
Remove Member	Select the Member Type as Local, Domain User, or Domain Group and specify/select the users to be removed from this group.

If you wish to modify more groups or to perform another action, click **Add More Actions** button and continue. The values gets added to the **List of Settings** table.

To modify a setting from the **List of Settings** table, select the appropriate row and click 📝 icon and change the required values.

To delete a setting from the **List of Settings** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Group Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Group Management Configuration in the targets defined. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Displaying Legal Notices

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

Be it important announcements or displaying legal notices, it can be configured easily throughout the enterprise using Desktop Central's Legal Notice configuration. The configured message will be displayed whenever the user presses ctrl+alt+del to login.

Step 1: Name the Configuration

Provide a name and description for the Legal Notice Configuration.

Step 2: Define Configuration

Specify the following:

Parameter	Description
Action	Choose the appropriate action to either create/modify or remove a legal notice
Window Title*	Specify the window title of the legal notice.
Message*	Specify the message that has to be displayed.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Legal Notice

Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Legal Notice Configuration in the defined targets. The configured legal notice will be displayed during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Displaying Message Box

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

For the computers in the network, the pop-up messages with the warning or error can be displayed during the system startup. If the system is already running while deploying this configuration, the message will be displayed during the system restart.

Step 1: Name the Configuration

Provide a name and description for the Message Boxes Configuration.

Step 2: Define Configuration

You have an option to create a new message box or delete the existing message box. Select the required option and specify the following:

Parameter	Description
Message Type	The message type as Information, Warning, or Error.
Window Title	The title of the message box.
Message	The message that has to be displayed.
Timeout in Seconds	The duration, in seconds, for the message display.
Frequency	Specify at what frequency you want the message box to be displayed - once, during every logon, during subsequent logon or during every logon until a specified time.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Message Boxes Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Message Boxes Configuration in the targets defined. The message will be displayed during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Managing Windows Local Users

- Name the Configuration
- Define Configuration
- Define Target
- Deploy Configuration

The User Management allows you to add, modify, or delete local users from the computers.

Step 1: Name the Configuration

Provide a name and description for the User Management Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add User
- Change Password
- Remove User
- Modify User

Add User

To add an user to the computer, select the **Add User** link from the Choose User Action table and specify the following:

Parameter	**Description**
User Name	The user name for the user to be created.
Full Name	The full name of the user.
Description	The description for this user.

Password	The password for this user.
Confirm Password	Confirm the password again.
Overwrite if user already exist	Select this option to overwrite the user, if one with the same name exists.
Advanced Settings	
User Must change password at next logon	Specify whether the user has to change the password during the next logon or not.
User Cannot Change Password	Specify whether the user can change the password or not.
Password Never Expires	Specify whether the password should expire or not.
Account is Disabled	Specify whether the user account should be disabled or not.
User Profile	
Member of	Specify the groups in which this user account is a member.
Logon Script	Specify the logon script that has to be executed during the user logon.
Profile Path	Specify the path where the user profiles has to be stored.

Local Path	Specify a local path as the home folder. For example, c:\users\johnsmith.
Connect Map To	If the user's home folder has to be stored in a network directory, select the drive letter in the **Connect Map** and specify the network path in the **To** field.

If you wish to add more users or to perform another action, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

Top

Change Password

To change the user password, select the **Change Password** link from the Choose User Action table and specify the following:

Parameter	**Description**
User Name	The user name of the user whose password has to be changed.
Password	Type the new password.
Confirm Password	Re-type the password to confirm.

If you wish to continue adding more actions, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

Remove User

To remove an user from the computer, select the **Remove User** link from the Choose User Action table and specify the user to be removed.

If you wish to remove more users or to perform another action, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

Modify User

To modify an user, select the **Modify User** link from the Choose User Action table and specify the following:

Parameter	**Description**
User Name	The user name of the user to be modified.
Full Name	The full name of the user.
Description	The description for this user.
Advanced Settings	
User Must change password at next logon	Specify whether the user has to change the password during the next logon or not.
User Cannot Change Password	Specify whether the user can change the password or not.
Password Never Expires	Specify whether the password should expire or not.
Account is Disabled	Specify whether the user account should be disabled or not.
Account is Locked	Specify whether the user account should be locked or not.
User Profile	
Member of	Specify the groups in which this user account is a member.
Logon Script	Specify the logon script that has to be executed during the user logon.

Profile Path	Specify the path where the user profiles has to be stored.
Local Path	Specify a local path as the home folder. For example, c:\users\johnsmith.
Connect Map To	If the user's home folder has to be stored in a network directory, select the drive letter in the **Connect Map** and specify the network path in the **To** field.

If you wish to modify more users or to perform another action, click **Add More Action** button and continue. The values gets added to the **List of Settings** table.

To modify a setting from the **List of Settings** table, select the appropriate row and click icon and change the required values.

To delete a setting from the **List of Settings** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the User Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined User Management Configuration in the targets defined. The configuration will take effect during the next system startup.

To save the configuration as draft, click **Save as Draft**.

Top

See also : Managing Configurations and Collections, Viewing Configuration Reports, Defining Targets

Launching Applications

Launch Application configuration enables you to launch an application during startup or shutdown of the computer.

Step 1: Name the Configuration

Provide a name and description for the Launch Application Configuration.

Step 2: Define Configuration

Select whether the application has to be launched from the local computer (using HTTP) or from the network share. If you select the Local option, all the selected target computers should have the application in the same location and the application needs to be uploaded. Specify the following:

Parameter	Description
Application Name*	Browse and select the application that has to be launched. The applications that are available in the local machine from where the application has to be launched can also be specified.
Arguments*	Specify the arguments for the application, if any.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

1. To launch more applications, click **Add More Application** and repeat Step 2. The added application gets added to the **Launch Application** table.
2. To modify an application from this table, select the appropriate row, click ✎ icon and change the required values.

3. To delete an application from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Launch Application Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Launch Application Configuration in the targets defined. The applications configured will be launched during the next system startup.

To save the configuration as draft, click **Save as Draft**.

User Configurations

This section details the configurations that can be applied to the users belonging to Windows Domain. These configurations are applied to the users during user logon or logoff.

Ensure that you have defined the scope of management before defining the configurations.

Follow the steps mentioned below for choosing a configuration that needs to be created and deployed:

1. Navigate to **Configuration** tab. This will list all the supported configurations for computers and users as well.
2. Choose the required user configuration.

Desktop Central supports the below mentioned configurations that cover the functionalities of 4 major categories extensively:

Security Configurations

Desktop Central offers a bunch of configurations that when deployed, aids in hardening the security of your endpoints. The security configurations offered by Desktop Central are as follows :

- Alerts
- Certification Distribution
- Permission Management
- Secure USB Devices
- Security Policies
- Browsers

Productivity Configurations

Amp up the productivity of your network by deploying the following configurations to all the computers in your network.

- Custom Scripts
- Environment Variables
- IP Printer
- Shared Network Printer

- Install/Uninstall Software
- Path
- Power Management
- Registry
- Shortcut
- WiFi
- Drive Mapping

Desktop Configurations

Deploy the below mentioned desktop configurations & save ample amount of time in managing the desktops.

- Display
- File Folder Operation
- Message Box
- Folder Redirection

Application Configurations

- Launch Application
- MS Office
- MS Outlook
- Outlook Exchange Profile

Configuring Alerts

Table of contents

Alert Configuration enables you to warn the users about the password expiration, lower hard disk space, and larger temp file size. The alert configuration are user-specific and requires the user to be logged on to view the alerts.

Step 1: Name the Configuration

Provide a name and description for the Alert Configuration.

Step 2: Define Configuration

The table given below lists the parameters for which alerts can be configured:

Parameter	Description
Password Expiration	The number of days before which the user has to be informed about the password expiration. The default value is 14 days.
Disk Space (MB)	When the disk space goes below the specified value, the user will be warned.

Purge Temp Files	Specify whether to delete the temp files when exceeding the specified limit. You also have an option to specify the file types, size of the files, and whether to prompt the user before deleting the temp files or not.

The alerts will be displayed during every logon of the user as long as the alert condition is met. For example, the user will be warned about the lower disk space during every logon until the free disk space exceeds the specified value.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Alert Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Alert Configuration in the targets defined. The alerts will be displayed when the defined conditions are met.

To save the configuration as draft, click **Save as Draft**.

Certificate Distribution

Table of contents

This document explains the steps required to distribute digital certificates that are used on Windows platform. Using the Certificate Distribution configuration, you can distribute certificates such as SSL Certificates (for web browsers like Chrome), AD CA Root Certificates (to authenticate users on your WiFi network) to specified targets.

Here are a few scenarios where Certificate Distribution configuration can be used to distribute certificates efficiently:

1. Installing root certificates to authenticate AD users for WiFi access in an organization.
2. Distribute security certificates to browsers like chrome, Internet Explorer, etc to securely access websites within an organization.

Installing Certificates

The following are the steps to install certificates to your specified targets:

1. Navigate to Configurations -> Windows -> User -> Certificate Distribution.
2. Specify the name and description of the configuration.
3. Select the Install option.
4. Select certificate store(s) to which the certificate should be distributed to.
5. Browse and upload the certificate file from your computer.
6. Specify password for the certificate file if required.
7. You can select multiple certificate files to install using 'Add More Certificates' option.

Deleting Certificates

The following are the steps to delete certificates from the certificate stores of targets selected:

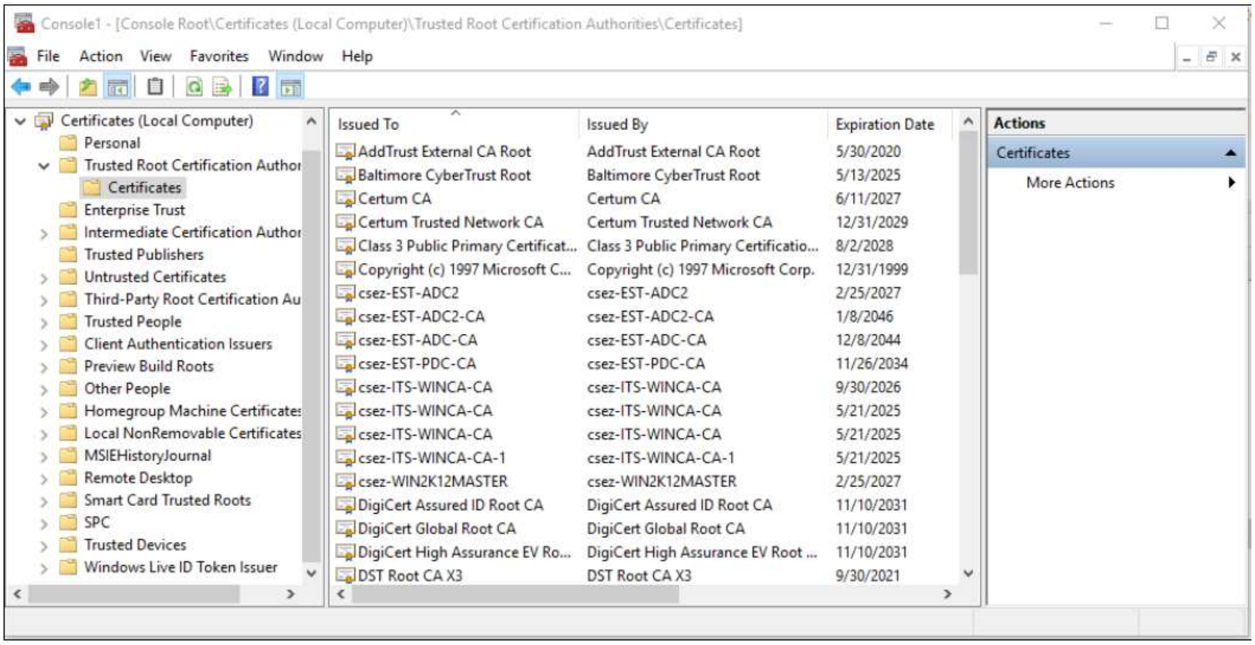
1. Navigate to Configurations -> Windows -> User -> Certificate Distribution.
2. Specify the name and description of the configuration.
3. Select the Delete option.
4. There are two delete actions that you can perform:
    - Delete specific certificate from the Certificate Store(s).
    - Delete all expired certificates from the Certificate Store(s).
5. Select the certificate store(s) from where certificates should be deleted.
6. Specify the Common Name (CN) value of the certificates.
7. All certificates with the given CN value will be deleted from the Store(s) selected above.
8. To delete a specific certificate, specify its unique Serial number.
9. You can select multiple certificate files to delete using 'Add More Certificates' option.

How to find the Common Name value (CN) and Serial Number of a certificate ?

To delete a specific certificate, you will have to specify a common name (CN) and its serial number. Find the CN and serial number from the certificate store of the computer where the certificate exists.

Steps:

1. Go to Run Prompt window.
2. Navigate to Run prompt and open Microsoft Management Console (MMC).
3. Select File -> Add/Remove Snap-in.
4. Select 'Certificates' from the available snap-ins.
5. You can select for which account you would like to manage certificates for.
6. Double click on the certificate to be deleted from the certificate store.



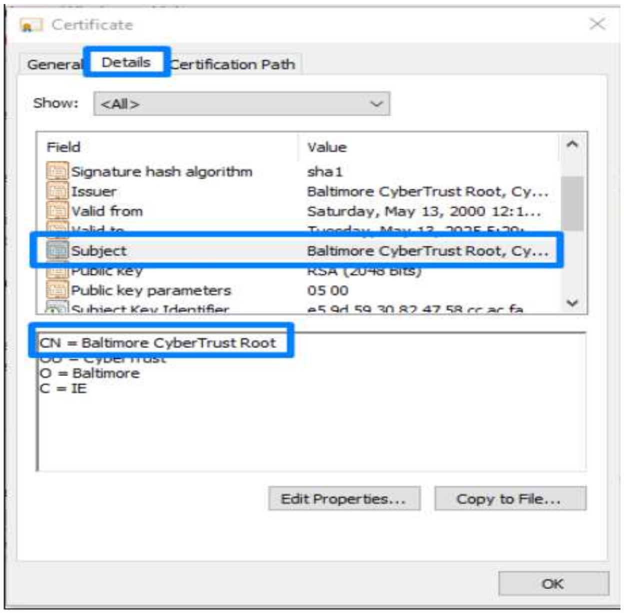
Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

- Certificates (Local Computer)
  - Personal
  - Trusted Root Certification Author
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Author
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Au
  - Trusted People
  - Client Authentication Issuers
  - Preview Build Roots
  - Other People
  - Homegroup Machine Certificates
  - Local NonRemovable Certificates
  - MSIEHistoryJournal
  - Remote Desktop
  - Smart Card Trusted Roots
  - SPC
  - Trusted Devices
  - Windows Live ID Token Issuer

Issued To	Issued By	Expiration Date
AddTrust External CA Root	AddTrust External CA Root	5/30/2020
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025
Certum CA	Certum CA	6/11/2027
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999
csez-EST-ADC2	csez-EST-ADC2	2/25/2027
csez-EST-ADC2-CA	csez-EST-ADC2-CA	1/8/2046
csez-EST-ADC-CA	csez-EST-ADC-CA	12/8/2044
csez-EST-PDC-CA	csez-EST-PDC-CA	11/26/2034
csez-ITS-WINCA-CA	csez-ITS-WINCA-CA	9/30/2026
csez-ITS-WINCA-CA	csez-ITS-WINCA-CA	5/21/2025
csez-ITS-WINCA-CA	csez-ITS-WINCA-CA	5/21/2025
csez-ITS-WINCA-CA-1	csez-ITS-WINCA-CA-1	5/21/2025
csez-WIN2K12MASTER	csez-WIN2K12MASTER	2/25/2027
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/10/2031
DST Root CA X3	DST Root CA X3	9/30/2021

Actions
- Certificates
  - More Actions

7. Select Details tab -> Subject field.
8. Copy the Common Name (CN) value. If CN value is not found, specify the value mentioned in Issued To column.

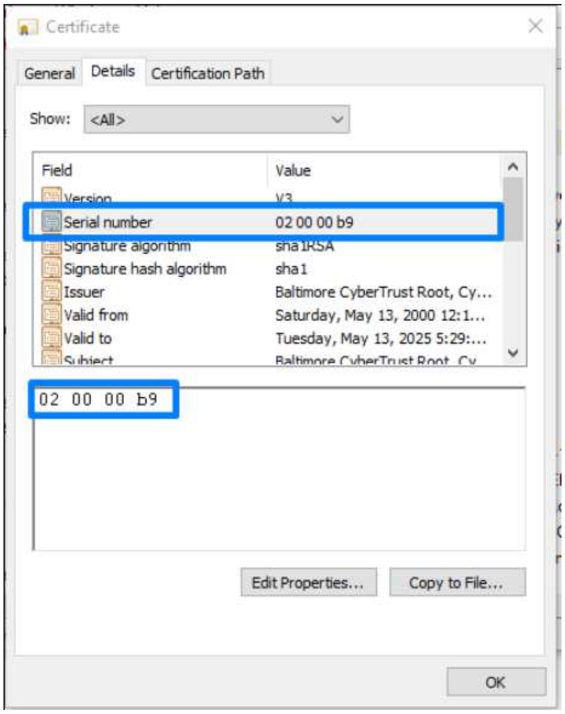


Show: <All>

Field	Value
Signature hash algorithm	sha1
Issuer	Baltimore CyberTrust Root, Cy...
Valid from	Saturday, May 13, 2000 12:1...
Valid to	Tuesday, May 13, 2025 5:29:...
Subject	Baltimore CyberTrust Root, Cy...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Subject Key Identifier	e5 9d 59 30 82 47 58 cc ac fa

CN = Baltimore CyberTrust Root
OU = CyberTrust
O = Baltimore
C = IE

9. Copy Serial number value from Details tab -> Serial number field.



Show: <All>

Field	Value
Version	V3
Serial number	02 00 00 b9
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Baltimore CyberTrust Root, Cy...
Valid from	Saturday, May 13, 2000 12:1...
Valid to	Tuesday, May 13, 2025 5:29:...
Subject	Baltimore CyberTrust Root, Cy

```
02 00 00 b9
```

You have successfully created a configuration to distribute or delete certificates from the certificate store of the required computer.

Managing Permissions

Table of contents

The Permission Management allows you to grant/revoke permission on the files, folders and registry for the users. Desktop Central Permission Management Configuration enables you to grant/revoke permissions to multiple users from a central point.

Step 1: Name the Configuration

Provide a name and description for the Permission Management configuration.

Step 2: Define Configuration

You can grant or revoke permissions for the following objects:

- Files
- Folders
- Registry

Files

To grant or revoke permissions for files, select the *File* tab and specify the following values:

Parameter	**Description**

File name	Specify the name of the file for which you need to specify permissions.
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: ● Append - To append to the existing file permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. ● Overwrite - To overwrite the existing file permissions ● Revoke - To revoke the existing file permissions of the specified user/group. All the permissions to the specified user/group on that file will be removed. However, the inherited permissions will not be removed.
Settings	Select the required options.

If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Folders

To grant or revoke permissions for folders, select the *Folder* tab and specify the following values:

Parameter	**Description**

Folder name	Specify the name of the folder for which you need to specify permissions.
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: ● Append - To append to the existing folder permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. ● Overwrite - To overwrite the existing folder permissions ● Revoke - To revoke the existing folder permissions. All the permissions to the specified user/group on that folder will be removed. However, the inherited permissions will not be removed.
Inheritance	Select the required option to specify how the permission should effect its subfolders and files
Settings	Select the required options.

If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

Registry

To grant or revoke permissions for registry, select the *Registry* tab and specify the following values:

Parameter	**Description**
Hive	Select the registry hive from the given options
Key	Specify the key within that hive for which you need to set the permissions
User/Group Principal	Select the users and groups for whom you would like to grant or revoke permissions.
Action	Select the action from the following: ● Append - To append to the existing registry permissions. Please note that it will only append to the existing permissions on the object and will not overwrite. For example, for an object having full permissions, if you just select a deny permission to write, only write permission will be removed while the user/group can still modify the object. ● Overwrite - To overwrite the existing registry permissions ● Revoke - To revoke the existing registry permissions. All the permissions to the specified user/group on that registry key will be removed. However, the inherited permissions will not be removed.
Inheritance	Select the required options to specify how the permission should effect its subkeys.
Settings	Select the required options.

If you wish to add more permissions, click **Add More Permissions** button and repeat step 2. The values gets added to the **List of Permission Actions** table.

To modify a permission from the **List of Permission Actions** table, select the appropriate row and click 📝 icon and change the required values.

To delete a permission from the **List of Permission Actions** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Permission Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Permission Management Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Securing USB Devices

Table of contents

Description

The Secure USB configuration is used for both users and computers to block or unblock the use of the USB devices. This configuration is applicable to users irrespective of the computers they use.

Using this configuration, you can block or unblock the following devices:

1. Mouse
2. Disk drives (for example: USB drives and external hard-disk drives)
3. CD ROMs
4. Portable devices (for example: mobile phones, digital cameras and portable media players)
5. Floppy disks
6. Bluetooth devices
7. Images (for example: USB cameras and scanners)
8. Printers
9. Modems
10. Apple USB devices (for example: iPhone, iPad and iPod touch)

You can also exclude devices using the Device Instance ID assigned to each device.

Secure USB Settings for Users

When you create the Secure USB configuration to block or unblock devices for users, you can set actions to take place once the user logs off. These actions enable you to retain or remove the settings that you make, using the Secure USB configuration, once the user logs off. The actions that you can set include the following:

1. Don't alter device status: Use this option to retain the settings you have made, even after the user has logged off.

   For example, if you use this option, the settings that you have made to block or unblock the usage of USB devices will apply to all users who log on.

2. Disable all devices excluding mouse: Use this option to remove the settings you have made, even after the user has logged off.

Applying Secure USB Settings to Computers and Users

When you apply the Secure USB configuration to both computers and users, the settings made for computers will be applied before the settings made for users. For example, assume that you have made the following settings:

1. **Settings configured for users**
   a. Administrator: You have unblocked the usage of the disk drive
   b. Other users (excluding the administrator): You have not deployed any configurations
2. **Settings configured for computers :** You have blocked the usage of portable devices and disk drives

The following actions will take place:

1. Computer startup: The Secure USB configuration settings made for the computer are applied when the computer is started. This means that no portable devices and disk drives can be used.
2. Administrator logon: The Secure USB configuration for the computer is applied. However, it is over written by the settings made for the administrator. This means that the administrator can use disk drives.
3. Other users (excluding the administrator) log on: The Secure USB configuration made

for the computer is applied.

4. Other users (excluding the administrator)log off: The log off-action settings made for users are applied when a user logs off. If the log off-action setting is set to Don't alter device status, then the settings made will apply to the next user who logs on, provided that the user does not have any settings that apply to them.

> **Note**: **Block USB**, represents to block the access to use any USB device.
> **Unblock USB,** represents to re-enable the access to the USB devices that has been blocked.
> **No Change,** represents that no change has been made to the current settings.

Adding Restrictions to secure USB Devices

As an administrator, you can create a configuration block or unblock specific USB devices. You can also exclude specific devices, if required.

To create a configuration to secure USB devices for users, follow the steps given below:

1. Navigate to **Configurations** tab and choose **Secure USB** from the list of Windows configurations.
2. Enter a name and description for the configuration
3. Click **Add** to apply restrictions
4. To add restrictions, select the devices, choose to block or unblock devices. When you have chosen to block devices, you can also specify the devices which needs to be excluded.
5. Select the required log-off action
6. Define the target
7. Specify the required execution settings
8. Click **Deploy**

You have created configurations to secure USB devices. These configurations will be applied when the user logs in to the computer.

Excluding Devices

When you block a device you can exclude certain devices from being blocked. This can be done, by using Vendor ID or the Device Instance ID assigned to each device. You can exclude devices only when you have blocked a device. To exclude devices, follow the steps given below:

1. Click the **Exclude Devices** link against a device
2. Enter the **Device Instance ID** for the device. You can also choose to block all the

devices, from the specified **vendor**. You will have to specify the Device Instance ID using which, Desktop Central will fetch the vendor instance ID and exclude all devices from the specific vendor.

3. You can choose to exclude **All Encrypted devices/encrypted devices from the list of specified devices.** Devices that are encrypted using bit locker can be added to the exclusion list. This is applicable only for Disk Drives and the target computer supports bit locker.
4. Click **Close**

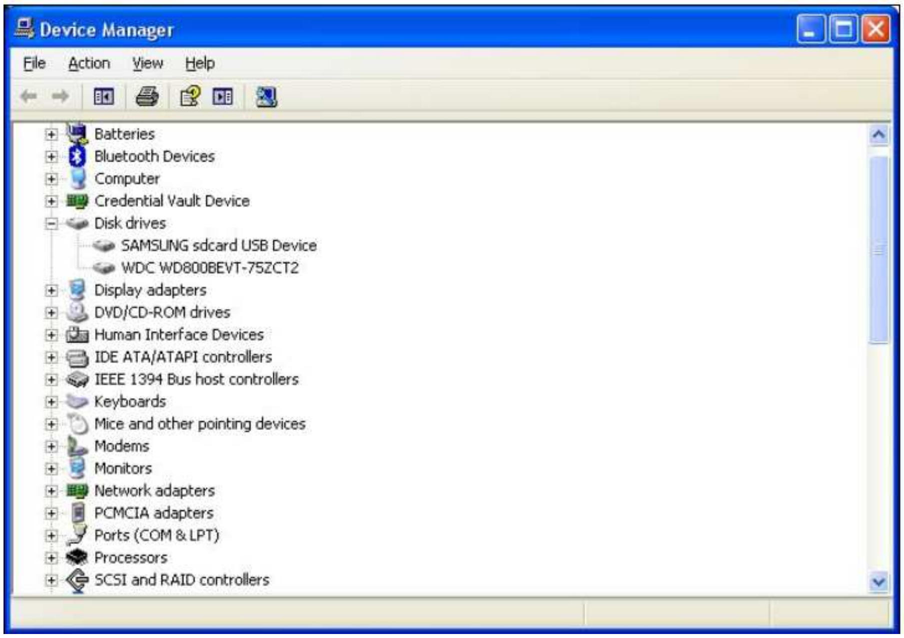
You have excluded a device from being blocked.

Device Instance ID

Every USB device has a unique ID. This ID is assigned to devices by the system to identify them easily. You can identify the Device Instance ID of a Device by following the steps mentioned below:

- Right-click **My Computer**
- Click **Properties**
- Click **Device Manager** (Refer to the figure below)
- From the list of devices, expand the list of devices for which you want the Device Instance ID.

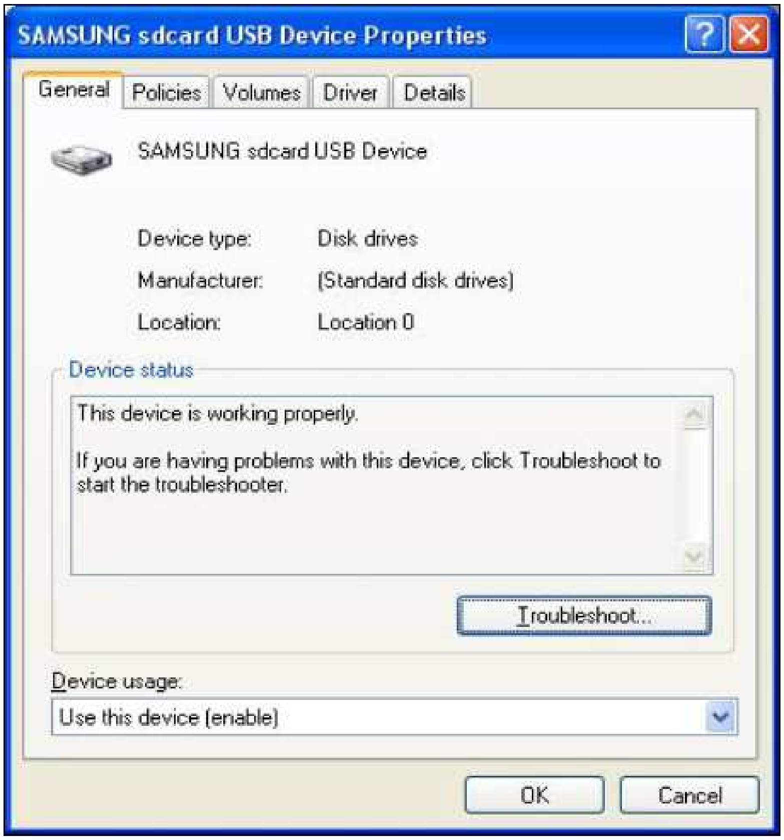
  (For example : if you want to identify the Device Instance ID of a mobile phone that you have connected to the computer, expand portable devices and follow the next step.)



- Batteries
- Bluetooth Devices
- Computer
- Credential Vault Device
- Disk drives
  - SAMSUNG sdcard USB Device
  - WDC WD800BEVT-75ZCT2
- Display adapters
- DVD/CD-ROM drives
- Human Interface Devices
- IDE ATA/ATAPI controllers
- IEEE 1394 Bus host controllers
- Keyboards
- Mice and other pointing devices
- Modems
- Monitors
- Network adapters
- PCMCIA adapters
- Ports (COM & LPT)
- Processors
- SCSI and RAID controllers

Figure 1: Device Manager

- Right-click on the name of a specific device and click **Properties** (Refer to the figure below)



SAMSUNG sdcard USB Device

Device type: Disk drives

Manufacturer: (Standard disk drives)

Location: Location 0

Device status

This device is working properly.

If you are having problems with this device, click Troubleshoot to start the troubleshooter.

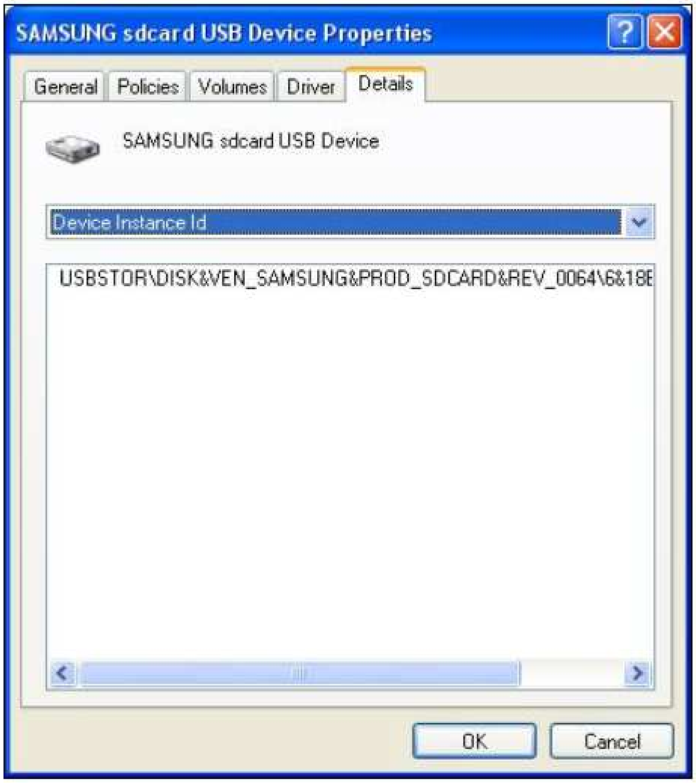
Device usage:

Use this device (enable)

Figure 2: Properties

i. Click the **Details** tab

ii. In the drop-down box, select **Device Instance ID** or Device Instance Path (Refer to the figure below)



SAMSUNG sdcard USB Device Properties
General
Policies
Volumes
Driver
Details
SAMSUNG sdcard USB Device
OK
Cancel

Device Instance Id

USBSTOR\DISK&VEN_SAMSUNG&PROD_SDCARD&REV_0064\6&18E

Figure 3: Device Instance ID

In computers which have the operating system Windows Vista (and later versions), the Device Instance ID is called the **Device Instance Path**. You can copy the Device Instance Path from the Properties property sheet of the Device Manager.

In computers that have older versions of the Windows operating system installed in them, you cannot copy the Device Instance ID directly from the Properties property sheet of the Device Manager.

To copy the Device Instance ID you must open the dcusbaccess log file. This file is located in **<Drive>\<Desktopcentral_Agent Folder>\logs\dcusbaccess.log.** It contains information about the following:

- Action Time (inserted\removed time)
- Action (inserted\removed)
- Friendly name
- Device Instance ID

You can now view and copy the Device Instance ID for a specific device.

Revoking All USB Restrictions applied to the User

Administrators can choose to revoke all USB related restrictions which are applied to the user.

To create a configuration, in order to revoke all USB related restrictions for users, follow the steps given below:

1. Navigate to **Configurations** tab and choose **Secure USB** from the list of Windows configurations.
2. Enter a name and description for the configuration
3. Click **Remove** to revoke all restrictions applied to the user
4. Select the required log-off action
5. Define the target
6. Make the required execution settings
7. Click **Deploy**

You have created configurations to secure USB devices. These configurations will be applied when the user logs in to the computer.

Configuring Security Policies

Table of contents

Security policies determine the various security restrictions that can be imposed on the users in a network. The security settings for Active Desktop, Computer, Control Panel, Explorer, Internet Explorer, Network, and System categories can be defined using **Security Policies Configuration**.

Step 1: Name the Configuration

Provide a name and description for the Security Policies Configuration.

Step 2: Define Configuration

Specify the following values:

Parameter	Description
Choose Policy Category	The specific policy area in which the security policy will be applied. Select the desired category from left. This displays the relevant security polices. For details on the each category, refer to Windows Help documentation. For details on the each policy in the **Select the Policy** list, refer to Security Policies topic.

Policy Value	To enable, disable, or to leave it unconfigured, select the appropriate option.

1. To modify a security policy from this table, select the appropriate row, click ✎ icon and change the required values.
2. To delete a security policy from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Security Policies Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Security Policies Configuration in the defined targets. The security policies will be applied during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Configuring Browser Settings

Table of contents

You can choose to configure browser settings for computers using Desktop Central. Securing browsers is one of the essential ways of securing corporate data. Desktop Central supports the following browsers on Windows operating system:

- Google Chrome
- Microsoft Edge
- Firefox
- Internet Explorer

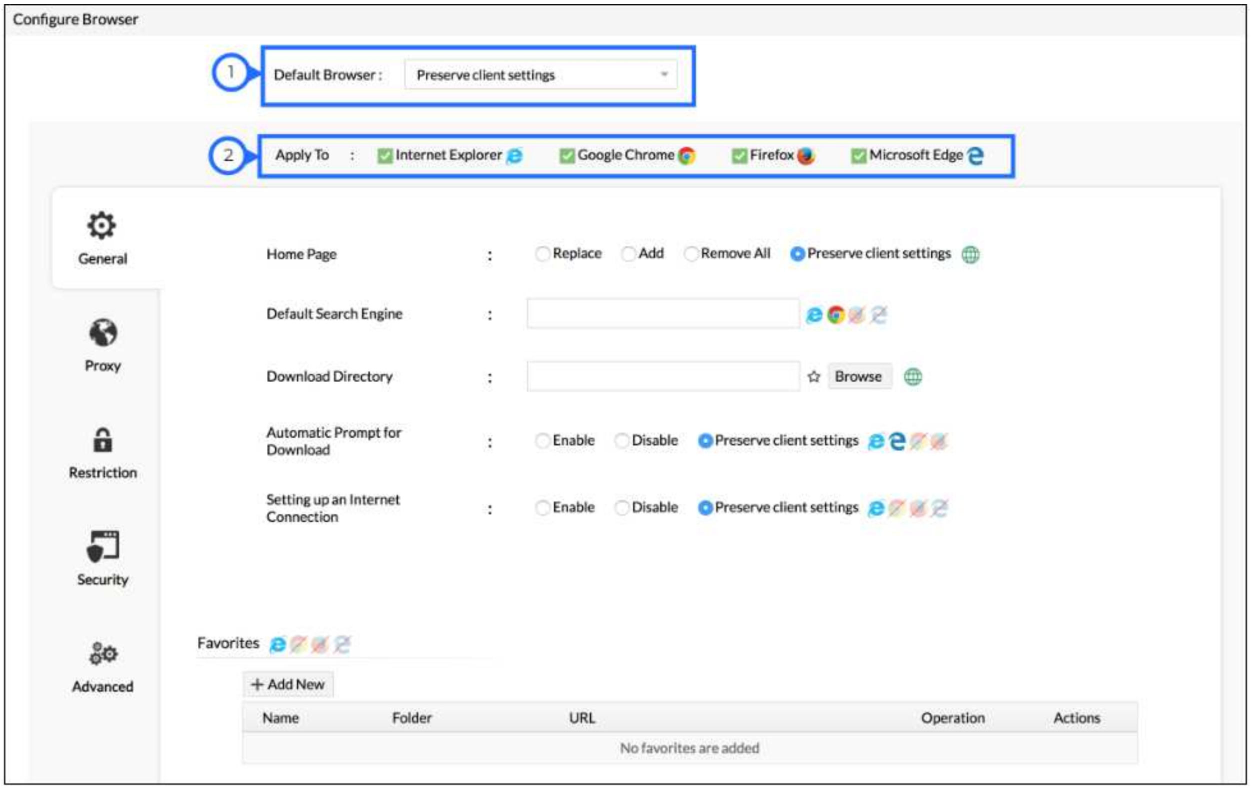
Securing Web Browsers

Web browsers are undoubtedly the most common portal used by end users for accessing the internet. Browsers are installed on almost all the computers and are used quite frequently. In addition to this, web browsers that come in a default setting with an operating system will not be in a secure set up. Hence, browsers need to be secured. Browser security needs to be hardened if you do not wish to let the intruders take control over your system.

Choose the default browser and configure the following settings :

General settings

- Specify the default home page, search engine and download directory. You can click the ☆ icon to select and assign a dynamic variable to assign download directory.
- Be it setting up an internet connection or selecting favorites, you can have it all under your control.
- You can choose to add multiple web pages and set it as default home page. This way, users will not have the need to manually open the web pages every time they launch a browser.


Configure Browser

1 Default Browser : Preserve client settings

2 Apply To : ☑ Internet Explorer ☑ Google Chrome ☑ Firefox ☑ Microsoft Edge

Home Page : ○ Replace ○ Add ○ Remove All ● Preserve client settings

Default Search Engine :

Download Directory : ☆ Browse

Automatic Prompt for Download : ○ Enable ○ Disable ● Preserve client settings

Setting up an Internet Connection : ○ Enable ○ Disable ● Preserve client settings

Favorites

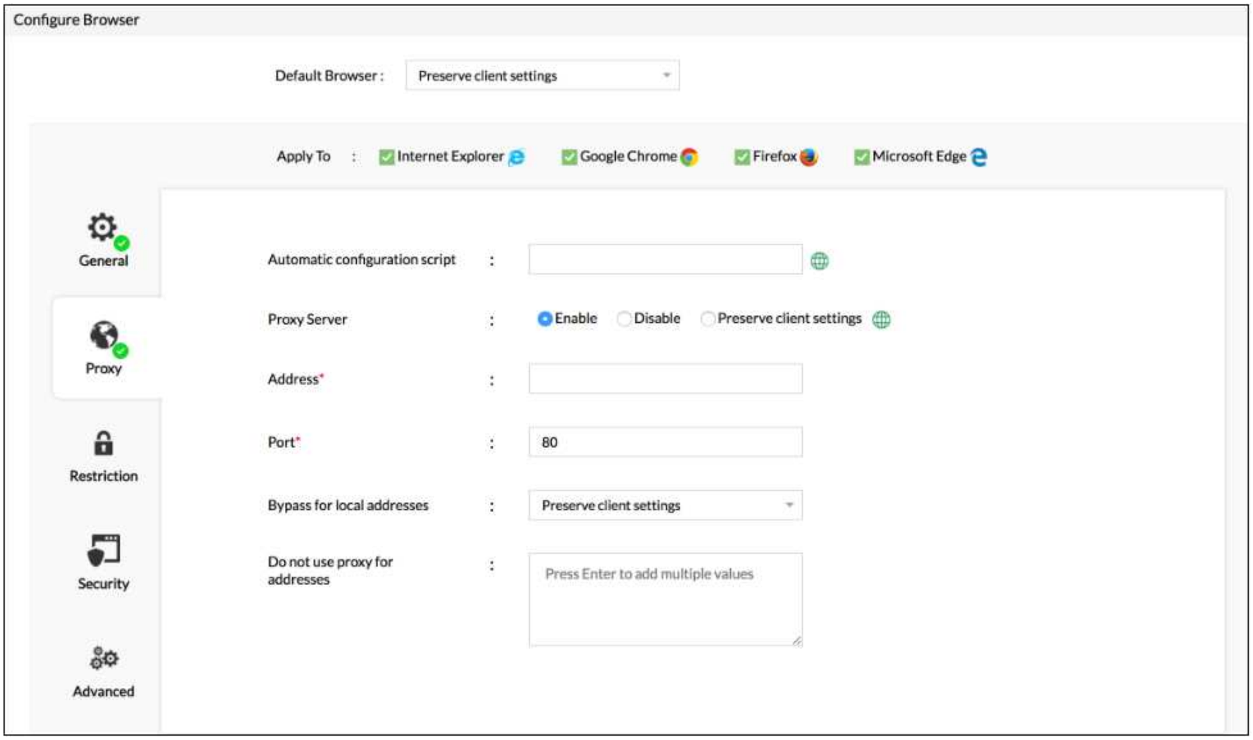
+ Add New

Name	Folder	URL	Operation	Actions
No favorites are added				

General Settings

Proxy

- Enable proxy server either manually or by running an automatic configuration script.
- While enabling the proxy server manually, provide details such as address, port (default port : 80).
- While proxy is configured for all communication using browsers, you can still choose to exclude web pages that will be exempted from proxy.



Configure Browser

Default Browser : Preserve client settings

Apply To : ☑ Internet Explorer ☑ Google Chrome ☑ Firefox ☑ Microsoft Edge

Automatic configuration script :

Proxy Server : ● Enable ○ Disable ○ Preserve client settings

Address* :

Port* : 80

Bypass for local addresses : Preserve client settings

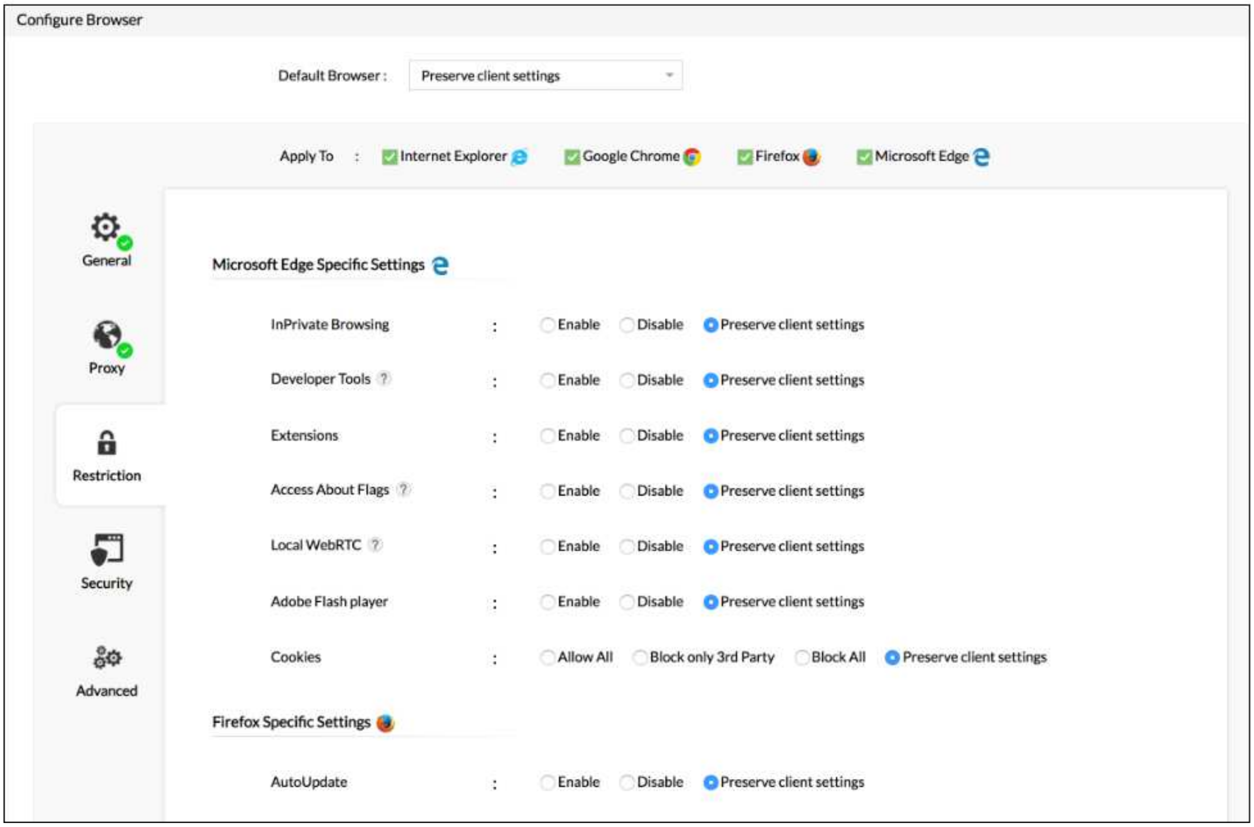
Do not use proxy for addresses : Press Enter to add multiple values

Proxy Settings

Restrictions

Your browser history is indicative of where you go on the internet and for what purpose, which is quite intrusive. While cookies are another potential source of vulnerability attacks, disabling them is one of the best solutions.

Impose Edge-specific restrictions and firefox-specific restrictions such as disabling AutoUpdates for turning off prompts that are nagging.



Configure Browser

Default Browser : Preserve client settings

Apply To : ☑ Internet Explorer ☑ Google Chrome ☑ Firefox ☑ Microsoft Edge

Microsoft Edge Specific Settings

InPrivate Browsing	:	○ Enable ○ Disable ● Preserve client settings
Developer Tools ?	:	○ Enable ○ Disable ● Preserve client settings
Extensions	:	○ Enable ○ Disable ● Preserve client settings
Access About Flags ?	:	○ Enable ○ Disable ● Preserve client settings
Local WebRTC ?	:	○ Enable ○ Disable ● Preserve client settings
Adobe Flash player	:	○ Enable ○ Disable ● Preserve client settings
Cookies	:	○ Allow All ○ Block only 3rd Party ○ Block All ● Preserve client settings

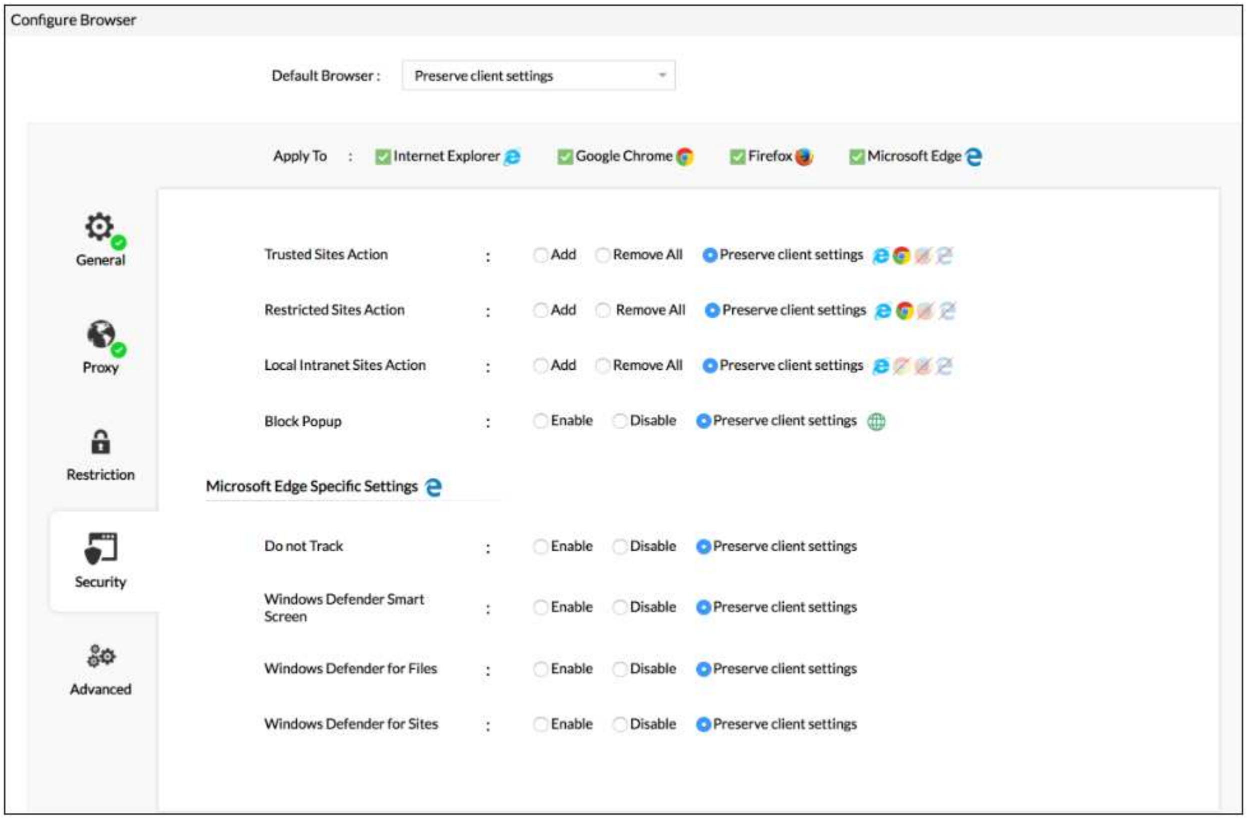
Firefox Specific Settings

AutoUpdate	:	○ Enable ○ Disable ● Preserve client settings

Impose restrictions

Security settings

- Stay in the security zone by adding addresses of the sites and local intranet sites that can be trusted along with the sites that need to be restricted. Listing trusted sites does not restrict the users from accessing sites that are not trusted.
- Block pop-ups and become phising-resistant.
- Windows defender settings can be enabled to strengthen the security of your browsers. It automatically scrutinizes files, sites and apps for malicious content and warns the user about the same.



Configure Browser

Default Browser : Preserve client settings

Apply To : ☑ Internet Explorer ☑ Google Chrome ☑ Firefox ☑ Microsoft Edge

Trusted Sites Action : ○ Add ○ Remove All ● Preserve client settings

Restricted Sites Action : ○ Add ○ Remove All ● Preserve client settings

Local Intranet Sites Action : ○ Add ○ Remove All ● Preserve client settings

Block Popup : ○ Enable ○ Disable ● Preserve client settings

Microsoft Edge Specific Settings

Do not Track : ○ Enable ○ Disable ● Preserve client settings

Windows Defender Smart Screen : ○ Enable ○ Disable ● Preserve client settings

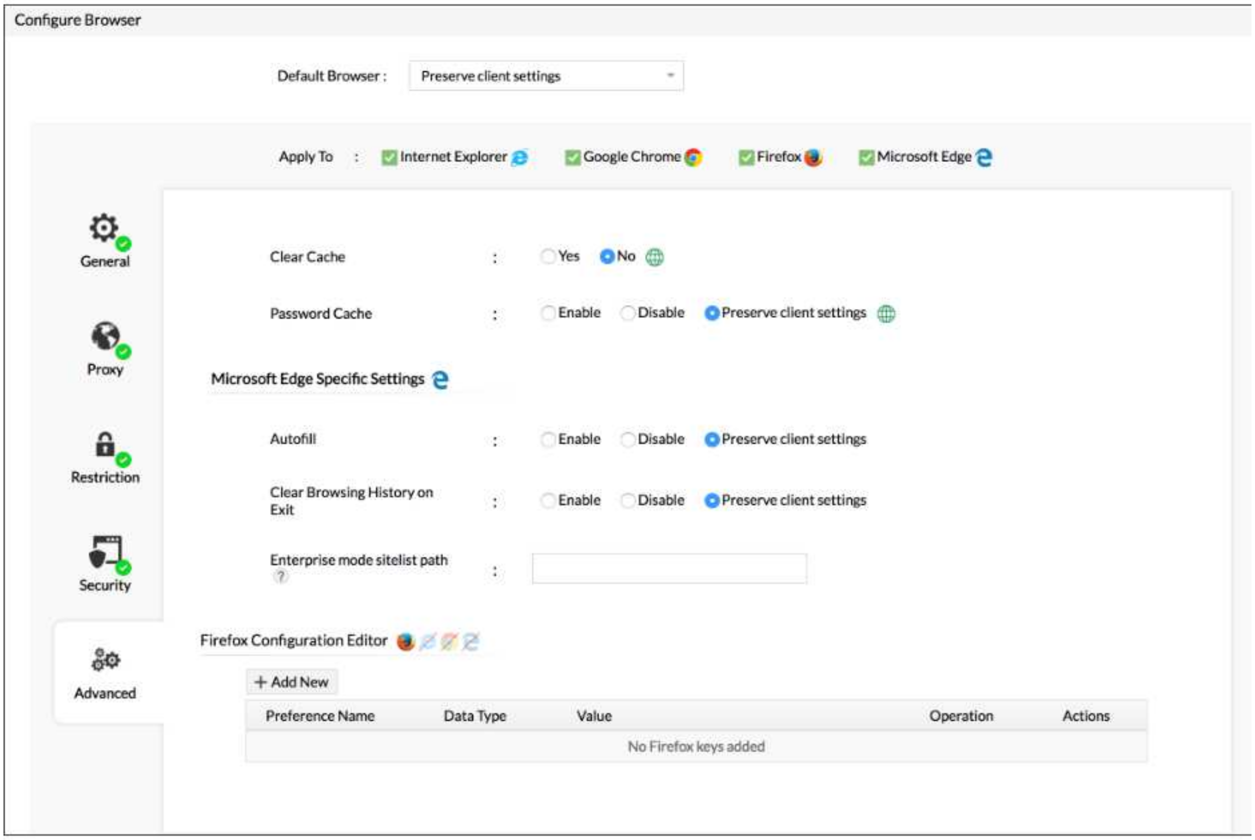
Windows Defender for Files : ○ Enable ○ Disable ● Preserve client settings

Windows Defender for Sites : ○ Enable ○ Disable ● Preserve client settings

Security Settings

Advanced settings

- Clear cache and password cache : Clearing cache is a good way of flushing potentially sensitive information.
- Autofill : While autofill saves time, it can prove to be deadly if they get trapped in the wrong hands.
- Clear browsing history on exit
- Enterprise mode sitelist path : Provide the path for enterprise mode sitelist to overcome compatibility issues. Legacy websites will automatically be opened using Internet Explorer. Everytime a browser renders a site, it compares it against the list of legacy sites. When a legacy site is to be rendered, it is routed to IE instead of Edge.
- Add new preferences to the configuration editor page of Firefox and determine what operation needs to be done.



Configure Browser

Default Browser : Preserve client settings

Apply To : ☑ Internet Explorer ☑ Google Chrome ☑ Firefox ☑ Microsoft Edge

Clear Cache : ○ Yes ● No

Password Cache : ○ Enable ○ Disable ● Preserve client settings

Microsoft Edge Specific Settings

Autofill : ○ Enable ○ Disable ● Preserve client settings

Clear Browsing History on Exit : ○ Enable ○ Disable ● Preserve client settings

Enterprise mode sitelist path ? :

Firefox Configuration Editor

+ Add New

Preference Name	Data Type	Value	Operation	Actions
No Firefox keys added				

Advanced Settings

Steps

- Configure all the aforementioned settings by creating a browser configuration under configurations tab.
- Define the targets and the execution settings before deploying the configuration.

You have successfully created a configuration to deploy browser settings.

Executing Custom Scripts

Table of contents

Desktop Central provides options for configuring almost all the user configurations from remote. In addition to the configurations that are supported by Desktop Central, administrators can also write their own scripts that could be run on the user machines for accomplishing specific configurations. The scripts could be any of the following:

- Batch file (.bat or .cmd)
- In any other language hosted by Windows Script Host (WSH), such as VB Script, JScript, Perl, REXX, and Python.

Note: The script engines for languages like Perl, REXX, and Python, must be registered with Windows. You can also execute single line commands, add dependent files and enable logging, to analyze the output of the script after execution.

Step 1: Name the Configuration

Provide a name and description for the custom script configuration.

Step 2: Define Configuration

The table given below lists the parameters that have to be provided for defining the

configuration.

Parameter	Description
Execute Script from	You can execute the script either from repository or as a command line.
Script Name*	The script that has to be added/removed in the user machines needs to be chosen from the script repository. It is mandatory to add the script to the script repository for this to work.
Script Arguments	The arguments that have to be provided while executing the scripts.
Dependency files	The required dependency files for execution of the script needs to be added.
Exit Code	Specify the exit code, which should be returned, when the script has been executed successfully
Frequency	Specify the frequency for this script to be executed, like only once, during every user logon, during subsequent user logon for specified number of times or all user logon until a specified time period.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Custom Script Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Custom Script Configuration in the targets defined.

To save the configuration as draft, click **Save as Draft**.

Setting Environment Variables

Table of contents

Environment variables are strings that contain information about the environment for the system, and the currently logged on user. Some software programs use the information to determine where to place files (such as temp, tmp, path etc). Environment variables control the behavior of various programs. Any user can add, modify, or remove a user environment variable. However, only an administrator can add, modify, or remove a system environment variable. Using Desktop Central, the environment variables can be defined and added.

Step 1: Name the Configuration

Provide a name and description for the Environment Variable configuration.

Step 2: Define Configuration

The following table lists the parameters that have to be specified**:**

Parameter	Description
Variable*	The environment variable name that has to be modified or added.

Value*	The value that has to be stored in the environment variable. Click the ☆ icon to select and assign a dynamic variable to this parameter.

* - denotes mandatory fields

1. To add more environment variables, click **Add More Variable** and repeat Step 2. The defined environment variable gets added to the **List of Environment Variable** table.
2. To modify a environment variable from this table, select the appropriate row, click📝 icon and change the required values.
3. To delete a environment variable from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Environment Variable Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Environment Variable Configuration in the targets defined. The configurations will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Configuring IP Printer

Table of contents

The IP Printer Configuration is for adding or deleting the IP Printer connection in the user computers. For configuring a shared printer in the computer for specific users, refer to the Configuring Shared Printer topic.

Step 1: Name the Configuration

Provide a name and description for the IP Printer configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add an IP Printer
- Delete an IP Printer

Add an IP Printer

To add an IP Printer, select the **Action** as *Add* and specify the following values:

Parameter	**Description**

DNS Name/IP	The host name or IP address defined for the printer. *Example*: `192.111.2.32`
Printer Name	The display name for the printer.
Protocol	The printing protocol supported by the printer. Select the printing protocol from the Protocol list box. The default option is "RAW".
Port Number	The port number/queue name in which printing protocol is communicating between the computer and printer. Enter the port number in the Port Number field if the "RAW" Protocol is selected or enter the queue name if the "LPR" Protocol is selected. The default value is 9100.
Port Name	This is an optional field. By default, the port name is IP_<IP_Address/DNS_Name>. You can change the port name if required.
Add new driver package	Add the driver package that is bundled along with your printer or download your model specific driver package and add. If you know the correct INF file specific to your printer you can choose to provide it below.
Use a pre-installed driver	If you want to use a pre-installed driver to configure this printer, specify the name of the driver. To find the driver name navigate to devices and printers -> right click on a printer -> advanced option in properties.
Shared Network Printer for driver installation	Provide the network path of the shared printer.

Connect Shared Network Printer using Credentials	To copy Driver Files across Domains or amongst Workgroup computers, you need to specify a credential that has access to domain/workgroup machine where the Shared Printer Driver Files are present.

Delete an IP Printer

To delete an IP Printer, select the **Action** as *Delete* and specify the following values:

Parameter	**Description**
Printer Name	The display name of the printer.
Delete all existing IP printer connections	To delete all the existing IP printer connections in the computer for the specified user, select this option.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the IP Printer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined IP Printer Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Configuring Shared Network Printer

Table of contents

When a printer is installed in a machine in the network and is shared, other machines in the network can use this printer for their printing needs. Desktop Central enables you to configure the Shared Network Printer in the user machines.

For configuring an IP printer connection to the computer, refer to the Configuring IP Printer topic.

To add the Shared Network Printer Configuration, a computer must be installed with printer connection and must be shared.

Step 1: Name the Configuration

Provide a name and description for the Shared Network Printer Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Add a Shared Network Printer
- Delete a Shared Network Printer

Add a Shared Network Printer

To add a Shared Network Printer, select the **Action** as *Add* and specify the following values:

Parameter	**Description**
Shared Network Printer Path*	Browse and select the path of the shared network printer location in the network.
Connect network share using credentials	Provide the necessary credentials for using the network shared printer.
Set as default printer	Select this check box, if you want to make this as the default printer for the user. By default, this option is cleared.

* - denotes mandatory field

Delete a Shared Network Printer

To delete a Shared Network Printer, select the **Action** as *Delete* and specify the following values:

Parameter	**Description**
Shared Network Printer Path*	Browse and select the path of the Shared Network Printer location in the network.
Delete all existing Shared Network Printer connections	Select this check box, if you want to delete all the existing Shared Network Printer connections. By default, this option is disabled.

* - denotes mandatory field

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Shared Network Printer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Shared Network Printer Configuration in the defined targets. The printer configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Installing Software - MSI & EXE Packages

Table of contents

The Software Installation configuration helps you to install MSI and EXE packages remotely to specific users of several computers of the Windows network from a central location.

Step 1: Name the Configuration

Provide a name and description for the Software Installation Configuration.

Step 2: Define Configuration

You have an option to install either an EXE or an MSI package

- Install MSI Package
- Install EXE Package

Install MSI Package

Select the Installer type as **MSI** and specify the following values:

Parameter	**Description**

MSI Package Name	This will list all the MSI packages that are available in the Software Repository. Select the MSI that has to be installed.
Operation Type	To specify how the installation should happen. Select any of the following options: ● *Install Completely:* Selecting this option will install the application automatically. ● *Advertise*: Selecting this option will notify the user about the availability of the software. Thy can choose whether to install the software or not. ● *Remove*: Selecting this option remove (uninstall) the application from the system
Install as	The user as whom the MSI has to be installed. *System User:* Default system user privilege *Run as User:* User Account with specific privilege *Target User:* User privilege to whom the package is deployed
Copy	You have an option to copy the installables to the client machines before installing them. Select the required option: ● *None:* Selecting this option will not copy the installation files. ● *Copy file to client machines:* Will copy the exe or the msi file alone as specified in the software package to the client machines. ● *Copy folder to client machines:* Will copy the entire directory that has the installation file to the client machines. Copy option will be mandatory, when the network share requires a user credential to access and when you opt to install the software as a different user using the Run As option. The content copied on the client machines will be removed after the software is installed successfully. If the software installation fails, the copied content will be maintained for

	trouble shooting purpose.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	**Description**
Schedule Time to Perform the Operation	Select his option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type & Installation / Uninstallation Option selected, but this will begin after the time specified here.

Specify the Deployment Settings for the software:

If you have defined Deployment Templates, you can load the Deployment Settings directly from a template by selecting the required template from the list.

Parameter	**Description**
Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after system startup: ● *During startup*: Select this option if the software has to be installed/uninstalled during computer startup. ● *After startup*: Select this option if the software has to be installed/uninstalled after the computer startup when the next GP update happens (within 90 minutes) ● *During or After Startup*: Either of the above, whichever is earlier
Install Between	If you want the installation to happen only between a specified time of a day, you can specify the Start and End time within which the deployment should begin. The Start Time can also be greater than the End time - in such cases the End time is assumed to be on the following day. For example, if you wish the deployment should happen between 10.00 PM and 4.00 AM, you can specify the Start Time as 22:00:00 and End Time as 04:00:00
Allow Users to Skip Deployment	Specify whether the use can skip the deployment at a later time by selecting the "Allow Users to Skip Deployment". When you do not select this option, the deployment will be forced and the user will not have any control on the deployment. When you allow users to skip deployment, you can also specify whether they can skip it as long as they wish or force deployment after a specific date.

Reboot Policy	● *Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. ● *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. ● *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to be displayed in the client machines. This option is applicable if the computer is turned on and even if there is no logged on user, the computer will get restarted after the specified time. ● *Allow user to skip Reboot*: Select this option to allow users to reboot later. Specify the message that has to be displayed in the client machines. ● *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to be displayed in the client machines.

Install EXE Packages

Select the Installer type as **EXE** and specify the following values:

Parameter	**Description**
EXE Package Name	This will list all the EXE packages that are available in the Software Repository. Select the EXE that has to be installed.
Operation Type	To specify how the installation should happen. Select any of the following options: ● *Install Completely:* Selecting this option will install the application automatically. ● *Advertise*: Selecting this option will notify the user about the availability of the software. Thy can choose whether to install the software or not.

	● *Remove*: Selecting this option remove (uninstall) the application from the system
Install as	The user as whom the EXE has to be installed. *System User:* Default system user privilege *Run as User:* User Account with specific privilege *Target User:* User privilege to whom the package is deployed
Copy	You have an option to copy the installables to the client machines before installing them. Select the required option: ● *None:* Selecting this option will not copy the installation files. ● *Copy file to client machines:* Will copy the exe or the msi file alone as specified in the software package to the client machines. ● *Copy folder to client machines:* Will copy the entire directory that has the installation file to the client machines. Copy option will be mandatory, when the network share requires a user credential to access and when you opt to install the software as a different user using the Run As option.

Click **Add More Packages** to install/uninstall additional software.

Note:You can also uninstall a previous version of the software either by running a pre-installation script (should be specified while creating a package) or by selecting the Operation Type as Remove. In the latter case, you need to add two packages, one to remove the older version and the other to install the new version.

Specify the Scheduler details for installing the software:

Parameter	**Description**
Installation / Uninstallation Option	Specify whether the installation/uninstallation should happen during or after user login: ● *During Login*: Select this option if the software has to be installed/uninstalled during the user login. ● *After Login*: Select this option if the software has to be installed/uninstalled after the user login but within 90 minutes. ● *During or After Login*: Either of the above, whichever is earlier
Schedule Time to Perform the Operation	Select his option and specify the data and time after which the installation should begin. It may be noted that the installation/uninstallation will still be based on the Operation Type selected, but this will begin after the time specified here.
Reboot Policy	● *Do not reboot*: Select this option if the client computers should not be rebooted after installing the software. ● *Force Reboot when the user has logged in*: Select this option to force the user to reboot the computer. Specify the time within which the client machines will be rebooted and the message that has to displayed in the client machines. ● *Force Shutdown when the user has logged in*: Select this option to force the user to shutdown the computer. Specify the time within which the client machines will be shutdown and the message that has to displayed in the client machines. ● *Allow user to skip Reboot*: Select this option to allow users

	to reboot later. Specify the message that has to displayed in the client machines. ● *Allow user to skip Shutdown*:Select this option to allow users to shutdown later. Specify the message that has to displayed in the client machines.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Windows Installer Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Windows Installer Configuration in the defined targets. The software installation for the selected targets will happen as scheduled.

To save the configuration as draft, click **Save as Draft**.

Setting Path

Table of contents

For the users in the network, the paths which are configured and stored in the **Path** variable in the **Environment Variables** window (invoked by Right-click the **My Computer** icon, choose **Properties** > **Advanced** tab, click the **Environment Variables** button). The search paths including local paths, network paths or UNCs (Universal Naming Conventions). Using the Path Configuration, the path entries are added in the **Environment Variables** window for the users in the network.

Step 1: Name the Configuration

Provide a name and description for the Path configuration.

Step 2: Define Configuration

Specify the path to be added to the environment variables. Multiple paths can be specified separated by a semi-colon (**;**). Click the ☆ icon to select and assign a dynamic variable to the Path variable.

Step 3: Define Target

Using the Defining targets procedure, define the targets for deploying the Path Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Path Configuration in the defined targets. The configurations will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Power Management for Users

Table of contents

Introduction to power management

The Power Management Configuration enables you to adjust your power settings to save energy. You can add, modify, and delete power schemes for users from a central point. You can cut down the cost that is spent on power, when the users are off-desk. You can create specific power schemes and apply it to users via configurations.

Desktop Central supports power management only if the user logs onto a computer running Windows Vista or later versions. You can perform the following operations by creating power schemes:

Action to be performed	**Impact on the target**
Turn Off the display	Computer's display will be turned off and the power consumption will be reduced reasonably

Turn Off to Sleep	Computer turns to standby mode, all working files/data will be stored on memory. Power consumed will be relative very low
System Hibernate	All working files/data will be stored on the hard disk and turns off the computer. Zero power is consumed
Turn Off Hard disk	Only the hard disk will be turned off, computer will not be shutdown. Power consumption will be cut down considerably

The above listed operations can be executed on the computers based on the idle time and mode of power supply such as plugged in and battery mode. After customizing the power schemes, you can choose to apply the power scheme as follows:

- **Overwrite the existing power schemes** with the latest one, that you have created. If more than one power scheme exists with the same name, you can choose to overwrite the previous one with the latest.
- **Set the newly created power scheme as active power scheme**, if you do not set it as active, then the power scheme will be deployed to the computer. You will have to apply/activate it manually for the power scheme to work.
- You can choose to **enable**, **support for hibernate**. If you do not enable support for hibernate, then the option to hibernate will not work, even if it is specified in the power scheme.

You can create/modify/delete power schemes using Desktop Central by navigating to Power Management configuration by clicking on configurations tab from Desktop Central web console. You can choose to create customized power schemes or modify the default power schemes provided by the operating system. Windows provides, three schemes such as Balanced, High Performance and Power Saver schemes. If you wish to delete a power scheme, you will have to specify the name of the power scheme and deploy it to the target computers.

You can execute advanced options like:

- Prompting for password, when the computer resumes from sleep
- Actions which needs to be performed, when the laptop's lid is closed
- Actions to be performed, when the power button is pressed
- Actions to be performed, when the sleep button is pressed

These actions can be customized, based on the mode of power, like plugged in mode or when it runs on battery.

Configuring Power Options

The Power Management Configuration enables you to adjust your power settings to save energy. You can add, modify, and delete power schemes for users from a central point.

Step 1: Name the Configuration

Provide a name and description for the Power Management Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create/Modify a Power Scheme
- Delete a Power Scheme

Create/Modify a Power Scheme

To create a new scheme, select the **Create Scheme** tab of the Power Management Configuration. Select the **Modify Scheme** tab to modify an existing scheme. Specify the following values:

Parameter	**Description**
Power Scheme*	The name of the power scheme that has to be created/modified. If you are modifying a default scheme, select the Default Scheme option and select the scheme.
Overwrite if scheme already exits	Select this option to overwrite the scheme, if one with the same name exists. This option is only available for create scheme.
Set as active power scheme	Select this option if you wish to make this scheme active. Clearing this option will only create or modify the scheme and the system will

	continue to use the previously applied scheme.
Turn Off Monitor	Turns off the monitor after the specified period of inactivity. Select the period from the combo box.
Turn Off Hard Disk	Turns off the hard disk after the specified period of inactivity. Select the period from the combo box.
System StandBy	The system goes to the standby mode after the specified period of inactivity. Select the period from the combo box.
System Hibernate	Turns off the computer after saving everything in memory to the hard disk after the specified period of inactivity. When the system is turned on again, it is restored to the same position. Select the period from the combo box.
Advanced Options	
Enable Hibernate support	Select this option to enable hibernation of the computer.
Always show icon on the taskbar	Select this option to display the power icon in the system tray.
Prompt for password when computer goes off StandBy	Select this option, if you wish the user to authenticate himself/herself when the computer is resumed from standby mode.

When I close lid	Select the action to be performed on closing the lid. It can be either left as such or made to go to the standby mode.
When I press the power button on my computer	Select the action to be performed when the power button is pressed from the following options: ● Do nothing - to leave it as such ● Ask me what to do - to prompt the user ● Standby - to go to the standby mode ● Shutdown to shutdown the computer
When I press the sleep button on my computer	Select the action to be performed when the sleep button is pressed from the following options: ● Do nothing - to leave it as such ● Ask me what to do - to prompt the user ● Standby - to go to the standby mode ● Shutdown to shutdown the computer

* - denotes mandatory parameters
While creating new schemes, you can select any of the default schemes from the list to load its values and then modify it to suit your need.
If you wish to create/modify more schemes, click **Add More Scheme** button and repeat step 2. The defined scheme gets added to the **List of Power Schemes added** table.

Delete a Power Scheme

To delete an existing power scheme, select the Delete Scheme tab of the Power Management Configuration and specify the name of the scheme that has to be deleted.
If you wish to create/modify/delete more schemes, click **Add More Scheme** button and repeat step 2. The defined task gets added to the **List of Power Schemes added** table.

To modify a scheme from **List of Power Schemes added** table, select the appropriate row and click 📝 icon and change the required values.

To delete scheme from **List of Power Schemes added** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Power Management Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Power Management Configuration in the defined targets. The Power Management configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Configuring Registry Settings

Table of contents

The Registry Settings allows you to add, modify, and delete the values in the registry of the users. Desktop Central Registry Settings Configuration enables you to modify the values in the registry centrally and for several users.

Step 1: Name the Configuration

Provide a name and description for the Registry Settings configuration.

Step 2: Define Configuration

You can choose to either **configure manually** or **import registry files.**

You can perform the following actions:

- Write Value
- Delete Value
- Add Key
- Delete Key

Write Value

To write a value in the registry, select the **Action** as *Write Value* and specify the following values:

Parameter	**Description**
Header Key	Select the header key from the following options: ● *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. ● *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. ● *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. ● *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value.
Type	The type of the value. This varies with respect to the Header Key selected. Select the appropriate type from the combo box.
Value	Specify the value to be added. Click the ☆ icon to select and assign a dynamic variable to this parameter.
Data / Expression	Specify the data or expression. If the new value has to be created without data, enter the word clear inside the parentheses as (clear). Click the ☆ icon to select and assign a dynamic variable to this parameter.

If you wish to write more values, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Value

To delete a value from the registry, select the **Action** as *Delete Value* and specify the following values:

Parameter	**Description**
Header Key	Select the header key from the following options: ● *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. ● *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. ● *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. ● *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value.
Value	Specify the value to be deleted.

If you wish to delete more values, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Add Key

To add a registry key, select the **Action** as *Add Key* and specify the following:

Parameter	**Description**

Header Key	Select the header key from the following options: ● *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. ● *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. ● *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. ● *HKEY_USERS/.Default*: It has the default profile preferences.
Key	Keys are sub-components of the hives. Specify the key value to be added.

If you wish to add more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

Delete Key

To delete a registry key, select the **Action** as *Delete Key* and specify the following values:

Parameter	**Description**
Header Key	Select the header key from the following options: ● *HKEY_CLASSES_ROOT*: It has all file associations, OLE information and shortcut data. ● *HKEY_CURRENT_CONFIG*: It has the currently used computer hardware profile. ● *HKEY_CURRENT_USER*: It has the preferences for the user currently logged in. ● *HKEY_USERS/.Default*: It has the default profile preferences.

Key	Keys are sub-components of the hives. Specify the key value that has to be deleted.

If you wish to delete more keys, click **Add Registry Settings** button and repeat step 2. The values gets added to the **Registry Settings** table.

To modify a registry setting from the **Registry Settings** table, select the appropriate row and click 📝 icon and change the required values.

To delete a registry setting from the **Registry Settings** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Registry Settings Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Registry Settings Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Managing Shortcuts

Table of contents

The shortcut is an icon that points to a file, folder or an Internet URL. The Shortcut Configuration enables you to add shortcuts to the users from a central point.

Step 1: Name the Configuration

Provide a name and description for the Shortcut Configuration.

Step 2: Define Configuration

You can perform the following actions:

- Create a Shortcut
- Create an Internet Shortcut
- Delete a Shortcut / Internet Shortcut

Create a Shortcut

To create a shortcut, select the **Action** as *Create Shortcut* and specify the following values:

Parameter	**Description**

Shortcut Name*	Specify the name of the shortcut.
Target Application*	Browse and select the target application from the network for which a shortcut has to be created. The target application can also be in the local machine where the configuration is being deployed.
Arguments*	If the application requires any arguments, specify the arguments. Leave it blank if it does not require any arguments.
Shortcut Location	Select the location to create the shortcut. The shortcut location can be any of the following: ● *User Desktop*: Refers to the desktop of that user. ● *User Favorites*: Refers to the favorites folder of that user. ● *User Start Menu*: Refers to the start menu of that user. ● *User Programs Group*: Refers to the Start --> Programs group of that user. ● *User Startup Group*: Refers to the Start --> Programs --> Startup group of that user. ● *User Quick Launch Bar*: Refers to the quick launch bar of that user. ● *All Users Desktop*: Refers to the desktop common for all the users. ● *All Users Start Menu*: Refers to the start menu common for all users. ● *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. ● *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.

Start In Folder*	Some applications may have some references to additional files during execution. In such cases, browse and select the location from where the application has to be started.
Shortcut Comments	Specify the comments for this shortcut.
Icon File*	Browse and select the icon for the shortcut.
Run Window	Select how the application has be started - *Normal*, *Maximized*, or *Minimized*.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Note: If you wish to create more shortcuts, click **Add Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

Create an Internet Shortcut

To create an Internet shortcut, select the **Action** as *Create Internet Shortcut* and specify the following values:

Parameter	**Description**
Shortcut Name*	Specify the name of the Internet shortcut.
Target URL*	Specify the URL for which the shortcut needs to be created.

Shortcut Location	Select the location to create the shortcut. The shortcut location can be any of the following: ● *User Desktop*: Refers to the desktop of that user. ● *User Favorites*: Refers to the favorites folder of that user. ● *User Start Menu*: Refers to the start menu of that user. ● *User Programs Group*: Refers to the Start --> Programs group of that user. ● *User Startup Group*: Refers to the Start --> Programs --> Startup group of that user. ● *User Quick Launch Bar*: Refers to the quick launch bar of that user. ● *All Users Desktop*: Refers to the desktop common for all the users. ● *All Users Start Menu*: Refers to the start menu common for all users. ● *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. ● *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.
Icon File*	Browse and select the icon for the shortcut.

Delete a Shortcut / Internet Shortcut

To delete a shortcut, select the **Action** as *Delete Shortcut / Internet Shortcut* respectively and specify the following values:

Parameter	**Description**

Shortcut Name	Specify the name of the shortcut. Click the icon to select and assign a dynamic variable to this parameter.
Shortcut Location	Select the location from where the shourcuts needs to be deleted. The shortcut location can be any of the following: ● *User Desktop*: Refers to the desktop of that user. ● *User Favorites*: Refers to the favorites folder of that user. ● *User Start Menu*: Refers to the start menu of that user. ● *User Programs Group*: Refers to the Start --> Programs group of that user. ● *User Startup Group*: Refers to the Start --> Programs --> Startup group of that user. ● *User Quick Launch Bar*: Refers to the quick launch bar of that user. ● *All Users Desktop*: Refers to the desktop common for all the users. ● *All Users Start Menu*: Refers to the start menu common for all users. ● *All Users Programs Group*: Refers to the Start --> Programs group common for all the users. ● *All Users Startup Group*: Refers to the Start --> Programs --> Startup group common for all the users.

Note: If you wish to delete more shortcuts, click **Add More Shortcut** button and repeat step 2. The defined shortcut gets added to the **Shortcut** table.

To modify a shortcut from the **Shortcut** table, select the appropriate row and click icon and change the required values.

To delete a shortcut from the **Shortcut** table, select the appropriate row and click icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Shortcut Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Shortcut Configuration in the defined targets. The shortcut configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Configuring WiFi

Configuring WiFi profiles for all the managed windows devices in the network is made easy using Desktop Central. You can now create, modify or delete WiFi configurations. Desktop Central supports WiFi configurations only for computers running Windows Vista or later version. You can choose to remove all the existing WiFi profiles and create/apply newly created WiFi profiles. You need to ensure that the WiFi adapter is enabled on all the target computers for deploying a WiFi profile. You can turn on the WiFi adapter while creating a new WiFi profile. You can navigate to WiFi configuration by clicking on Configurations from Desktop Central web console and choose to create/modify or delete WiFi configurations.

- Creating WiFi Profiles
- Modifying WiFi Profies
- Deleting WiFi Profiles

Multiple Profiles can be added in a single configuration, which could include delete/modify and create WiFi profiles. Profiles within a configuration will be applied as per the sequence it is specified. If you have chosen to delete all configurations first, then all the existing WiFi profiles will be removed from the computer and then the second profile will be added.

Creating WiFi Profiles

You can create one or more WiFi profiles for the target computer. You can choose to remove all the existing WiFi profiles before deploying the newly created profiles. You will have to follow the steps mentioned below to create a WiFi profile. There are 2 ways to create a WiFi profile, they are :

- Creating a New Profile
- Importing from an existing Profile

Creating a New profile:

You will have to provide the following details

- Profile Name : Name for the WiFi configuration

- Security Type : No Authentication / WEP / WEPA2 Personal / WPA Personal / WPA2 Enterprise / WPA Enterprise / 802.1x
- Encryption Type : Specify the encryption type as required
- If you have chosen the security type as 802.1x, this is considered to be more secure than WPA and WEPA2 Personal.
- You can also choose to connect the WiFi that you have configured automatically
- Establish connection even if the network is not broadcasting
- Choose to overwrite if any existing profiles exists with the same name

Importing from an Existing Profile

You can choose to import an existing WiFi profile and deploy the same to the target computers. WiFi profile should be located and uploaded in the Desktop Central server. Desktop Central currently supports WiFi profiles only in xml format.

Modifying the WiFi Profiles

You can choose to modify the existing WiFi profiles by creating a new profile with the required modifications. When a profile is created with a name which already exists on the target computer, then the previous profile will be modified, however the changes will apply only to the computers to which the configuration is applied. Modifying WiFi profiles will not work, if the network adopter is disabled on the device.

Deleting WiFi Profiles

You can choose to delete one or all the WiFi profiles that exists on the target computer. It is always recommended to use Delete All option only as the first profile in the configuration. When Delete All profile is applied, all the existing WiFi profiles applied for the users, will be removed from the target computer and the newly added profiles will be applied. You can choose to delete a specific profile by specifying the name of the profile which needs to be deleted.

Mapping Network Drives

Table of contents

The Drive Mapping configuration enables you to map a remote network resource to the user machines. The mapped resource can then be accessed from the local machine using the drive name.

Step 1: Name the Configuration

Provide a name and description for the Drive Mapping configuration.

Step 2: Define Configuration

The table given below list the parameters that have to be specified for mapping a network drive:

Parameter	Description
Drive Name	The drive letter that has to be mapped with the resource.
Resource to be Shared	The shared resource in the network that has to be mapped.
Hide from Windows	To specify whether the mapping has to be hidden in the

Explorer	Windows Explorer. Select this option, if you want to hide.
Drive Label	The label name for the mapped drive that has to displayed in Windows Explorer.
Preferences	You can set preferences to either skip or over write if the drive already exists or to disconnect all the existing drives before mapping the new one.

1. To map more network drives, click **Add More Drives** and repeat Step 2. The mapped drive gets added to the **List of Drives to be Mapped** table.
2. To modify a mapping from this table, select the appropriate row, click ✎ icon and change the required values.
3. To delete a mapping from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Drive Mapping Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Drive Mapping Configuration in the targets defined. The configurations will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Configuring Display Settings

Table of contents

The Display Configuration is for customizing the display settings for wallpaper and screensaver. In addition to this, the DPI settings for font can be set.

Step 1: Name the Configuration

Provide a name and description for the configuration.

Step 2: Define Configuration

The table below lists the display settings that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
Wallpaper	

Action	Specify one of the following action: ● Retaining the existing Wallpaper - Will not make any changes to the present settings ● Disable the Wallpaper - Wallpaper will be disabled and a blank screen will be displayed ● New Wallpaper - Will set a new wallpaper, you can choose to specify the path, if the wallpaper is in a network share or upload it from a stored location.
Position	Specify one of the following action: ● Retaining the existing position - Will not make any changes to the present settings ● Tile - Will display the wallpaper image as multiple smaller tiles on the desktop ● Center - Will set the wallpaper image in the center of the desktop, size of the image will not be modified ● Stretch - Will stretch the image to full screen on the display ● Fit - Will make the image fit to the screen ● Fill - Will fill the wallpaper image on the screen
Permit User to Modify Wallpaper (this is not supported for virtual machines or when a machine is being accessed from a remote computer)	Specify one of the following action: ● Retain Existing Permission - Will not make any changes to the user level permission ● Yes - Will allow the user to modify to the wallpaper ● No - Will restrict the user from modifying the wallpaper
Screensaver	
Action	Specify one of the following action: ● Retaining the existing Screensaver - Will not make any changes to the present settings ● Disable the Screensaver - Screensaver will be disabled ● New Screensaver - Will set a new Screensaver, you can choose to specify the path, if the

	Screensaver is in a network share or upload it from a stored location.
Wait Time	Specify the time limit for the computer to be idle before the Screensaver appears, or retain the existing settings
On resume, display logon screen	Specify one of the following action: ● Retain Existing Settings - Will not make any changes to the existing settings ● Show logon screen - Will prompt the user for password, once the screen is resumed ● Do not show logon screen - Will not prompt for password
Permit User to Modify Screensaver	Specify one of the following action: ● Retain Existing Permission - Will not make any changes to the user level permission ● Yes - Will allow the user to modify to the Screensaver ● No - Will restrict the user from modifying the Screensaver
General	
Rename "My Computer" Icon	Specify the name, that you wish to configure in place of "My Computer". Click the ☆ icon to select and assign a dynamic variable to this parameter
Rename "My Network Places" Icon	Specify the name, that ☆ you wish to configure in place of "My Network Places". Click the icon to select and assign a dynamic variable to this parameter (this feature is supported only for computers running Windows XP or older versions)
Font DPI	Specify one of the following action: ● Retain Existing Settings - Will not make any changes to the existing settings ● Specify the font DPI to be displayed as 100 %

	/125% / 150 % / 200 %
Disable "Windows Welcome Screen"	Will remove the welcome message displayed by Windows (this feature is supported only for computers running Windows XP or older versions)
Disable "Intellimouse Tips Screen"	Will remove the intellimouse tips (this feature is supported only for computers running Windows XP or older versions)
Disable "My Documents" Desktop Icon	Will remove the My Documents" icon from the desktop (this feature is supported only for computers running Windows XP or older versions)

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Display Configuration.

Step 4: Deploy Configuration

1. Click the **Deploy** button to deploy the defined Display Configuration in the targets defined. The configuration will take effect during the next user logon.
2. To save the configuration as draft, click **Save as Draft**.

Managing Files and Folders

Table of contents

The File and Folder Operation allows you to copy, move, rename, delete files and folders of the users. Desktop Central File and Folder Operation Configuration enables you to copy/move/delete files for several users from central location.

Step 1: Name the Configuration

Provide a name and description for the File and Folder Operation configuration.

Step 2: Define Configuration

You can perform the following actions:

- Copy Files and Folders
- Rename/Move Files and Folders
- Delete Files and Folders

Copy Files and Folder

To copy files and folders, select the *Copy* tab and specify the following values:

Parameter	**Description**

Select Action Type	Select the Action from any of the following for HTTP : ● *Files* ● *Files as archive* Select the Action from any of the following for network share: ○ *Copy a File* - To copy a file from one location to another ○ *Copy a File to a Folder* - To copy a file from one location to a specified folder ○ *Copy Multiple Files* - To copy multiple files to a specified folder ○ *Copy a Folder* - To copy a folder from one location to another
Source File	Specify the file that has to be copied. The file can either be in a shared location or in the specified location in the client machines.
Destination Folder	Specify the destination location to copy the files/folders.
Overwrite Existing Files	Select this option to overwrite the existing files.
Create Destination Directory if doesn't Exist	Select this option to create the destination directory, if it does not exist.
Modified, Created, Accessed	Select this option to specify the modified, created or accessed details of the file/folder.

If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Rename/Move Files and Folders

To rename or move the files and folders, select the *Rename/Move* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: ● Rename/Move a file ● Rename/Move a folder
Source File/Folder	Specify the file or the folder that has to be copied
Destination File/Folder	Specify the destination file or the folder.

If you wish to copy more files/folders, click **Add More Action** button and repeat step 2. The values gets added to the **List of File Actions** table.

Delete Files and Folders

To delete the files and folders, select the *Delete* tab and specify the following values:

Parameter	Description
Select Action Type	Select the Action from any of the following: ● Delete a File ● Delete Multiple Files ● Delete a Folder
Source File	Specify the files/folders that has to be deleted
Include Read Only Files	Select this option, if you wish to copy the files even if it has only read-only permissions
Include System Files	Select this option if you wish to copy the system files.

Include Hidden Files	Select this option if you wish to copy the hidden files.
Modified, Created, Accessed	Select this option to specify the modified, created or accessed details of the file/folder.

To modify a file action from the **List of File Actions** table, select the appropriate row and click ✎ icon and change the required values.

To delete a file action from the **List of File Actions** table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the File and Folder Operation Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined File and Folder Operation Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Displaying Message Box

Table of contents

For the users in the network, the pop-up messages with the warning or error can be displayed during the user logon. If the user has already logged on while deploying this configuration, the message will be displayed during the next logon.

Step 1: Name the Configuration

Provide a name and description for the Message Box configuration.

Step 2: Define Configuration

You have an option to create a new message box or delete the existing message box. Select the required option and specify the following:

Parameter	Description
Message Type	The message type as Information, Warning, or error.
Window Title	The title of the message box.
Message	The message that has to be displayed.

Timeout in Seconds	The duration, in seconds, for the message display.
Frequency	Specify at what frequency you want the message box to be displayed - once, during every logon, during subsequent logon or during every logon until a specified time.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Message Boxes Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Message Boxes Configuration in the targets defined. The message will be displayed during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Redirecting User-Specific Folders

Table of contents

The Folder Redirection configuration helps you to change the location of the standard user profile directories to a different location in the network. So, when the user logs in from a different machine in the same domain, he/she will have access to his/her profiles.

Step 1: Name the Configuration

Provide a name and description for the Folder Redirection configuration.

Step 2: Define Configuration

You can perform the following actions:

- **Redirect the folders and copy the existing contents** - This redirects the user-specific folders from the local machine to a network share and copy the existing contents to the new location. You also have an option to exclude specific folders from being copied.
- **Redirect the folders without copying the contents** - This redirects the user-specific folders from the local machine to a network share without copying the existing contents.
- **Restore to default** - Will restore the settings to default (All folders will be pointed to the local machine).

Select the required options and specify the values for the following fields that require change in settings. For each of the fields in the following table, click the **Browse** button next to the corresponding field to launch **Network Browser** window. Select the folder location and click

OK button. If this field is left blank, the corresponding folder settings is left unchanged.

The following table provides a brief description about the user-specific folders that can be redirected using Desktop Central.

User-specific Folder	Description
Start Menu*	Contains the shortcuts that appear in the start menu.
Programs Menu*	Contains the shortcuts that appear in the Programs group of the start menu.
Startup Group*	Contains the shortcuts that appear in Start --> Programs --> Startup menu. This specifies the applications that should be started during the user logon.
Desktop*	Contains the shortcuts and files that appear in the user's desktop.
Favorites [IE Bookmarks]*	Contains the Internet Explorer bookmarks.
Personal [My Documents]*	Contains the personal documents of that user.
Exclude Folders	This option is available only when you choose to copy the existing contents. Specify the folders as comma separated that should not be copied.
My Pictures*	Contains the personal pictures and images of that user.
Cookies*	Contains the cookies used by the Web sites/applications.
History*	Contains the bookmarks of the previously accessed sites.
Recent*	Contains the shortcuts of the recently accessed documents.
Temporary Internet Files*	The temporary Internet files are cached by Internet Explorer in this folder.
Don't copy temporary internet files	This option is available only when you choose to copy the existing contents. Select this option if you do not wish to copy the temporary internet files.
Send To*	Contains the shortcuts listed in the **Send To** sub-menu. The **Send To** sub-menu is displayed in the right-click menu of a file.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Folder Redirection configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Folder Redirection Configuration in the targets defined. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Launching Applications

Table of contents

Launch Application configuration enables you to launch an application during user logon.

Step 1: Name the Configuration

Provide a name and description for the Launch Application configuration.

Step 2: Define Configuration

Select whether the application has to be launched from the local computer or from the network share. If you select the Local option, all the selected target computers should have the application in the same location. Specify the following:

Parameter	Description
Application Name	Browse and select the application that has to be launched. The applications that are available in the local machine from where the application has to be launched can also be specified. Click the ☆ icon to select and assign a dynamic variable to this parameter.

Arguments	Specify the arguments for the application, if any. Click the ☆ icon to select and assign a dynamic variable to this parameter.

1. To launch more applications, click **Add More Application** and repeat Step 2. The added application gets added to the **Launch Application** table.
2. To modify an application from this table, select the appropriate row, click ✎ icon and change the required values.
3. To delete an application from this table, select the appropriate row and click ✖ icon.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the Launch Application Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Launch Application Configuration in the targets defined. The applications configured will be launched during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Configuring MS Office Settings

Table of contents

The MS Office related settings such as Open or Save, Clip Art, User Options, Command Bars, Shared Template, etc can be configured for all the users using Desktop Central MS Office Configuration.

Step 1: Name the Configuration

Provide a name and description for the MS Office configuration.

Step 2: Define Configuration

The MS Office applications that can be configured using Desktop Central are listed in the Choose Application/Suite combo box. Select the application version and specify the values that have to be changed. Leave it blank, if no change is required.

The following table lists the parameters that can be configured for each MS Office applications:

Parameter	Description
Word	
Open/Save Folder*	Refers to the default working folder for Microsoft Word. Clicking Open or Save menu will open this folder location.

Clip Art Folder*	Refers to the default Clip Art folder. This opens when you insert an image from the clip art.
User Options Folder*	Refers to the folder where the user options are stored.
Tools Folder*	Refers to the folder where the office tools are stored.
Auto Recover Folder*	Refers to the folder where the recovered files are stored due to the system crash.
Startup Folder*	Refers to the location where the templates and add-ins are loaded during the startup of Microsoft Word.
Excel	
Open/Save Folder*	Refers to the default working folder for Microsoft Excel. Clicking Open or Save menu will open this folder location.
At startup, open all files in*	Refers to the folder containing the files that have to be opened during startup.
Access	
Open/Save Folder*	Refers to the default working folder for Microsoft Access. Clicking Open or Save menu will open this folder location.
Command Bars Folder*	Refers to the location where the command bar buttons of Microsoft Access are stored.
PowerPoint	
Open/Save Folder*	Refers to the default working folder for Microsoft Powerpoint. Clicking Open or Save menu will open this folder location.
Command Bars Folder*	Refers to the location where the command bar buttons of Microsoft Powerpoint are stored.
Office	
Template Folder*	Refers to the location where the Microsoft Office templates are

	stored.
Shared Template Folder*	Refers to the location where the shared Microsoft Office templates are stored.
Outlook	
Journal Item Log File*	Refers to the location where the old journal item file is stored.
Journal Outlook Item Log File*	Refers to the location where the old journal item file that is referred by the journal entry is stored.
Office Explorer Favorites Folder*	Refers to the default location for storing the favorites. Clicking the Add Favorites menu item will store the URLs in this location.
Office Explorer Views Folder*	Refers to the location where the user views are stored.
Print Settings File*	Refers to the file which stores the print styles of the user views.

* - Click the ☆ icon to select and assign a dynamic variable to this parameter.

Step 3: Define Target

Using the Defining Targets procedure, define the targets for deploying the MS Office Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined MS Office Configuration for the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Configuring Outlook Settings

Table of contents

Microsoft Outlook settings such as general settings, new mail arrival, automatic archive, sending a message, message format and handling, and spell check can be configured. The Outlook Configuration is used to configure these settings for the users of the network from a central location.

Step 1: Name the Configuration

Provide a name and description for the Outlook configuration.

Step 2: Define Configuration

The table given below lists the Outlook parameters that can be configured using Desktop Central. Specify the values only if a change is required for a particular parameter, else, leave it blank.

Parameter	Description
General Settings	
Warn before deleting items	To enable or disable the warning message when deleting entries from the *Deleted Items* folder.

Startup in this Folder	The folder which must be opened after the Outlook is invoked. Select from the following options: *Outlook Today*, *Inbox*, *Calendar*, *Contacts*, *Tasks*, *Journal*, *Notes*, and *User-defined*. Select *User-defined*option to make the user configure this option.
Empty the Deleted Items folder upon exit	Select the frequency at which the contents of the *Deleted Items* folder should be cleared when exiting the Outlook. Select *User-defined* option to make the user configure this option.
New mail arrival	
Display a New mail Desktop Alert	To enable or disable the notification message when a new mail arrives.
Play a sound	To enable or disable playing sound when a new mail arrives.
AutoArchive	
Run AutoArchive	To enable or disable the automatic archiving of folder. Specify the required option and choose the frequency at which archiving should be done.
Prompt to AutoArchive	To specify whether to prompt before archiving or not.
Move old items to	The location where the archived files must be stored. Click the ☆ icon to select and assign a dynamic variable to this parameter.
File name	The name of the archived file.
Delete expired items (e-mail folders only)	To specify whether the expired items should be deleted or not.
When sending a message	
Allow comma as address separator	To specify whether comma should be used as a address separator or not.

Automatic name checking	To enable or disable automatic checking for the validity of names in the recipient list.
Message format & handling	
Compose in this Message Format	Select the message format as *HTML*, *Rich Text*, or *Plain Text*. Select User-defined to leave it to the user to configure.
Use Microsoft Word to edit email messages	Specify whether Word should be used as a default editor.
Send a copy of the pictures instead of the reference to their location (only for HTML format)	To specify whether to send pictures along with the mail or not.
Save copies in Sent items folder	To specify whether to save copies in the sent folder or not.
Autosave unsent	To specify whether to save the unsent messages or not. Select the frequency if you are enabling this option.
Spelling	
Always check spelling before sending	To specify whether to check spelling before sending the message or not.
Always suggest replacements for misspelled words	To specify whether to suggest replacement for misspelt words or not.
Ignore words in UPPERCASE	To enable or disable checking words in upper case letters.
Ignore words with numbers	To enable or disable checking words containing numbers.
Ignore original message in replies	To enable or disable checking the spelling of original mails in replies.

Step 3: Define Target

Using the Defining targets procedure, define the targets for deploying the Outlook Configuration.

Step 4: Deploy Configuration

Click the **Deploy** button to deploy the defined Outlook Configuration in the defined targets. The configuration will take effect during the next user logon.

To save the configuration as draft, click **Save as Draft**.

Configure Exchange Profile for Outlook

Table of contents

Configuring mailbox is one of the essential needs for every enterprise. Configuring Exchange profile for outlook users consumes a lot of time and involves effort. Desktop Central helps you in automating this by creating a configuration to create/delete the exchange profile for outlook users.

Creating Exchanging Profile

Configuring mail communication is the first task that needs to be performed for every new user. This routine task can be simplified using Desktop Central. You can choose to create the exchange profile for all outlook users by creating a configuration from **Configurations -> Outlook Exchange Profile**. You will have to specify the following information:

- Profile Name : Display name of the profile. When you create a profile, you can choose to set the newly created profile as default. You can also choose to overwrite the existing profiles if any, exists with the same name.
- Server Name : Name of the Outlook Server, this should be a FQDN or DNS
- User Name : Specify the name of the user for the outlook profile.
- Exchange Account : The name of the exchange account, as it is referred.
- Under Advanced Options, enable 'Use Cached Mode' if you wanted the emails to be downloaded on the user's computers. You can also specify, what type of contents should be downloaded and the location to store it.
- It is always recommended to encrypt the communication between MS Outlook and MS Exchange. Additionally, you can choose to prompt for login credentials by specifying the logon network authentication.
- Specify the mode as either HTTP or HTTPS. Specify the proxy URL, principal name (the only name with which it connects in the certificate) and authentication type.

Exchange profile is ready for outlook users, you can choose the target and deploy the configuration. You can see that you have successfully configured exchange profile for outlook users.

Deleting Exchange Profile

When a user moves out of the organization or role, you can choose to delete the exchange profile deployed using Desktop Central. You can create a configuration, from **Configurations -> Outlook Exchange Profile**. You will have to specify the name of the profile, which needs to be deleted and specify the target before deploying the configuration.

You can now see that Exchange profile has been successfully removed from all the target computers.

Deploying Login Items

Items that appear on the dock, are called as login items. This document will explain the steps involved in adding/removing "Login Items" to computers. Administrators can choose to configure the login items, which need to be mounted/removed when the user logs on. Applying this configuration will set the login items as default. When this configuration is applied, users will not be able to modify the login items.

Adding Login Items

The following steps will explain you on how to add "Login Items" to computers:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Login Items** and choose **Computer**
3. Specify the name and description for the configuration
4. Choose the operation type as "**Add**".
5. Specify the path of the login items, which needs to be mounted during the user logon. You can add more than one login item using the same configuration.
6. Define the **target**
7. Specify retry options if required and deploy the configuration

You have successfully created a configuration to add login items for the computers.

Removing Login Items

Removal of login items, will work only if they are deployed using Desktop Central.

The following steps will explain you on how to add "Login Items" to Computers:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Login Items** and choose **Computer**
3. Specify the name and description for the configuration
4. Choose the operation type as "**Remove**". You can create a configuration to remove one or more login items, or remove all login items which were deployed using Desktop Central
5. Define the **target**
6. Specify retry options if required and deploy the configuration

You have successfully created a configuration to remove the login items for the computers.

Installing Fonts for Computer

Administrators can choose to install specific Fonts for the computers. Applying this configuration will not have any impact on restricting the users to use specific fonts. This configuration can be used, when a specific font needs to be installed for specific computers. Administrators can remotely install the font files to computers which are located in different geographic locations.

Adding Fonts

The following steps will explain on how to deploy "Fonts" to specific computers:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Font** and choose **Computer**
3. Specify the **name** and **description** for the configuration
4. Select the option as Add
5. Upload the **Font** files, which needs to be deployed to the users. Ensure that the uploaded font is in **.otf* or**.ttf** format.
6. Define the **target**
7. Specify **retry options** if required and deploy the configuration

You have successfully created a configuration to deploy fonts to specific computers.

Removing Fonts

The following steps will explain you on how to remove "Fonts" from specific computers:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Font** and choose **Computer**
3. Specify the **name** and **description** for the configuration
4. Select the option as "**Remove**"
5. Upload the **Font** files, which needs to be removed for the users. You can choose to remove one or more Fonts, or remove all Fonts, which were deployed using Desktop Central
6. Define the **target**
7. Specify **retry options** if required and deploy the configuration

You have successfully created a configuration to remove fonts from the target computers. You cannot remove the fonts which were not deployed using Desktop Central.

Securing App installation using Gatekeeper

Overview

Gatekeeper is a security feature that can be provisioned on computers running Mountain Lion or later versions of Mac Operating System. This feature can be used to restrict the users from downloading Apps from the internet, other than the App Store. When users are allowed to download Apps from the internet, there is always a probability for security glitches. Every App that is downloaded or approved by the App Store has been certified against malware, tampered, or security issues. Administrators can use this setting, to allow users downloading Apps from the App Store or identified developers. Apple provides a "Developer ID" to the developers, whose Apps can be trusted. Apple uses the Developer ID to digitally sign the Apps, which means the Gatekeeper can recognize Apps which has a Developer ID and allow installation of such apps.

Secure Installing Apps from Identified Developers and App Store

Administrators can choose to configure the Gatekeeper, which will be applied to specific computers. Applying this configuration to the computer will allow all the communication, from the specific computer through the Gatekeeper. So administrator will have the complete control over the communication, from the computer.

The following steps will explain on how to deploy "Gatekeeper Settings" to computer:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Gatekeeper** and choose **Computer**.
3. Specify the name and description for the configuration .
4. Specify from where download of applications need to be allowed, be it App Store or App Store & Identified Developers or Anywhere.
5. Specify whether to allow 'Control Click' to open such applications.
6. Define the **target**
7. Specify retry options if required and deploy the configuration

You have successfully created a configuration to configure "Gatekeeper Settings" for the computers.

Configuring System Preferences

This document will explain the steps involved in configuring System Preferences to computer. Administrators can choose to configure the System Preferences, which need to restricted on the computer. When this configuration is applied to computer, the Preferences forced by the administrator cannot be modified by the user.

The following steps will explain you on how to deploy "System Preferences" to computer:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **System Preferences** and choose **Computer**
3. Specify the name and description for the configuration
4. Specify the System Preferences, which needs to be restricted for the computer.
5. Define the **target**
6. Specify retry options if required and deploy the configuration

You have successfully created a configuration to mount System Preferences for the computers.

System Preferences:

The following system preferences can be restricted:

- Personal - contains preferences like, Display & Screen Saver, Dock, Displays, Energy Saver, General, Language & Text, Notifications, Security & Privacy and Spotlight
- Network - contains preferences like, Bluetooth, Network and Sharing
- Account - contains preferences like, App Store, Fibre Channel, iCloud, Ink, Internet Accounts, MobileMe and Xsan
- Hardware - contains preferences like, CDs & DVDs, Keyboard, Mouse, Print & Scan, Sound and Track
- System - contains preferences like, Accessibility, Date & Time, Dictation & Speech, Parental Controls, Profiles, Software Update, Startup Disk, Time Machine and Users & Groups
- App - contains preferences like, Flash Player and Java

Configuring Energy Saver

This document will explain you the steps involved in configuring "Energy Saver" to save power that is consumed by computers which are idle in the network. You can use this configuration to reduce the cost spent on electricity. Whenever a computer is not in use, idle and not turned off, the power consumed by computers can be cut short. Power Management is essential for all the enterprises, immaterial of the total number of computers used in the network. Administrators can choose to configure the Energy Saver settings on the computer, using Desktop Central. This configuration will be applied to the computers during the subsequent refresh cycle.

The following steps will explain you on how to deploy "Energy Saver" to computer:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Energy Saver** and choose **Computer**.
3. Specify the name and description for the configuration .
4. Choose **Battery/Power Adapter** and specify the settings like:
    a. Idle time allowed to put the computer to sleep
    b. Idle time allowed to put the computer's display to sleep
    c. Specify whether to put the hard disk to sleep, whenever it is not in use
    d. Startup automatically after a power failure
5. Define the **target**
6. Specify retry options if required and deploy the configuration

You have successfully created and applied Energy Saver settings for the computers.

Configuring Login Window

Administrators can choose to configure the login window, which need to be displayed when the user logs on. Applying this configuration will customize the login window based on the settings specified by the administrator.

The following steps will explain you on how to deploy "Login Items" to computer:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Login Window** and choose **Computer**
3. Specify the name and description for the configuration
4. Choose to configure the details, whichever should appear on the login window:
   a. **Message which should appear on the login window** - Message which should be displayed to the user during logon
   b. **Display Sleep/Shutdown/Restart Buttons** - Shows the buttons on the login window, allows the users to perform any of these operations
   c. **Prompt Users with User Name and Password** - Prompt to enter both user name and password
   d. **List of Available Users** - Shows a list of users, who have previously logged onto this computer like local users, mobile accounts, network users, administrators and option for others
5. You can also choose to specify the Login Options, like :
   a. **Show Password Hint as per Settings** - Displaying hint for password
   b. **Disable Automatic Login** - User will have to logon every time a computer is re-started, or woke up after sleep mode
   c. **Enable Console Login** - Users will have to logon to the Desktop Central console
   d. **Enable External Accounts** - Allow external accounts other than AD accounts
   e. **Allow Guest User** - Allow to login as Guest user
   f. **Enable Fast User Shifting** - Allow to switch user accounts without logging out users
   g. **Log out the user, if the idle time exceeds** - Automatically log out the user, by specifying an idle time limit
   h. **Display Screen saver, if the idle time exceeds** - Display screen saver, by specifying an idle time limit
   i. **Prompt for password after sleep/screen saver mode** - Prompt the user to enter password every time, the user logs on after sleep/screen saver mode

6. Define the **target**
7. Specify retry options if required and deploy the configuration

You have successfully created a configuration to configure Login Window for the computers.

Executing Custom Scripts for Computer

Administrators would have the necessity to execute Custom Scripts, before or after deploying configurations. In some cases, executing custom scripts will help the administrators to perform some of the complex tasks at ease. Custom scripts can be executed during system startup or refresh cycle. The first step in executing a custom script is to add Custom Scripts to the Desktop Central's Script Repository, for them to be deployed to the target users.

Adding Custom Scripts

The following steps will explain you on how to execute "Custom Scripts" to computers:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Custom Scripts** and choose **Computer**.
3. Specify the **name** and **description** for the configuration.
4. Select the operation type as **create**.
5. You can choose the custom script, which has been added in the script repository. If you want to add a new custom script, then it should first be added to the script repository.
6. Specify the arguments if any, needs to be specified.
7. Specify an Exit code, which should be returned when the script is executed successfully.
8. Specify the frequency for this script to be executed, like only once, during every system startup, during subsequent system startup for specified number of times or all system startup until a specified time period.
9. Define the target and execution settings.
10. Deploy the configuration.

You have successfully created a configuration to execute the custom scripts for computers.

Removing Custom Scripts

The following steps will explain you on how to remove "Custom Scripts", which were deployed using Desktop Central:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Custom Scripts** and choose **Computer**.
3. Specify the **name** and **description** for the configuration .
4. Select the operation type as **Delete**.
5. Specify the custom script which needs to be removed, you can also choose to remove all the custom scripts which were deployed using Desktop Central.
6. Define the target and execution settings.
7. Deploy the configuration.

You have successfully created a configuration to delete the custom scripts for computers.

Managing Custom Scripts

It is mandatory to add all the custom scripts in the script repository. Custom script files are used to configure the software settings, trigger events, etc in the computer of a network. The custom script for files can be batch (.bat), command (.cmd), Windows Script Host (WSH) files. The WSH files includes the VBScript (.vbs), Java Script (.js), Perl (.php), REXX, Python, sh, scpt, pl, and py files.

Adding the Script Details

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

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Script Repository** link under **Repository**. This invokes the **Script Repository** page.
3. Click the **Add Script** button to invoke the **Add Script** page.
4. Select the script from local disk of the computer by clicking **Browse,** and upload the script
5. Enter the description for the script in the **Description** field.
6. Enter the arguments for the script in the **Script Arguments** field.
7. Specify the exit code, which should be returned, when the script has been executed successfully
8. Click the **Add** button. You can find the script added to the table in the **Script Details** page.
9. Repeat steps 3 to 8 for adding more scripts.

Modifying the Script Details

To modify the Script details, follow these steps:

1. Click the **Admin** tab to invoke the **Admin** page.
2. Click the **Script Repository** link under **Repository**. This invokes the **Script Repository** page.
3. Click the 📝 icon under the **Actions** column next to corresponding **Script Name**.
4. You can choose to edit the script in the default editor which will be open, or you can choose to download the script, modify it and upload the modified version.
5. Click the **Modify** button to complete the process.

Removing the Script Details

To remove the Script details, follow these steps:

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

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

Message Box for Computer

Administrators can create a configuration to display messages using "Message Box" to the users. These messages will be displayed on the user's computer for a time interval specified by the administrator. Users will not have control to close the message box, which will be displayed using this configuration.

Adding Message Box

The following steps will explain you on how to display "Message Box" to Computers:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Message Box** and choose **Computer**
3. Specify the **name** and **description** for the configuration
4. Select the operation type as **create**
5. Specify the type of Message type as "Information, Warning or Error"
6. Enter the Title and Message, which needs to be displayed on the target computer
7. Specify the time interval, for how long should the message be displayed on the computer
8. Specify the frequency for this message to be displayed, like only once, during every system startup logon, during subsequent system startup for specified number of times or all system startup until a specified time period.
9. Define the target and execution settings
10. Deploy the configuration.

You have successfully deployed a configuration to display message to computers.

Removing Message Box

The following steps will explain you on how to remove messages, which were displayed using Desktop Central:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Message Box** and choose **Computer**

3. Specify the **name** and **description** for the configuration
4. Select the operation type as **Delete.** This will remove all the messages, which were displayed using message box configuration.
5. Define the target and execution settings
6. Deploy the configuration.

You have successfully deployed a configuration to remove messages, which were displayed using Desktop Central

Mac User Configuration

When a configuration is deployed for a user, the configuration will take effect during the subsequent user logon. For example, you are applying a configuration to a user "X". If user "X" is active while deploying the configuration, then the configuration will impact the user only during the subsequent logon. Computer configuration takes precedence over the user configuration.

This document lists the various configurations that can be applied for a user, which are:

- Custom script
- Fonts
- Login Items
- Message Box
- Network Share
- System Preferences
- Web Clips

Executing Custom Scripts

Administrators would have the necessity to execute Custom Scripts, before or after deploying configurations. In some cases, executing custom scripts will help the administrators to perform some of the complex tasks at ease. Custom scripts can be executed during user logon or refresh cycle. The first step in executing a custom script is to add Custom Scripts to the Desktop Central's Script Repository, for them to be deployed to the target users.

Adding Custom Scripts

The following steps will explain you on how to execute "Custom Scripts" to users:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Custom Scripts** and choose **User**.
3. Specify the **name** and **description** for the configuration .
4. Select the operation type as **create**.
5. You can choose the custom script, which has been added in the script repository. If you wanted to add a new custom script, then it should first be added to the script repository.
6. Specify the arguments, if any, needs to be specified.
7. Specify an Exit code, which should be returned when the script is executed successfully.
8. Specify the frequency for this script to be executed, like only once, during every user logon, during subsequent user logon for specified number of times or all user logon until a specified time period.
9. Define the target and execution settings.
10. Deploy the configuration.

You have successfully created a configuration to execute the custom scripts for users.

Removing Custom Scripts

The following steps will explain you on how to remove "Custom Scripts", which were deployed using Desktop Central:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Custom Scripts** and choose **User**.
3. Specify the **name** and **description** for the configuration .
4. Select the operation type as **Delete**.
5. Specify the custom script which needs to be removed, you can also choose to remove all the custom scripts which were deployed using Desktop Central.
6. Define the target and execution settings.
7. Deploy the configuration.

You have successfully created a configuration to delete the custom scripts for users.

Installing Fonts

This document will explain you the steps involved in installing fonts for users. Administrators can choose to install specific fonts for the user. Applying this configuration will restrict the users to use specific fonts. This configuration can be used, when a specific font needs to be installed for specific users. Administrators can remotely install the font files to users who are located in different geographic locations.

Adding Fonts

The following steps will explain on how to deploy "Fonts" to users:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Font** and choose **User**
3. Specify the **name** and **description** for the configuration
4. Select the option as Add
5. Upload the **Font** files, which needs to be deployed to the users. Ensure that the uploaded font is in *****.otf** or**.ttf** format.
6. Define the **target users**
7. Specify **retry options** if required and deploy the configuration

You have successfully created a configuration to deploy fonts to users. You cannot remove the fonts which were not deployed using Desktop Central.

Removing Fonts

The following steps will explain you on how to remove "Fonts" for users:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Font** and choose **User**

3. Specify the **name** and **description** for the configuration
4. Select the option as "**Remove**"
5. Upload the **Font** files, which needs to be removed for the users. You can choose to remove one or more Fonts, or remove all Fonts, which were deployed using Desktop Central
6. Define the **target users**
7. Specify **retry options** if required and deploy the configuration

You have successfully created a configuration to remove fonts from users. You cannot remove the fonts which were not deployed using Desktop Central.

Deploying Login Items

Items that appear on the dock, are called as login items. This document will explain the steps involved in adding/removing "Login Items" to users. Administrators can choose to configure the login items, which need to be mounted/removed when the user logs on. Applying this configuration will set the login items as default. When this configuration is applied, users will not be able to modify the login items.

Adding Login Items

The following steps will explain on how to add "Login Items" to users:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Login Items** and choose **User**
3. Specify the name and description for the configuration
4. Choose the operation type as "**Add**".
5. Specify the path of the login items, which needs to be mounted during the user logon. You can add more than one login item using the same configuration.
6. Define the **target users**
7. Specify retry options if required and deploy the configuration

You have successfully created a configuration to add login items for the users.

Removing Login Items

Removal of login items, will work only if they are deployed using Desktop Central.

The following steps will explain you on how to add "Login Items" to users:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Login Items** and choose **User**
3. Specify the name and description for the configuration
4. Choose the operation type as "**Remove**". You can create a configuration to remove one or more login items, or remove all login items which were deployed using Desktop Central
5. Define the **target users**
6. Specify retry options if required and deploy the configuration

You have successfully created a configuration to remove the login items for the users.

Message Box

Administrators can create a configuration to display messages using "Message Box" to the users. These messages will be displayed on the user's computer for a time interval specified by the administrator. Users will not have control to close the message box, which will be displayed using this configuration.

Adding Message Box

The following steps will explain you on how to display "Message Box" to users:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Message Box** and choose **User**
3. Specify the **name** and **description** for the configuration
4. Select the operation type as **create**
5. Specify the type of Message type as "Information, Warning or Error"
6. Enter the Title and Message, which needs to be displayed on the user's computer
7. Specify the time interval, for how long should the message be displayed on the user computer
8. Specify the frequency for this message to be displayed, like only once, during every user logon, during subsequent user logon for specified number of times or all user logon until a specified time period.
9. Define the target and execution settings
10. Deploy the configuration.

You have successfully deployed a configuration to display message to users

Removing Message Box

The following steps will explain you on how to remove messages, which were displayed using

Desktop Central:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Message Box** and choose **User**
3. Specify the **name** and **description** for the configuration
4. Select the operation type as **Delete.** This will remove all the messages, which were displayed using message box configuration.
5. Define the target and execution settings
6. Deploy the configuration.

You have successfully deployed a configuration to remove messages, which were displayed using Desktop Central

Configuring Network Share for Users

This document will explain the steps involved in configuring Network Share for users. Administrators can choose to configure the Network Shares, which need to be mounted when the user logs on. Applying this configuration will allow the user to access the Network Shares, which will be set as default.

Adding a Network Share

The following steps will explain you on how to create a "Network Share" for users, when they logon to computers:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Network Share** and choose **User**
3. Specify the name and description for the configuration
4. Choose the operation type as "**Add**"
5. Specify the path of the Network Shares, which needs to be created and mounted during the user logon. You can simply enter the path of the network share, if you have chosen "**Simplified View**". If you chosen "**Standard View**", then you will have to enter the details of the network share like:
    1. Protocol Type : SMB/AFP/NFS.
        - i. SMB : This is a Windows protocol, can be used to share its contents with other operating systems.
        - ii. AFP : This protocol is exclusively designed for sharing contents among computers running Mac operating system.

        iii. NFS : This is a Unix protocol, can be used to share its contents with other operating systems.
    2. Host Name of the Network Share
    3. Volume of the Network Share
6. Define the **target users**
7. Specify retry options if required and deploy the configuration

You have successfully created a configuration to add Network Shares for the users.

Removing a Network Share

The following steps will explain you on how to remove a "Network Share" for users, when they logon to computers:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Network Share** and choose **User**
3. Specify the name and description for the configuration
4. Choose the operation type as "**Remove**"
5. Specify the path of the Network Shares, which needs to be removed during the user logon. You can create a configuration to remove one or more network shares, or remove all network shares which were deployed using Desktop Central. You can choose to enter the path of the network share, if you have chosen "**Simplified View**". If you chosen "**Standard View**", then you will have to enter the details of the network share like:
    1. Protocol Type : SMB/AFP/NFS.
        i. SMB : This is a Windows protocol, can be used to share its contents with other operating systems.
        ii. AFP : This protocol is exclusively designed for sharing contents among computers running Mac operating system.
        iii. NFS : This is a Unix protocol, can be used to share its contents with other operating systems.
    2. Host Name of the Network Share.
    3. Volume of the Network Share.
6. Define the **target users**
7. Specify retry options if required and deploy the configuration

You have successfully created a configuration to remove Network Shares for the users.

Configuring System Preferences

This document will explain the steps involved in configuring System Preferences for users. Administrators can choose to configure the System Preferences, which need to restricted for the users. Applying this configuration will restrict the users from accessing the System Preferences which includes personal, network, account, hardware, system, and Apps. System administrators use this configuration to secure users from accessing the resources available on the managed computers.

The following steps will explain on how to deploy "System Preferences" to users:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **System Preferences** and choose **User**
3. Specify the name and description for the configuration
4. Specify the path of the System Preferences, which needs to be restricted during the user logon.
5. Define the **target**
6. Specify retry options if required and deploy the configuration

You have successfully created a configuration to mount System Preferences for the users.

System Preferences:

The following system preferences can be restricted:

- Personal - contains preferences like, Display & Screen Saver, Dock, Displays, Energy Saver, General, Language & Text, Notifications, Security & Privacy and Spotlight
- Network - contains preferences like, Bluetooth, Network and Sharing
- Account - contains preferences like, App Store, Fibre Channel, iCloud, Ink, Internet Accounts, MobileMe and Xsan

- Hardware - contains preferences like, CDs & DVDs, Keyboard, Mouse, Print & Scan, Sound and Track
- System - contains preferences like, Accessibility, Date & Time, Dictation & Speech, Parental Controls, Profiles, Software Update, Startup Disk, Time Machine and Users & Groups
- App - contains preferences like, Flash Player and Java

Configuring Web Clips

The shortcut that appears on the system, which can be used to launch the application is called as a web clip. Administrators can choose to configure the Web Clips, which need to be mounted when the user logs on. Applying this configuration will allow the user to access the Web Clips, which will be set as default. When this configuration is applied to user, the items which need to be mounted during the logon cannot be defined by the user.

The following steps will explain you on how to deploy "Web Clips" to User:

1. From **Configurations** tab, navigate to Add Configurations -> Configuration -> Mac.
2. Select **Web Clips** and choose **User**
3. Specify the name and description for the configuration
4. Specify the path of the Web Clips, which needs to be mounted during the user logon.
5. Define the **target**
6. Specify retry options if required and deploy the configuration

You have successfully created a configuration to mount Web Clips for the users.

Linux Configurations

Enterprises today have shown a rapid growth in the usage of Linux. They are being widely accepted as an alternative to traditional operating systems. Along with their ease of installation and usage, Linux offers more flexibility to apply custom configurations. In fact being an open source operating system is one of the main driving factors for its adoption. After adoption, one of the major task for an administrator is to manage such computers, which often consumes a lot of time and effort. Desktop Central helps administrators increase their efficiency by automating all the desktop management activities and managing heterogeneous operating systems from a single console.

Following are the Linux configurations offered by Desktop Central -

- Custom script
- Install Linux patch
- Install/uninstall Linux software

Configuring Collections

Table of contents

A bunch of configurations is known as a Collection. Collection can be deployed in the target client workstation using Desktop Central. The advantages of Collection are -

- The targets are defined once for multiple configurations.
- When the configuration is deployed, it saves time to apply the configuration since collection of configuration is applied in each workstation.

Step 1: Define Collection

1. Navigate to **Collections** from **Configurations** tab.
2. Choose the collection type as **User Collection** or **Computer Collection**. This opens the **Add Collection Wizard**.
3. Provide a name and description for the collection.
4. Choose the configurations that have to added to this collection and click Next. The configurations are specific to the collection type you have selected above.
5. Define the chosen configurations. Refer to User Configurations and Computer Configurations sections for details about the configurations.

Step 2: Define Target

Select the targets for which the configurations have to be applied. Refer to the Defining Targets topic for more details.

Step 3: Save or Deploy Collection

After defining the configurations and targets, click **Finish** to deploy the defined configurations to the selected targets. You also have an option to save the configurations as drafts for later modifications by clicking the **Save as Draft** button.

Configuration Templates

Templates are predefined configurations that help in achieving a specific task. While you can perform any configuration by defining them on your own, templates help in getting things done faster. The following are advantages of templates over normal configurations:

1. Helps to complete the configurations quickly
2. You do not have to know how to achieve a specific task; you just have to select the target computers to apply the configuration
3. You do not have to explore all the supported configurations and then select to define

To view the available templates, navigate to Configurations from Admin tab and click on Templates. This will list all the templates provided by Desktop Central. You can also filter the view by selecting an appropriate category from the combo box. The Type column indicates whether the configuration is applied to Users or Computers.

To use the template, follow the steps below:

1. Select **Admin** --> **Configurations --> Add Configurations --> Templates** to view the templates.
2. Click the Template that has to be applied to view its details; click **Create Configuration** to create the configuration.
3. Using the Defining Targets procedure, define the targets for deploying the configuration.

4. Click the **Deploy** button to deploy the defined Configuration in the targets defined. To save the configuration as draft, click **Save as Draft**.

Desktop Central supports various templates that can be applied to Users/Computers -

- Computer Configuration Templates
- User Configuration Templates

Computer Configuration Templates

- Change local admin account password
- Cleanup Recycle bin to free-up Hard Disk space
- Create Alternate local Admin Account
- Defrag Hard Disk for performance
- Delete local Administrator Account
- Disable/Enable USB storage devices
- Disable Unused local Guest account
- Open MEDC ports for communication
- Restrict CD-ROM access
- Restrict Floppy Access to locally logged on users
- Scan and Fix Hard disk Errors
- Start MEDC Agent Service
- Write Protect the USB Storage Devices

Change local admin account password

To enhance the security, the administrators will prefer to change the password periodically. This template enables you to change the password of the local administrator account in the client machines.

Cleanup Recycle bin to free-up Hard Disk space

This helps in freeing up the hard disk space by removing the unwanted files/data from 18 different locations.

Create Alternate local Admin Account

To keep the computers secured, the administrators will prefer to change the local administrator account periodically. This template enables you to create an alternate local administrator account in the client computers.

Defrag Hard Disk for performance

A fragmented disk reduces the performance. It is recommended to defragment the disk periodically to improve the hard disk performance.

This template enables defragmentation of the hard disk at the scheduled time.

Delete local Administrator Account

This template enables you to delete the local administrator account in the client computers.

Disable/Enable USB storage devices

To prevent data theft, the administrators prevent the users from using USB drives. These templates, when applied to client computers, either prevent from using the USB drives or allow them to use.

Disable Unused local Guest account

Unused guest accounts are vulnerable points for the hackers. It is recommended to delete or disable any unused guest accounts from the client computers to avoid any misuse.

This template helps to disable the unused guest accounts from the client computers.

Open MEDC ports for communication

Desktop Central requires port 8020 for agent server communications and port 8443 for Remote Desktop Sharing. These ports should not be blocked by the Windows Firewall for smooth functioning.

This template, when applied to client computers, will open up these ports to enable proper communication between the agent and server.

Restrict CD-ROM access

This template restrict the users form accessing the CD-ROM drives.

Restrict Floppy Access to locally logged on users

Allowing locally logged on users to access the floppy drives is a vulnerable point for hacking. Administrators prefer to disable access to the floppy drives when the users have not logged on to the domain.

This template helps in restricting the locally logged on uses to access the floppy drives.

Scan and Fix Hard disk Errors

The hard disks have to be periodically scanned for any errors and fix them. This will improve the life and performance of the disk.

This template enables scanning and fixing the hard disk errors in the client machines at the scheduled time.

Start MEDC Agent Service

When Scope of Management is defined, Desktop Central agent is installed in all the client computers that are within the scope. The Desktop Central agent has to be running as a service in the client computers to ensure proper communication with the Desktop Central Server.

This template helps you to start the Desktop Central Agent service in the client computers.

Write Protect the USB Storage Devices

To prevent data theft, the administrators prevent the users from writing data to USB storage devices. This template, when applied to client computers, prevent them from writing any data to the USB storage devices.

User Configuration Templates

- Restrict Network Connections
- Restrict Control Panel Applets
- Proxy configuration for Internet Explorer
- Laptop Power Saver Scheme
- IE Browser restrictions for clients
- Disable Control Panel

Restrict Network Connections

Network properties when changed by the user result in bad network connectivity and unnecessary help desk calls in resolving the problem. This could be avoided by restricting the users from changing the network properties.

This template, when applied to users, will prevent them from changing the network properties.

Restrict Control Panel Applets

To enhance the security, the administrators can restrict the users from accessing specific Control Panel applets. This includes, Add/remove programs, Add/remove hardware, Internet options, Power options and System applet.

Proxy configuration for Internet Explorer

This template can be used to configure proxy server settings in the Internet Explorer browser of the client machines.

Laptop Power Saver Scheme

Establishing correct power settings helps in saving energy costs substantially. This template provides the recommended power settings for Laptops.

IE Browser restrictions for clients

This template restricts users from changing the Internet Explorer settings like Connections, Content, Favorites, Programs, Security, Advanced, History and Save As options

Disable Control Panel

You can use this template to disable the Control Panel completely. When applied to users, the users will not be able to access the Control Panel.

Predefined Configuration Templates

Such templates are predefined configurations that help in achieving a specific task. While you can deploy any configuration by defining them on your own, predefined templates help to get things done faster.

Predefined Templates

To view the list of available templates, navigate to **Templates** from **Configurations** tab. This will list all the templates provided by Desktop Central. You can also filter the view by selecting an appropriate category from the combo box. The templates are tagged as below:

- Control Panel
- Hard Disk Maintenance
- Internet Explorer
- Network
- Power Management
- Proxy Configuration
- Restrict Media
- Security
- Service Management

- System Tools
- USB Security
- User Management
- XP Firewall Management

To use these template, follow the steps given below:

1. Navigate to **Templates** from **Configurations** tab to view the templates.
2. Choose the appropriate template and click **Create Configuration** for creation of a configuration using the selected template.

User-defined Templates

Description

Desktop Central offers user-defined templates using which you can customize, create and deploy configurations that meet your enterprise or business requirements. These templates can also be published to ServiceDesk Plus.

Steps

To create a user-defined template, follow the steps given below:

1. Navigate to Configurations -> Templates.
2. Select **User-defined** as your template type.
3. Click on the **Create Template** option and specify the OS Platform, Configuration Type and Category of your choice.
4. Provide all the required details for creation of the template and click Save.
5. You have successfully created a user-defined template using which a configuration can be created and deployed in no time.

Note-You can also create a user-defined template from a configuration that has been deployed already. To create a template from configuration:

1. Navigate to Configurations tab.
2. In the 'All Configurations' view, select the configuration of your choice.
3. Select Save as Template from the 'Actions' button.
4. Saving a configuration as a template will not include the targets.

Publish user-defined configuration templates to ServiceDesk Plus

This feature is supported only for customers, who have integrated Desktop Central (100139 and above) with ServiceDesk Plus (9325 and above).

Steps to publish user-defined templates from Desktop Central to SDP:

1. Navigate to **ServiceDesk Plus Settings from Admin tab** and modify the features integrated.
2. Enable **Publish user-defined configuration templates** and choose to publish templates manually or automatically.

Note -On selecting 'automatically', every time a template is added to Desktop Central, it will immediately be published to ServiceDesk Plus. On selecting 'manually', you can select the templates of your choice and publish them to ServiceDesk Plus. This can be performed from Configurations -> Templates -> User-defined templates -> Publish to ServiceDesk Plus.

Deploying published user-defined templates from ServiceDesk Plus requests

3. Navigate to ServiceDesk Plus console.
4. Select Admin -> Integrations -> Desktop Central.
5. Under Desktop Central Actions, select 'Resolve requests using templates' option.
6. Select Associate Templates for which Desktop Central's user-defined templates should be enabled.
7. Click on the 'Action Menu' against any request and select 'Resolve Requests Using Templates' option to deploy user-defined configuration templates.

Example:

This example will help you understand how user-defined templates come in handy for administrators when they need to perform business specific administrative tasks regularly.

Scenario

As an administrator, you need to ensure that all the users in your enterprise have access to the printer located in their respective floors.

Solution:

1. Create an 'IP Printer Configuration' with all necessary details and save as Template.
2. A template is successfully created. In the future, whenever a new machine is discovered in your network, you can just deploy this template by specifying the target computers alone. This eliminates the need to create new configurations, thus saving time and manual efforts.

Defining Targets

Table of contents

After defining the configuration, the configuration has to be deployed in the target client workstations. The target client workstations have to be defined for the configurations individually. Defining the targets involves selecting various types of targets given below:

The targets must be defined to deploy the Configuration in the machines of the network. When you add a configuration or collection of configurations, you will find a step for **Defining Targets**. This section explains the procedure to define the target for a configuration or collection of configurations.

To define the targets for deploying the configuration or collection, the targets must be added to the **Target List**. A target can be added, removed or modified in the **Target List**.

Selecting Targets from a Domain

To add target computers and users from a Active Directory based domain, follow the steps below:

1. Select a domain from the list.
2. You can deploy the configuration to any of the following:
    a. **Site** - to deploy the configuration to all the users/computers of that site.
    b. **Domain** - to deploy the configuration to all the users/computers of that domain.
    c. **Organizational Unit** - to deploy the configuration to all the users/computers of that OU.
    d. **Group** - to deploy the configuration to all the users/computers of that Group.
    e. **User/Computer** - to deploy the configuration to the specified users/computers.
    f. **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
    g. **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.
3. After adding the target computers, you can specify the filtering criteria to exclude certain types of users/computers from applying the configuration. Specify the criteria as required.
4. Click **Add More Targets** and repeat steps 1 to 3 for adding more targets.

Note: If you wish to deploy the configuration for users/computers in different domains, use the **Add More Targets** button to add targets from multiple domains.

Selecting Targets from a Workgroup

To add target computers and users from a workgroup, follow the steps below:

1. Select a workgroup from the list.
2. You can deploy the configuration to any of the following:
    a. **Workgroup** - to deploy the configuration to all the users/computers of that

workgroup.

   b. **User/Computer** - to deploy the configuration to the specified users/computers.
   c. **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
   d. **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.
3. After adding the target computers, you can specify the filtering criteria to exclude certain types of users/computers from applying the configuration. Specify the criteria as required.
4. Click **Add More Targets** and repeat steps 1 to 3 for adding more targets.

Note: If you wish to deploy the configuration for users/computers in different workgroups, use the **Add More Targets** button to add targets from multiple workgroups.

Selecting Targets in Remote Offices

To add target computers and users from remote offices, follow the steps below:

1. Select a remote office from the list. The remote office can either be a domain or a workgroup.
2. You can deploy the configuration to any of the following:
   a. **Site** - to deploy the configuration to all the users/computers of that site. This option is only available if the selected remote office is a domain.
   b. **Remote Office** - to deploy the configuration to all the users/computers of that remote office.
   c. **Organizational Unit** - to deploy the configuration to all the users/computers of that OU. This option is only available if the selected remote office is a domain.
   d. **Group** - to deploy the configuration to all the users/computers of that Group. This option is only available if the selected remote office is a domain.
   e. **User/Computer** - to deploy the configuration to the specified users/computers.
   f. **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
   g. **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.
3. After adding the target computers, you can specify the filtering criteria to exclude certain types of users/computers from applying the configuration. Specify the criteria as required.
4. Click **Add More Targets** and repeat steps 1 to 3 for adding more targets.

Note: If you wish to deploy the configuration for users/computers in different remote offices, use the **Add More Targets** button to add targets from multiple domains.

Filter the selected target

You can exclude certain parts of the network which does not require the configuration to be deployed. This is optional when defining the targets. Desktop Central provides the option to exclude the parts of the Windows network. Select the Exclude Target check box to view the available options:

Exclude if Target Type is

The target types can be excluded which are in the lower hierarchy to the target selected in the **Select the target type and define** field. The target type can be excluded using the **Browse** button. Click the **Browse** button next to the required target types under the **Exclude if Target Type is** field to launch **Network Browser** window. Select the target type to be excluded for configuration deployment and click **Select** button. This field is mandatory. The target type can be any of the following (varies based on the target options selected):

- Branch - The branch offices to be excluded
- Domain - The domains to be excluded
- Organization Unit - The OUs to be excluded
- Group - The groups to be excluded
- Computer - The computers to be excluded
- IP Address - The IP Addresses to be excluded
- IP Range - The range of IP Addresses to be excluded
- Custom Group - The custom groups to be excluded

Exclude if Operating System is

The targets with specific Windows OS can be excluded for configuration deployment. Select the options under the **Exclude if Operating System is**field which has to excluded for configuration deployment.

Exclude if Machine Type is

The targets with specific machine type such as Notebook, Tablet PC, Desktop, Member Server, TermServClient, or Domain Controller can be excluded for configuration deployment. Select the options under the **Exclude if Machine Type is** field which has to excluded for configuration deployment.

Modifying a Target

To modify a target in the Target List, follow these steps:

1. Select the 📝 button under **Actions** column in the desired row that has to modified.
2. Change the targets as required and click the **Modify Target** button. The target details are updated in **Target List**.

Deleting a Target

To delete a row in the **Target List**, select the ✖ button under **Actions** column next to target that has to removed.

Defining Execution Settings

When you deploy a configuration to client computers, the deployment could fail in a few computers due to various reasons. In such cases, you can re-deploy the configuration. Desktop Central enables you to automate the redeployment process through the Execution Settings option. This option enables you to do the following:

- Specify whether you want the agent to try to apply this configuration in the computers in which the deployment of the configuration failed
- Choose the number of times you want the agent to try deploying a configuration. You can also specify how many times, out of the number of times that you have specified, you want the configuration to be deployed when:
  - Users log on
  - Computers complete the 90-minute refresh cycle

Based on the specified input, configurations will be re-deployed on the computers till the depolyment is successful or the retry limit has reached.

Configuring Execution Settings

You can configure the execution settings while defining the individual configurations or from the configuration's details view. To configure execution settings you will have to specifty the following:

- Retry Configuration on Failed Targets
- Enable Notifications

Retry Configuration on Failed Targets

Enabling this option, will retry to apply the configuration on the failed targets. You can choose to specify the maximum number of retry attempts. These retry attempts can be executed during the refresh cycle or user logon.

You can break up the number of times you want deployment of the configuration to be retried into the number of times you want it retried during logon or startup and the number of times you want it retried during the refresh cycle. Neither option can be set to zero. For example, if you want an option to be retried 8 times and you set the number of times it should be retried during the refresh cycle to 7, the number of times is should be retried during login or startup will automatically be set as one.

Enable Notifications

Specify the email address, if you wanted to receive email notifications. These notifications will begin when the status is moved to "Ready to Execute". You can also set a frequency for the notifications to be sent. Notification will be sent only if there is any change in the status, from the previous notification. The example below will brief you in detail:

You have deployed a configuration to a target of 10 computers. The notification settings has been configured to "Notify via email every 2 hours for 3 days". The configuration has been moved to Ready to execute status at 10.00 hours. on day 1. The first notification will be sent at 12.00 hours. Assume none of the computers were reachable during the time interval. The notification mail will be sent stating that the configuration is yet to be deployed, and the reason as Agents not reachable.

The second notification should be sent at 14.00 hours, however still none of the computers are reachable, and there is no specific change in the status from the previous notification, then the second notification will not be sent.

Assume 5 computers were reachable at 15.00 hours, then the subsequent notification will be sent as per schedule at 16.00 hours with the status of the configuration.

Managing Configurations and Collections

Table of contents

Clicking on the **Configurations** tab will list the details of the configurations and collections that are defined using Desktop Central. You can view the details of the configurations by clicking the corresponding configuration name. Apart from viewing the configuration details, you can perform the following actions:

- Modify the Configuration/Collection
- Suspend a Configuration/Collection
- Resume a suspended Configuration/Collection

Viewing Status of Configuration/Collection

To view the status of the defined configuration/collection, follow the steps given below:

1. Clicking on the **Configurations** tab will list the details of the configurations and collections that are defined using Desktop Central.
2. The status column provides the current status of the configuration/collection. The table given below lists the various states of the configuration/collection and its description:

Status	**Description**
Draft	Represents the configurations/collections that are saved as draft.
Ready To Execute	Represents the configurations/collections that are ready for execution. This will be the initial state of the deployed configurations/collections. Configurations will be **"Ready to Execute"** status in the following scenarios: ○ While the patch/software is scheduled to be deployed during system startup. ○ If it is specified in Deployment Settings, patches/software will be deployed only during the **Install Between** time ○ If it is specified in Deployment Settings, patches/software will be deployed during the **Install Between** time after the next **system startup**. ○ If it is specified in Scheduler Settings, patches/software will be deployed only during the **Install After** time
In Progress	Represents that the configuration is applied on one or more targets. Will continue to remain in this state until the configurations are applied to all the defined targets.
Suspended	Represents that the configuration/collection has been suspended.

✔ Executed	Represents that the configuration/collection has been applied to all the defined targets.
✖ Failed	Represents that the attempt to deploy the configuration has failed.
✖ Draft Download Failed	Represents that one or more patches / service packs defined in the configuration could not be downloaded from the Microsoft Website.
✔ Retry in Progress	Represents that Desktop Central is currently retrying to deploy the configuration.

3. To view the status of the configurations on individual targets, click the configuration name.

Modifying the Configuration/Collection

To modify a configuration/collection, follow the steps given below:

1. Clicking on the **Configurations** tab will list the details of the configurations and collections that are defined using Desktop Central.
2. All the configurations and collections that are defined are listed here. Click the ✎ icon from the Actions column of the corresponding configuration/collection.
3. Change the values as required.
4. Click **Deploy**.

Suspending the Configuration/Collection

To suspend a configuration/collection, follow the steps given below:

1. Clicking on the **Configurations** tab will list the details of the configurations and collections that are defined using Desktop Central.
2. All the configurations and collections that are defined are listed here. Click the ⛔ icon from the Actions column of the corresponding configuration/collection that has to be suspended.

Note: Configurations that have been applied to targets prior to suspension will not be reverted. Suspending a configuration will only stop further deployments.

Resuming the Suspended Configuration/Collection

To resume a suspended configuration/collection, follow the steps given below:

1. Clicking on the **Configurations** tab will list the details of the configurations and collections that are defined using Desktop Central.
2. All the configurations and collections that are defined are listed here. Click the ▶ icon from the Actions column of the corresponding configuration/collection that has to be resumed.

Configuration Settings

This document explains the recommended settings for configurations. Any configuration when deployed to an OU/Group will have its target modified, whenever a computer is moved into the OU/Group. So, the newly added computers will have to get the configurations, which were applied for the OU/Group. You can choose to specify the frequency for the deployment to happen. You can also specify the time interval to automatically move the unused configurations to trash. Additionally, you can specify the number of days after which configurations from trash will be deleted permanently.

1. Navigate to **Configuration Settings** from Configurations tab.
2. Click **Configuration Settings**
3. Click the checkbox to configure the settings, "**When computer(s) is added to the OU/Group, Apply configuration(s) during:**"
    - **System Startup/User Logon** : Whenever a computer is moved to the OU/Group, then the configurations will be applied during the subsequent system startup/user logon.
    - **During Refresh Cycle after < > hours** : You can specify a time interval for the configurations to be applied. Whenever a computer is moved to the OU/Group, then the configurations will be applied during the next refresh cycle after the specified time interval.
    - Enable the check box to **automatically move unused configurations to Trash** and specify the time interval until which the unused configurations will be retained.
    - Enable the checkbox **Permanently delete configurations which are in trash for < > days** to delete the configurations from trash.

- Click **Save Changes.**

Move Unused Configurations to Trash

A configuration is said to be unused, based on the criteria explained below:

1. If the configuration is not modified and there is no change in the status of the configuration
2. If the configuration creation date exceeds a specified time period and there is no change in the status of the configuration
3. If the configuration was deployed to be applied once and it has been applied on all chosen targets

You can specify a time interval for all the unused configurations to be moved to Trash. Whenever a configuration has been deleted manually, the configuration will be moved to Trash View. Configurations removed from the Trash View cannot be retrieved.

Note: Configurations which are set to be deployed during "every statup/logon", Alerts & collections will not be moved to trash.

Viewing Configuration Reports

The Configuration reports helps the administrators to view the details of the configurations that are applied on users, computers, and based on the configuration type. To view the reports, follow the steps given below:

1. Click the **Reports** tab to invoke the **Reports** page.
2. Click the desired report from the Configuration Reports.

The Configuration Reports includes the following reports:

- Configuration by User
- Configuration by Computer
- Configurations by Type

Configuration by User

This report provides a list of users for whom configurations were applied using Desktop Central. It also provides details about the total number of configurations applied for a particular user and the last configuration and time at which it was applied. Clicking the user name will list the details of the configurations applied for that user.

You also have an option to filter your view based on the time at which the configuration was applied or by the configuration type.

Configuration by Computer

This report provides a list of computers for which configurations were applied using Desktop Central. It also provides details about the total number of configurations applied for that computer and the last configuration and time at which it was applied. Clicking the computer name will list the details of the configurations applied for that machine.

You also have an option to filter your view based on the time at which the configuration was applied or by the configuration type.

Configurations by Type

This report provides you the list of configurations that have been applied on users and computers based on the configuration type. It also provides you the total number of configurations that have been applied for a particular type and the last configuration, and time at which it was applied.

Desktop Central Tools

Desktop Central offers a wide range of tools that come handy for IT administrators on any given day. With these tools by your side, you can perform a variety of operations while troubleshooting that simplifies the whole process of remote troubleshooting.

The following tools are offered by Desktop Central:

1. Remote Control
2. System Manager
3. Remote Shutdown
4. Wake on LAN
5. Chat
6. Announcement
7. Windows System Tools

Remote Desktop Sharing

The Remote Desktop Sharing feature in Desktop Central enables administrators to access remote computers in a network. This Web-based feature enables you to access computers in both Local Area Networks (LAN) and Wide Area Networks (WAN).

Read the following sections to learn more about the Remote Desktop Sharing feature:

1. Prerequisites
2. Making required settings
3. Connecting to remote computers
4. Transferring files
5. Troubleshooting tips

Advantages

The advantages of using the Remote Desktop Sharing feature are as follows:

1. Does not require authentication to gain access to a remote computer
2. Supports viewing and accessing remote computers using Active X and Java Plug-ins
3. Enables administrators to prompt users for confirmation before providing access to a remote desktop

4. Ability to record the remote sessions for audit purpose

Prerequisites for Sharing Computers Remotely

You can access computers in a Local Area Network (LAN) or in a Wide Area Network (WAN) to complete various tasks. Desktop Central supports remote desktop sharing across platforms i.e for Windows, Mac and Linux Operating Systems.

Ensure that the following prerequisites are met before you access computers remotely:

1. Configure Browser Settings
2. Ports that need to be open

Configuring Browser Settings

You are required to configure certain controls in your browser before connecting remotely to a computer.

- Ensure that you configure controls only in the browser from where a remote connection is being established.
- HTML 5 Viewer is supported on the following versions of the browser: Edge (all versions), Internet Explorer 10 and later versions, Firefox 38 and later versions, Google Chrome 31 and later versions and Safari 8 and later versions.

Ports that need to be open

The following TCP ports should be open on the Desktop Central server to establish connection with a remote computer:

- 8443 : Secure port to establish remote connection.
- 8444 : Used to establish remote connection
- 8031 : Secure port for File Transfer
- 8032 : Used for File Transfer

Enabling the **UDP port 8443** will let your viewer directly control your remote agent. However, an initial handshake will happen via Desktop Central server. Know more on different communication modes here.

Ensure that the above mentioned ports are opened on the Desktop Central server and are reachable from the Desktop Central agent as well as the viewer machine.

You can now configure the settings required for establishing remote connection.

Configuring Remote Desktop Sharing Settings

You are required to configure the following before you connect to a remote computer:

1. Configure Settings
2. Configure Screen Recording
3. Configure Performance
4. Configure User-confirmation

Configure Settings

The following options can be customized under Settings, they are:

- General Settings
- Port Settings
- Idle Session Settings

General Settings

i. Select the type of viewer you want to use, to view the remote computer. You can choose either an **ActiveX** or a **Java viewer**. Only Java viewer is supported for Mac computers, even if you have selected Active X, only java viewer will be used for Mac computers.

ii. **Enable Quick Launch Tray :** Notify users that you have connected remotely to their computer (this is not supported for Mac computers).

iii. **Disable Wallpaper :** Disable the wallpaper set by the user during a remote connection (this is not supported for Mac computers).

iv. **Disable Aero Theme** : Disable the Aero theme during a remote connection. This is only applicable for computers that have the Microsoft Windows Vista operating system, and later versions, installed in them (this is not supported for Mac computers).

v. **Blacken the monitor of the client computer :** Blacken the user's monitor during a remote connection. This ensures that the user does not see the changes that are made by the administrator (this is not supported for Mac computers).

vi. **Disable the keyboard and mouse of the client computer :** Lock the keyboard and the mouse of the client computer during remote administration. You can use this option when you want to take full control of the user's computer to complete a task (this is not supported for Mac computers).

vii. **Capture Alpha-Blending :** This enables you to capture transparent windows (this is not supported for Mac computers).

viii. Log the reason for remote connection : Ensure that a reason is entered while connecting remotely to a computer.

ix. **View-only mode :** You can only view remote computer, using this mode. You cannot give any inputs or make changes in the computer that you are viewing.

x. **Hide Remote Cursor** : Enabling this option will hide the mouse movements made on the client computer

Port Settings

1. Enable the check box to use **Secured Connection**
2. Enter the **Gateway Port** number as 8443.
3. Enter the **File Transfer Port** number as 8031

Idle Session Settings

i. Specify the maximum time limit allowed, for the remote session to be idle

ii. Specify the action that needs to be performed when a remote session's idle time limit exceeds, such as disconnect the remote connection or disconnect and lock the remote computer.

Configure Screen Recording

Screen recording enables you to record the entire remote control session that can be used for auditing purposes. This feature is currently supported only for windows operating system. Given below are the operations performed when you have enabled screen recording:

1. When you connect to a computer, the Desktop Central Agent on the computer to which you connect will check for the available hard disk space for saving the video.
2. If sufficient space is available, the session and recording will start and a notification will be displayed on the client computer that this session is being recorded (configurable)
3. After the session is completed, the recorded video is uploaded to the Desktop Central Server. The recorded video is available under the History tab available within the Remote Control tool.

To enable and configure Screen Recording, follow the steps below:

1. Click the **Tools** tab
2. Click **Remote Control**
3. Select the **Screen Recording** tab
4. Select the "Enable Screen Recording" check box and specify the following
    a. Select the required **Codec** that have to be used for compression and decompression of the video. If the selected Codec is not available on the remote computer, the default codec will be used.
    b. Specify the **Frames per Second**. The higher the frames per second will give you a smooth mouse movements, while it also increases the size of the video. If it is just for auditing purposes, it is better to leave it with the default value.
    c. Choose the required **color quality**. Higher the color quality the broader, would be the range of color depth, but also increases the size of the video.
    d. Specify the **maximum storage size** for the recorded videos. When the storage limit exceeds, the previously recorded files are automatically deleted to increase the free disk space.
    e. Specify what should be done when the disk runs out of free space on the remote computer, when the session is in progress. You can either choose to stop the recording and continue with the session or disconnect the session.
    f. If you want only authenticated users to download the recorded videos, then you can enable the check box which will prompt the user for password before downloading the videos.
    g. If you wish to notify the users that the remote control session is being recorded,

select the "Enable User Notification" checkbox and specify the message and notification duration. If you want the notification be permanently displayed throughout the session, select "Always show a notification when recording is in progress" option.

Configure Performance

You can configure the following performance settings to increase the performance of remote session:

1. Compression Settings (this is not supported for Mac computers)

Compression settings includes the following options:

i. Fast: Use this option, when you want the rendering to be faster. The compression ratio will be lower and will consume higher bandwidth comparatively.
ii. Best: Use this option, when you want to optimize bandwidth utilization. The compression ratio will be higher and the User Interface (UI) rendering will be comparatively slower.

2. Color-quality Settings

Selecting an appropriate color-quality level enables you to use your bandwidth effectively during a remote session. Lowering the level of the color quality will decrease the consumption of your bandwidth. This will ensure effective bandwidth consumption.

Note: The default settings for performance settings are as follows:

1. Compression Settings
    1. For LAN (local offices): Fast
    2. For WAN (remote offices):Best
2. Color Quality
    1. For LAN (local offices): High (16 bit)
    2. For WAN (remote offices):High (16 bit)

Configuring Performance Settings

To configure performance settings, follow the steps given below:

1. Click the **Tools** tab

2. Click **Remote Control**
3. Click the **Performance** tab
4. Click ✎ in the **Action** column against the name of the required Remote Office
5. Select the required settings for the following from the dropdown boxes:
    i. Compression
    ii. Color Quality
6. Click **Save**

You have configured the performance settings as required.

Configure User-confirmation

You can send users a message asking for permission to connect remotely to their computers. This option allows you to get confirmation from a user before connecting to their computer. Only Desktop Central users with administrative privileges can configure this option.

If a user is logged in, Desktop Central sends a remote-connection confirmation request for the user's approval. Remote connection is established only if the user approves the request within 30 seconds. If the user does not approve the request within 30 seconds, the remote connection is not established automatically.

If a user is not logged in, the remote connection is established without waiting for a confirmation from the user.

You can also do the following:

1. Set the amount of time you want to give the user to approve the request to allow a remote connection
2. Enter the text that you want the user to see when prompted for confirmation to allow remote control
3. Check the **Always Prompt** checkbox to send a user-confirmation message to users even if they have logged off or in locked state
4. Exclude computers from receiving a user-confirmation message

Making User Confirmation Permanent

One of the prerequisites required to comply with HIPAA is to protect user privacy. Therefore, it is mandatory to get the approval of users before connecting remotely to their computers. Making user confirmation permanent will ensure that you always get the user's consent before establishing a remote connection.

If you choose to make user confirmation permanent you cannot revert the settings.

Using Other Settings After Making User Confirmation Permanent

This section comprises information about how other settings like Always Prompt and Exclude Computers will work when user confirmation has been made permanent.

1. If you enable the **Make User Confirmation Permanent** option. All the computers in your network will receive a user-confirmation message before a remote connection is established.
2. If you check the **Exclude Computers** checkbox after you have enabled the **Make User Confirmation Permanent** option, the following actions will take place:
    i. All computers in your network will receive a user-confirmation message
    ii. Computers in the **Exclude Computers** list will not receive a user-confirmation message
3. If you check the **Always Prompt** checkbox after you have enabled the **Make User Confirmation Permanent** option, the following actions will take place:
    i. All computers in your network will receive a user-confirmation message
    ii. Computers that are locked and users that have logged off will receive a user-confirmation message
4. If you check both the **Always Prompt** and **Exclude Computers** checkbox after you have enabled the **Make User Confirmation Permanent** option, the following actions will take place:
    i. All computers in your network will receive a user-confirmation message
    ii. Computers in the **Exclude Computers** list will not receive a user-confirmation message
    iii. Computers that are locked and users that have logged off will receive a user-confirmation message

Excluding Computers

You can also exclude computers from receiving a user-confirmation message. When you exclude computers from receiving user-confirmation messages, you can connect to them immediately, without an approval from the user.

If you have made the user-confirmation option permanent, check the **Exclude Computers** checkbox to ensure that the computers in the Exclude Computers list do not receive a user-confirmation message before a connection is established.

To exclude computers from receiving a user confirmation message requesting users to allow a remote connection, follow the steps given below:

i. Click the **Tools** tab
ii. Click **Remote Control**
iii. Click the **User Confirmation** tab
iv. In the **Exclude Computers** section, click **Add Computers**
v. Filter computers as required. For example, you can filter the computers by domain
vi. Select the computers that should not receive a confirmation message before you connect remotely to them
vii. Click **OK**

These settings will be effective only when you check the User Confirmation checkbox.

Idle Session Settings

You can enhance the security of remote control feature by using idle session time out feature. When no actions are performed on the remote computer, the session is said be 'idle'. You can specify a maximum time limit for the remote session to be idle. when the idle time limit exceeds the specified time, the session gets disconnected and remote machine will be locked automatically. To configure the idle session settings follow the steps mentioned below;

1. Click the **Tools** tab
2. Select **Remote Control**
3. Click **Settings** tab
4. Click the check box to enable **Idle Session Settings**
5. Specify the maximum time limit allowed for the remote session to be idle.
6. Specify the action that needs to be performed while the idle session exceeds the specified time. Click to enable one of the below mentioned options;
   a. Disconnect the remote connection
   b. Disconnect and lock the remote connection
7. Click **Save Changes.**

You have configured the idle session settings successfully.

Connecting to Remote Desktop

Table of contents

Desktop Central's Remote Control feature enables administrators to access any computer in a Local Area Network (LAN) or a Wide Area Network.

Ensure that you have completed these prerequisites and made the required settings before you connect remotely to a computer.

Using this feature you can do the following:

1. Connect remotely to computers
2. Transfer files between computers
3. Switch between multiple monitors during a remote session

Connecting Remotely to Computers

To connect remotely to computers, follow the steps given below:

1. Navigate to **Tools -> Remote Control**.
2. Click Connect icon to establish connection with a remote computer

You have connected remotely to a computer. You can use the **View Desktop** link to control the user's computer. When you establish a remote session with a Mac computer, and no user has logged on or no user is active then you will not have control over the remote computer's mouse or key board. It is recommended to use "Fast User Switch" option in such cases.

> When you are connecting to a remote desktop for the first time from a specific system, you must log in to the system with local administrative privileges. Subsequent connections from the same machine do not require this, as the necessary ActiveX controls and plug-ins would have got downloaded.

Transferring Files Between Computers

To transfer files to remote computers, follow the steps given below:

1. Navigate to **Tools -> Remote Control**.
2. Click **Connect** against the name of a computer to connect remotely to it
3. On top of the remote connection screen, click **File Transfer**
4. Select the required file from a folder from your computer
5. Click ➡ to transfer it to a folder in the remote computer

You have transferred files to a remote computer.

Switching Between Multiple Monitors

When you establish a remote connection, Desktop Central automatically detects the monitors that are available and displays this information on the ActiveX tool bar. You can choose the monitor that you want to view and can switch between the available monitors whenever you want, during the session.

To switch between multiple monitors during a remote session, follow the steps given below:

1. Navigate to **Tools -> Remote Control**.
2. On the **Computers** tab, in the **Viewer** section, select Active X.

Only the Active X viewer supports viewing multiple monitors during a remote session.

4. In the **Action** column, against the computer that you want to connect to, click Connect
5. Click **View Desktop**

When Desktop Central detects multiple monitors, it automatically adds an icon on the toolbar, which enables you to switch between multiple monitors. It is known as the Multi Monitor icon. The primary monitor gets displayed by default.

6. Click the Multi Monitor icon to switch between monitors

You can now switch between multiple monitors during a remote session.

Controlling a Remote Computer

After establishing connection with a remote desktop, you can complete the same tasks that you do from any computer. For example, you can create and deploy a configuration. You can use the toolbar to complete the following tasks:

Toolbar Icon	Action

Ctrl AltDel	Send a Ctrl+Alt+Delete message to a remote computer
🔄	Refresh the current view. If the computer is locked or no user has logged on, you are required to login
AltTab	Switch between different applications in the remote computer
🖥	Black out a user's monitor so that the user cannot view the tasks that you are completing on the the remote computer
⌨	Lock a user's keyboard and mouse
⌨🔒	Unlock a user's keyboard and mouse
🖥	Gain control to access a user's computer
❌🖥	Give the control back to the user
🔍	Zoom in

🔍	Zoom out
✥	Reset a view to its original size
⛶	Reset the size of the view so that it fits onto the screen
▭	View a remote desktop in full screen mode

Read about known issues and limitations related to sharing desktops remotely, here.

Auditing Remote Access Details

Whenever a user establishes a remote connection using Desktop Central, all the events performed on the remote computer are logged. Clicking the 👤 icon available beside the computer name will list all the remote access made to that computer with the details of the user and the start/end time.

You can also view the history of all the remote connections that have been established, using Desktop Central, in the History tab. The details that you can view are as follows:

1. Date on which the connection was made
2. User name of the user who made the connection
3. Name of the computer which was accessed
4. Time at which the connection was made
5. Duration for which the connection lasted
6. IP address of the viewer
7. Name of the domain from which the viewer logged on

Recording the Remote Session

Desktop Central has a unique facility to record the remote sessions, administrators can configure the remote control settings like quality of the video, file format type,etc. During the video recording the files are stored in the clients computer and at the end of the session, it will be uploaded to the Desktop Central server. sessions are stored are To record the remote sessions follow the steps mentioned below.

1. Navigate to **Tools -> Remote Control**.
2. Click on **Screen Recording** to configure the settings
3. To enable secure recording click on the check box.
4. Select the compressor code to specify the format of the video
5. Specify the frames to be captured every second, this helps in determining the quality and size of the video.
6. Specify the colour quality and also the default storage capacity.
7. Choose the option to discontinue the recording or disconnect the remote session when the client computer runs out of space.
8. Specify whether the user needs to be notified about the recording process
9. Click on the check box to always show a notification while recording or specify the time for notification.
10. Enter the notification message in the box displayed.
11. Click on **Save**.

File Transfer

Desktop Central allows you to remotely access desktops and transfer files between them. The Remote Desktop Sharing mechanism supports remote login to any desktop in your network by any user account that has Remote Control privileges.

File Transfer - Advantages

1. Files can be transferred between both the machines viz.,the one initiating the Remote Control Session and that which is getting connected with.
2. Ability to transfer files across domains and workgroup machines.
3. The entire process is fast, reliable, and secure.

File Transfer Ports

The following are the list of ports that need to opened in the Desktop Central Server to enable File Transfer:

For Secure Mode:

For Desktop Central:

- Gateway Port : 8443
- File Transfer Port : 8031

For Desktop Central MSP

- Gateway Port : 8047
- File Transfer Port : 8053

For Non Secure Mode

For Desktop Central:

- Gateway Port: 8444
- File Transfer Port: 8032

For Desktop Central MSP

- Gateway Port: 8048
- File Transfer Port: 8054

The default mode is Secure mode. However to select non-secure mode, click on the *Edit Settings* link in the *Remote Control* page and simply uncheck the "Use Secure Connection" checkbox under the *Port Settings* of *Remote Control Settings* page.

Follow the links to learn more:

- Pre-requisites
- Connecting to Remote Desktop
- Troubleshooting Tips

Troubleshooting Tips

1. I was able to connect to a desktop from remote, but nothing is visible.
2. I am getting an "Access Denied" error when I try to connect to a remote desktop.
3. On connecting to a remote desktop, "The specified service does not exist as an installed service" error is shown.
4. When I select a desktop from the list, the status is always shown as not available, though the system is up.
5. I am getting an "The system cannot find the file specified" error when I try to connect to a remote desktop.
6. I was able to connect to a remote Desktop. But, the display is not proper.

1. I was able to connect to a desktop from remote, but nothing is visible.

Please check the following:

- Whether you have enabled ActiveX controls in the browser from where a connection is established. Refer to the Pre-requisites topic for details on configuration.
- If you are connecting to a desktop for the first time, log in to the system as a local administrator and connect. Subsequent connections from the same machine do not require administrative privileges as the necessary ActiveX controls and plug-ins would have got downloaded.

2. I am getting an "Access Denied" error when I try to connect to a remote desktop.

This error message is shown when the supplied credentials while defining the Scope of Management ( ) is invalid or changed.

3. On connecting to a remote desktop, "The specified service does not exist as an installed service" error is shown.

This error message is shown when the Desktop Central Agent is not installed properly in the client machine. To reinstall the agent, follow the steps below:

1. Click the SoM link from the Quick Links.
2. Select the machines in which the agent needs to be re-installed and click **Install Agent**.

4. When I select a desktop from the list, the status is always shown as not available, though the system is up.

This happens when the client machine has firewall enabled with the "Don't Allow Exceptions" option selected. Disable the firewall to connect to that machine from remote.

5. I am getting an "The system cannot find the file specified" error when I try to connect to a remote desktop.

This error message is shown when one of the required files has been deleted from the client machine. Reinstall the agent as given below:

1. Click the SoM link from the Quick Links.
2. Select the machines in which the agent needs to be re-installed and click **Install Agent**.

6.I was able to connect to a remote Desktop. But, the display is not proper.

Try by changing the screen resolution using the Zoom in / Zoom Out icons.

System Manager

As networks grow, IT departments need to efficiently manage remote computers. Desktop Central's System Manager enables administrators to perform various system management tasks silently with no user interactions. You can monitor the processes, services, software, users and other details about the systems you manage.

To get started with System Manager go to **Tools -> System manager -> Computer Name -> Manage**

The following are the system management tasks that can be performed:

1. Process
2. Services
3. Command Prompt

4. Registry
5. File Manager
6. Event Viewer
7. Device Manager
8. Shares
9. Printers
10. Groups
11. Software
12. Users

Process

The Process tab displays a list of all running processes on managed computers from where you can remotely view, manage and kill processes that are not required.

Services

The Services tab allows to remotely perform actions to start, stop, restart the service as well as set their mode of start up as needed for best performance.

Command Prompt

Using Command Prompt, you can execute commands used to automate tasks via scripts and batch files, perform advanced administrative functions and other DOS operations on managed computers. You can also switch to view the user's command prompt by clicking Run As available in the right corner.

Registry

The Registry contains settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows operating systems. Remote registry displays registry details of managed computers. Using the remote registry, you can:

1. Remotely view the registry of the managed computer.
2. View or modify all keys and values in the Registry of managed computer.

3. Make use of the 'Search option' to identify a key/value/data.
4. Use Export to download registry details of a managed system for troubleshooting purposes.

File Manager

File Manager lets you view the drives of the remote machine. This comes handy when all the files present in remote machine need to be viewed. Additionally, files can be transferred from the local machine to the remote machine.

Device Manager

With Device Manager, you can get the list of devices associated to each computer and choose to enable/disable the drivers related to the devices.

Event Viewer

The Remote Event Viewer displays details of events logged in the managed computer. These logs (classified as errors, information messages and warnings) help in auditing and troubleshooting.

Device Manager

With Device Manager, you can get the list of devices associated to each computer and choose to enable/disable the drivers related to the devices.

Shares

Remote Shares displays a list of all shared folders by the managed computer with path and description given. It allows you to view and manage the shared folders with it's sessions and open files details and also set restrictions for number of users to access.

Printers

This displays the list of printers connected to the managed computer.

Groups

You can view and manage local users and groups of the managed computer. You can also perform actions like adding a new group removing group, adding new members and removing members from group.

Software

Using this, you can view and manage currently installed software of the computer. You can also uninstall a software that is not required.

Users

Using this, you can view the list of users of the managed computers and their current status - active or disabled users.

System Manager Settings

By configuring your system manager settings, you can provide users the permission to access specified tools. You can choose any one of the following options for File Manager and Command Prompt -

1. Enable for all users
2. Enable only for admin
3. Disable for all users
4. Permanently disable for all users

Remote Shutdown Tool

Table of contents

The Remote Shutdown tool of Desktop Central provides options to shutdown, restart, lock and hibernate systems remotely.

Completing Tasks Manually

You can complete the following tasks manually using Desktop Central. You can do this by using the **Shutdown Now** button.

Shutdown Options

When you want to shutdown a computer, you are required to specify the following options for shutting down:

- **Shutdown Mode**

  Choose one of the following options:

  - **Do not disturb if the user has logged in**: Use this option to leave the user undisturbed.
  - **Allow users to skip/postpone the operation**: Use this option to allow Windows and Mac users to either skip or postpone the operation.
  - **Normal**: Use this option to close all the applications, as they would close normally, before shutting down computers
  - **Forced**: Use this option to close all the applications forcibly, before shutting down the computers. You can also use this option when applications are running in the background and you want to shutdown the computer immediately.
- **Timeout**

  Use this option to specify the time in seconds to display a warning message in all the client computers before shutting down. Specify zero to skip the message and shutdown immediately

- **Shutdown Message**

  Enter a message in the field provided. This message will be displayed in all the computers before they are shutdown.

Supported Operations

You can complete the following tasks on a remote computer:

Shutting down a computer

To shut down a computer, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. Click **Shutdown Now**
5. Specify the required settings

6. Click **Shutdown**

You've successfully shut down the selected computers.

Restarting a computer

To restart a computer, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. From the **More Actions** list, select **Restart Now**
5. Click **Restart**

You've successfully restarted the selected computers.

Setting a computer in Hibernate mode

To set a remote computer in Hibernate mode, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. From the **More Actions** list, select **Hibernate**
5. Click **Yes**

You have successfully set the selected computers in Hibernate mode.

Setting a computer to Stand by mode

To set a remote computer to Stand by mode, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. From the **More Actions** list, select **Stand by**
5. Click **Yes**

You have successfully set the selected computers to Stand by mode.

Locking a computer

To lock a computer, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Select the required computers
4. From the **More Actions** list, select **Lock Computers**
5. Click **Yes**

You have successfully locked the selected computers.

Scheduling Automatic Tasks

You can complete the following tasks automatically using Desktop Central. You can do this by using the **Schedule Shutdown** tab.

Creating and Scheduling Tasks

You can create and schedule various tasks. To create and schedule a shutdown task, follow the steps given below:

1. Click the **Tools** tab
2. Click **Remote Shutdown**
3. Click the **Schedule Shutdown** tab
4. Click **Add Shutdown Task**
5. Enter a name for the task
6. From the **Operation** section, select the required type of task
7. Select the required computers
8. Schedule when you want the task to take place:
    - **Once**: Use this option if you want the task to take place only once. Specify a start time and start date.
    - **Daily**: Use this option if you want the task to take place everyday. Specify whether the task should take place on all days or only on weekdays.
    - **Weekly**: Use this option if you want the task to take place on a weekly basis. Specify a start time and the required days of the week.
    - **Monthly**: Use this option if you want the task to take place on a monthly basis. Specify the start time, when you want this task to take place (for example, first Sunday or the day), and months in which you want this task to take place.
10. Click **Save Task**
11. Select the required task
12. In the **Action** column, select **Execute Now**

You have created and deployed a task using the **Schedule Shutdown** tab

Wake on LAN

Table of contents

The Wake on LAN Tool of Desktop Central helps to schedule booting of systems in the Windows Network remotely. It allows you to create different task to group the computers and specify a time to boot the machines in that task.

Waking Up Computers Manually

Desktop Central has the ability to wake up computers within the same subnet and different subnets. When a task is initiated to wake up a computer, the target computer's broadcast address is sent to the Desktop Central agents which are live in that subnet. Desktop Central agent version should be 8.2.93.W or above to perform the wake up task. If you are trying to wake up a computer which belongs to a different subnet, then at least one of the computer in the specified subnet should have a live Desktop Central agent to perform the wake up task.

If you try to wake a computer which belongs to a remote office, then one of the following criteria should be met:

1. IP redirected broadcast should be enabled on the router
2. One of the computer with Desktop Central agent should be live in the same subnet, to perform the task.

You can Wake computers on LAN manually using Desktop Central by following the steps mentioned below:

1. From **Tools** tab, click **Wake On LAN**.
2. This lists all the managed computers in the network. From this list, select the computers that need to be booted and click **Wake Up Now**.

You can see that the wake up process has been initiated and the status will be updated.

When computers running on Windows 8 operating system are shutdown, we will not be able to wake up those computers. To know more details on the work around for waking up those computers, refer this article: http://support.microsoft.com/kb/2776718 .

Creating and Scheduling Wake on LAN Tasks

To create a Wake on LAN task, follow the steps below:

Step 1: Define Task

1. Navigate to Wake on LAN from Tools tab.
2. Click the Schedule Wake Up button to create a new task and specify the following:
    a. Provide a name of the task
    b. Waiting time after wake up: Desktop Central, after broadcasting the Wake On LAN packets, will wait for the period specified here to check the status of the computer.
    c. Resolve IP Address on each schedule: Select this option to resolve the IP Addresses of the machines during every schedule.

Step 2: Select Computers

a. Define the targets that comprise of the list of computers to be booted.
b. Broadcasting of the WOL packtes is based on the subnet address of the computers. If the subnet address is blank or if it is incorrect, the task may fail. You can modify the details such as MAC address, IP address and Subnet mask of the computer by choosing to Modify from under Actions column against the corresponding computer.

Step 3: Define Scheduler

1. *Once:* To run the task only once. You need to specify the date and time.
2. *Daily:* To run the task daily. Specify the time and duration to run the task.
3. *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run.
4. *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months.

Step 4: Deploy Task

Click the **Submit** button to deploy this task. The tasks will be run at the scheduled time and interval. The status of the tasks and its execution history can be verified from the Task Details page.

Viewing and Modifying Wake on LAN Tasks

To view the Wake on LAN tasks that have been created, follow the steps below:

1. Navigate to Wake on LAN from Tools tab. This lists all the tasks that are already created/scheduled.
2. To modify a task, choose to Modify from Actions column against the corresponding task.
3. To delete a task, choose to Delete from the Actions column against the corresponding task.

Viewing Wake on LAN Task Status

To View the status of the Wake on LAN tasks that have ben created, follow the steps below:

1. Navigate to Wake on LAN from Tools tab. This lists all the tasks that are already created/scheduled.
2. Click on the task name to view the status of the computers in that task.
3. You can filter to view the details of the computers by filtering status such as Scheduled, Processing, Success, and Failed.

Configuring Wake on LAN

BIOS Settings

The Wake-On-LAN functionality is generally disabled by default. The option to enable Wake-On-LAN varies with the manufacturer of each computer. The most common method adopted across different PC's are as follows:

1. During the computer’s power-on self-test enter the BIOS setting screen by pressing the F1, INS, or DEL keys.
2. Select **Power Management**.
3. Choose **Wake on LAN/WLAN**
4. Under **Wake on LAN/WLAN**, choose **LAN or WLAN.**
   Note: If you could see a mode called "**Deep Sleep Mode**", ensure that it is **disabled**. This mode can not be found on all the computers.
5. Save and **Exit** the BIOS settings.

Operating System (OS) Settings

In some Windows OS, the drivers can enable the Wake ON LAN features of network adapters. Follow the steps mentioned below:

1. Right click **My Computer** icon, and select **Properties**
2. Click **Device Manager**
3. Under **Network Adapters**, choose "**Ethernet Adapter & Wireless Adapter**".
   Note: The below mentioned operation needs to be performed on both "the Ethernet and Wireless Adapters"
4. Right Click on Ethernet & Wireless Adapter and select properties
5. Click **Power Management** tab
6. Enable the check box against all the below mentioned options:

   a. Allow the computer to turn off this device to save power
   b. Allow this device to wake the computer
   c. Only allow a magic packet to wake this computer
7. Click **OK** to save the settings.

You will now be able to wake the computers using Desktop Central's Wake On LAN.

Chat

The chat feature in Desktop Central enables administrators to communicate with any logged in user within the network and remote locations. You can maintain the chat history of the chat sessions. The following sections will help you in learning more about the chat feature:

1. Prerequisites
2. Setting Up Chat
3. Text chat
4. Voice/Video Chat
5. Troubleshooting tips

Prerequisites

Desktop Central chat uses **port 8443/8444** as a default port. Ensure that you follow the below mentioned prerequisites before trying to connect a chat session.

- Port # 8443/8444 should be open in the Desktop Central Server. If you want to change this port, refer our troubleshooting document.
- Configure your browser to allow pop ups from Desktop Central. In case your web

browser blocks the Pop Up, then you will not be able to see the chat window even if the chat session is initiated successfully.

Setting Up Chat

You can configure the chat history settings even before we initiate the chat session. Follow the steps mentioned below to configure the chat history settings,

1. Click **Tools** -> **Chat**
2. Select **History** and click **History Settings**
3. Enter the number of days for maintaining the chat history. If you choose last 30 days, chat history will be stored only for the last 30 days and the previous chat history files will be deleted (Only logs will be retained for voice/video calls).
4. Click **Save.**

Initiate Text Chat

To initiate the chat session, follow the steps given below:

1. Click **Tools** -> **Chat**
2. Select the name of the user and **Click** 💬 against the specific **user name** under **Action.**
3. Request to connect chat session will be initiated successfully. For more information refer troubleshooting tips.

> **'User name'** lists all the users who have currently logged in the computer. This list will be refreshed every 90 minutes. **In case of a user being logged on multiple computers, then both the computers will be listed against the user name from which you can choose to initiate the chat session.**

Voice/Video Chat

You can initiate a voice and video chat to provide live assistance to your end users. This is applicable only for enterprise edition and UEM edition. There are two approaches to establish communication between technicians and end users:

1. Direct communication
2. Communication via Desktop Central server

For example, consider a scenario where a voice/video call is established between a technician and a user within a same remote location and the Desktop Central server is located in a different site. In this case, the initial connection will be established using the Desktop Central server, however further communication will happen seamlessly without the server's intervention thus optimizing bandwidth consumption as well. In cases where direct connection between technician and user fails, all data transfer will be routed via the Desktop Central server.

For communication via an intermediate component such as the Desktop Central server, you need to ensure:

1. The dynamic port range (49152-65535) should not be blocked by firewall.
2. If you have rerouted Desktop Central Server using NAT settings, then dynamic port range should also be configured according to the NAT settings.

Initiate a Voice/Video Chat

To initiate the chat session, follow the steps given below:

1. Click **Tools** -> **Chat**
2. To initiate a **voice** call, select the name of the user and click 📞 against the specific user name under **Action.**
3. To initiate a **video** call, select the name of the user and click 📹 against the specific user name under **Action**.
4. Request to connect chat session will be initiated successfully. For more information refer troubleshooting tips.

Troubleshooting Tips

1. How to change the port numbers used by chat?
2. What do you mean by 'Agent is not reachable'?
3. What do you mean by 'Chat connection timed out'?
4. I am unable to view a chat window inspite of chat session successfully initiated, why?
5. How often will the list of user names be refreshed?

Changing the port numbers in the Desktop Central server

To change the port number after the Desktop Central server is installed, follow the steps given below:

1. From the Desktop Central web console, navigate to **Admin tab** -> Under Tools Settings -> **Port Settings.**
2. Under Port Details, change the default port numbers for chat settings.

You can now establish chat sessions using the port you have configured.

Agent is not reachable

You might get this error message when you try to connect a chat session. Following are the scenarios when a agent cannot be reached.

- Computer is in hibernate mode.
- Computer is in standby mode.

- Computer is shutdown.
- Computer is disconnected from the network.
- Communication cannot be established between the agent and the server.

In such cases, you can try waking the computers remotely and then establish a chat session once the Desktop Central agent is up and running.

Connection timed out

You will receive the 'chat connection time out' error message if the chat request session has exceeded the maximum time limit of one minute. In such cases you can try to initiate the chat session again.

Chat session successfully initiated but unable to see a chat window

While initiating a chat session, you might face situations wherein the chat session has been initiated successfully but you are still unable to view the chat window. In such cases your web browser might block the pop-up. So, ensure that your browser allows pop-up from Desktop Central.

How frequently will the list of online users be updated?

The list of user names will be refreshed in three scenarios as specified below.

- During 90 minutes refresh interval while the agent communicates with the server.
- During every user logon if it is configured in the User Logon Settings.
- During every user logoff.

Announcement

Table of contents

Announcement feature of Desktop Central allows system administrators to send announcements to all the users within the network. Announcements can be created to be displayed once or at scheduled intervals. Administrators can also customize the start and end date for displaying the announcements.

Creating an Announcement

1. Navigate to **Announcements** from Tools tab.
2. Click **Create Announcement** button
3. Enter a **Title** for the message and a message that needs to be shown on the client computers
4. Specify the start date and the end date for displaying the announcement. If no end date

is specified, then the announcement will be displayed forever.

5. Set the frequency to display the announcement. You can choose to display the announcement once or multiple times. When you want to display the announcement multiple times, you can also specify the time interval for displaying the announcement.
6. Select the **target computers** and save the changes.

Your announcement has been created successfully. It will be displayed on the client computers after the specified start date and frequency mentioned above.

Modifying an Announcement

1. From Tools tab, click on **Announcements**.
2. Select the **Announcement** that needs to be modified
3. Under **Actions** choose to **Modify** and make the necessary changes.

Your announcement has been successfully modified. The modified announcement will be displayed to the targets to which the announcement has not been displayed so far or to the announcements to which it is scheduled to be displayed.

Suspending an Announcement

1. From Tools tab, click on **Announcements**.
2. Select the **Announcement** that needs to be suspended
3. Under **Actions** choose to **Suspend**

Your announcement has been successfully suspended. This announcement will not be displayed to the targets henceforth. You can resume this announcement to continue displaying it in the client computers.

Resuming an Announcement

1. From Tools tab, click on **Announcements**.
2. Select the **Announcement** that needs to be resumed.
3. Under **Actions** click on **Resume**
4. Click **Save** to save the changes.

Your announcement has been successfully resumed. This announcement will be displayed to the targets as per the schedule or to the computers to which it was not displayed before.

Deleting an Announcement

1. From Tools tab, click on **Announcements**.

2. Select the **Announcement** that needs to be deleted.
3. Under **Actions** click on **Delete**

Your announcement has been successfully deleted. This announcement will not be displayed to any computer henceforth.

FAQs

1. What will happen if an announcement is scheduled to be displayed on a computer only once within a specific time period but the computer is inactive?
2. How can I create a new announcement by editing the existing one?
3. What will happen when I suspend an announcement which is scheduled to be displayed only once?
4. What will happen when an announcement is targeted to an user who is logged on in multiple computers?

1. What will happen if an announcement is scheduled to be displayed on a computer only once within a specific time period but the computer is inactive?

If an announcement is scheduled to be displayed on a computer only once within a specific time interval and the target computer is inactive during that time interval then the status of the announcement will be displayed as "expired", which means, the announcement has not been displayed but the time limit has ended.

2. How can I create a new announcement by editing the existing one?

You can follow the steps mentioned below to create a new announcement by editing the existing one:

a. From Tools tab, click on **Announcements**.
b. Select the **Announcement** that needs to be cloned
c. Under **Actions** click on **Save As New**
d. Make necessary changes and Click **Save** to create a new announcement.

3. What will happen when I suspend an announcement which is scheduled to be displayed only once?

If an announcement is suspended, then the announcement will not be displayed to the client computers henceforth. You can resume the announcement in future to continue displaying the announcement. However the announcement will be displayed only if the announcement's end date has not been reached and it will be displayed to computers to which this was not displayed.

4. What will happen when an announcement is targeted to an user who is logged on in multiple computers?

Announcement will be displayed on all the computers wherever the targeted user is logged on.

Windows System Tools

Desktop Central provides various system tools, such as Disk Cleaner, Disk Checker, and Disk Defragmenter, that can be run on multiple computers simultaneously. This section guides you through the process of creating and scheduling tasks to run these tools and to view the status history of the tasks that are executed. Follow the links to learn more:

- Creating and Scheduling Tasks
- Viewing and Modifying the Tasks
- Viewing the Task History

Creating and Scheduling Tasks

Follow the steps given below for creating and scheduling a task to run the Windows system tools in multiple computers :

1. Navigate to **System Tools** from Tools tab. This lists all the tasks that are already created and scheduled.
2. Upon clicking the Add Task button for creating a new task, the Add Task Wizard opens. Follow the below specified instructions to proceed further:

Step 1: Define Task

1. Provide a name and description for the task.
2. Select the tools that you wish to run and click Next.
3. Based on the tool selection, specify the options for executing the task as below:
    - Check Disk: Select the drive that has to be checked and the required options and click Next. You can select from any of the following options:
        - *Verbose* - Displays the name of each file in every directory as the disk is checked.
        - *Quick Check* - This option is only available for NTFS file system. This skips the checking of cycles within the folder structure and performs a less vigorous check of index entries to reduce the time.
        - *Fix Errors on Disk* - Enable this option to automatically fix the errors present in this disk.
    - Disk Cleanup: Select the files and folders to be cleaned and click Next. The following actions can be performed **
        - *Compress old files* - Windows can compress files that you have not used in a while. Compressing the files saves disk space while still enabling you to use them. No files are deleted. Because files are compressed at different rates, the displayed amount of disk space you will gain is approximate.
        - *Remove content indexer* - The Indexing service speeds up and improves file searches by maintaining an index of the files on the disk. These files are left over from a previous indexing operation and can be deleted safely.

- ■ ***Remove downloaded Program Files*** - Downloaded program files are ActiveX controls and Java programs that are downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.
- ■ ***Remove internet cache files*** - The Temporary Internet Files folder contains Web pages that are stored on your hard disk for quick viewing. Your personalized settings for Web pages are left intact.
- ■ ***Remove Office setup files*** - Installation files used by office. If these files are removed from your computer, you may be prompted for original installation media or source during Reinstall, Repair, or Patch operation. It is recommended that you not remove these files unless you always have ready access to your installation media
- ■ ***Remove offline files*** - Temporary files are local copies of network files that you specifically made available offline so that you can use them when you are disconnected from the network.
- ■ ***Remove old check disk files*** - When Chkdsk checks your disk for errors, it might save lost file fragments as files in your disk's root folder. These files are unnecessary and can be removed.
- ■ ***Empty recycle bin*** - The Recycle Bin contains files you have deleted from your computer. These files are not permanently removed until you empty the Recycle Bin.
- ■ ***Remove Temporary files*** - Programs sometimes store temporary information in a Temp folder. Before a program quits, it usually deletes this information. You can safely delete temporary files that have not been modified in over a week.
- ■ ***Remove temporary offline files*** - Temporary offline files are local copies of recently used network files that are automatically cached for you so that you can use them when you are disconnected from the network.
- ■ ***Remove Active Setup Temp Folders***
- ■ ***Remove memory dump files***
- ■ ***Remove remote desktop cache files***
- ■ ***Remove setup log files***
- ■ ***Remove old system restore positions.***
- ■ ***Remove web pages***
- ■ ***Remove uninstall backup images***
- ■ ***Remove webclient and web publisher cache files***

●. Disk Defragmenter: Select the drive that has to be defragmented and the required options and click Next. Seelct from the following options:

- ■ *Verbose*: Displays the complete analysis and defragmentation reports
- ■ *Analyze*: Analyzes the volume and displays a summary of the analysis

report.

- *Force Defragmentation*: Forces defragmentation of the drive regardless of whether it needs to be defragmented.

Step 2: Define Target

Using the Defining Targets procedure, define the targets for deploying the tasks.

Step 3: Define Scheduler

Specify the following scheduling options:

Parameter	Description
Run As*	The name of the user as whom the task will be run. Click the ☆ icon to select and assign a dynamic variable to this parameter, for example, $DomainName\$DomainUserName or $ComputerName\$DomainUserName.
Password	The password of the user.
Confirm Password	Confirm the password again.

Perform this task*	Specify the time to perform the task. You can select from the following options: ● *Daily:* To run the task daily. Specify the time and duration to run the task. ● *Weekly:* To run the task on specific day(s) in a week. Specify the time, start date, and days on which the task has to be run. ● *Monthly:* To run the task specific day every month(s). You need to specify starting time, select a day and select a month/months. ● *Once:* To run the task only once. You need to specify the date and time. ● *At System Startup:* To run the task when the system is started. ● *At Logon:* To run the task during the user logon. ● *When Idle:* To run the task when the system is idle for the specified time.
Advanced Settings	
General	● *Enabled*: Select this option to run the task at the specified time. ● *Run only when logged on:* Select this option to run the task only when the user has logged on.
Scheduled Task Completed	● *Delete the task if it is not scheduled to run again:* Select this option to delete the task when it is no longer scheduled. ● *Stop Task:* Select this option and specify the duration after which the task will be stopped.

Idle Time	Select the required options: ● Specify the duration,the system has to be idle before starting a task. ● Stop the task if the computer ceases to be idle
Power Management	Select the required options: ● Don't start the task if the computer is running on batteries ● Stop the task if battery mode begins ● Wake the computer to run this task

Step 4: Deploy the Task

Click the **Deploy** button to deploy the task in the defined targets. The tasks will be run at the scheduled time and interval. The status of the tasks and its execution history can be verified from the Task Details page. Refer to the Viewing the Task History topic for details.

Viewing and Modifying the Tasks

Desktop Central allows the creation of multiple tasks that can be created to run various actions on different target computers at different intervals. You can view the tasks that are created by following the steps below:

1. Navigate to **System Tools** from Tools tab. This lists all the tasks that are already created and scheduled.
2. To modify a task,
    a. Choose to Modify from the Actions column of the corresponding task.
    b. This opens the **Modify Configuration** Wizard. You can add/remove tools, change the tool options, the target systems, and the scheduled time as required.
    c. Click **Deploy** to effect the changes.
3. To Delete a task, choose to Delete from the Actions column of the corresponding task.

Viewing Task History

Desktop Central provides the details of the tasks executed on the target devices and the access logs of the tool execution.

Viewing Last Execution Status

1. Navigate to **System Tools** from Tools tab. This lists all the tasks that are already created and scheduled.
2. Click on a task to view the details, such as the systems in which the task is executed, the last execution time, and the status of the task execution. Clicking the status will provide the access log of the performed task.

Viewing Task Execution History

1. Navigate to **System Tools** from Tools tab. This lists all the tasks that are already created and scheduled.
2. To view the history of the task executed on a specific system, click the **computer name**. This will provide the history of the task execution on that computer along with the status on each execution. Clicking the **status** will provide the access log pertaining to that execution.

Desktop Central Integrations

Desktop Central is a unified endpoint management solution that helps in heterogenous device management from a single console in a connected and cohesive manner. Desktop Central integrates with several products that make the life of an IT admin much easier.

1. Browser Security Plus : Browser security and management software
2. Analytics Plus : Advanced analytics software
3. ServiceDesk Plus : Help desk software
4. ServiceDesk Plus On-Demand : Help desk software on the cloud
5. Asset Explorer : Inventory management software
6. Spiceworks : Manage incidents seamlessly
7. Zendesk : Meet your SLAs faster than ever
8. Jira : Solve issues in Jira at the click of a button
9. ServiceNow : Centralize all your ITIL processes

Configuring Help Desk Integration

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

Steps to Integrate with Help Desk

1. Navigate to **Help Desk Settings** from Integrations under Admin tab.
2. The **Help Desk Settings** tab is selected by default.
3. Under **Mailing options** section, specify the "To Email addresses" of the help desk and the "From Email Domain", which will be used when emails are sent from the agent tray icon. Refer this: **How do we form "From Email Address?"**
4. Enter the email subject prefix which will be prefixed to all the tickets that has been created from the help desk ticket.
5. Under the **Attachment options** section, enable the screen shot file format type, so that the end user will be notified to attach the screen shot in the correct format.
6. Enable any of the given video recording option, to capture issues in video format. The video recording time will vary based on your screen resolution and rapid screen changes.
   a. Save video in server and send link - Enabling this option will save video in the server and the video download link would be sent.
   b. Send as attachment - Enabling this option will send video as attachment.
7. If you have enabled the option to save video in server and send as download link, specify the number of days to retain video files in the server. If the number of days exceeds, the files will be deleted automatically.
8. If you have enabled the option to send video as attachment, specify the maximum attachment size supported by your configured mail server. If the video exceeds the configured attachment size, recording will not be proceeded further, you can either send the recorded video or discard it based on your requirement.
9. Click **OK** to save the changes.
10. Sharing an attachment (screen capture/video) while creating a helpdesk ticket, might include users private data. It is recommended to inform the users, to verify that no private/critical data is shared.

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

Customizing the Ticket Subjects and Messages

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

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

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

How do we form "From Email Address", when an email is sent from the agent tray icon?

Active Directory based Set Up:

Desktop Central will use the default email address of the user, which is associated with the Active Directory user name. If no email address is mapped for the user, then the "From Email Address" will be formed by using the "From Email domain" which was specified by the administrator. Desktop Central will use this windows network domain name if "From Email Domain" is not specified. When an email is sent from the agent tray icon, then the logged on user's "Active Directory User name" will be prefixed to the network domain name to form the "From Email address". You can also choose to "allow the user's to modify the From Email address", when a mail is sent from the agent tray icon.
Example:

Windows domain is "mycompany.com"

Active Directory user name is "abc-123"

Email domain is "myemaildomain.com"

1. When "From email domain is filled, then the sender's email address will be **abc-123@myemaildomain.com**

2. When "From email domain" is not filled, then the sender's email address will be **abc-123@mycompany.com**

Workgroup based Set Up:

When an email is sent from the agent tray icon, the email domain which is associated with the Workgroup will be prefilled, and the logged on user name will be prefixed to the domain name to form the "From Email address". If this email address cannot be used to send emails, then the user will have the choice to modify the "From Email address". It is recommended to enable the settings which allows the users to modify the "From Email Address".

Integrating Desktop Central with ServiceDesk Plus

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

1. Data related to hardware and software assets
2. Help-desk requests
3. Deploying software packages
4. Initiate Chat Sessions with requesters
5. Broadcast Announcements to computers
6. Complete UI Integration - This makes you access all the features of Desktop Central from the ServiceDesk Plus console.

Benefits

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

1. Get comprehensive information about IT assets like hardware and software assets installed in the computers in your network
2. Log service and configuration requests, made by users as tickets automatically
3. Install software packages from the ServiceDesk Plus console
4. Deploy configurations with the help of predefined and user defined templates from the ServiceDesk Plus console
5. Carry out operations such as lock, restart, hibernate, standby, shutdown, Wake on LAN
6. Perform various system management tasks efficiently from ServiceDesk Plus console

Steps to Integrate

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

1. Authenticating the Integration
2. Integrating Asset Data with ServiceDesk Plus
3. Automatically Log Help Desk Requests as Tickets in ServiceDesk Plus
4. Include Software Install / Uninstall option under the Actions menu of a Help Desk request in ServiceDesk Plus
5. Make a complete UI integration between ServiceDesk and Desktop Central

Authenticating the Integration

Overview

This document will explain you the steps involved in configuring Desktop Central and ServiceDesk Plus integration. The first step in integrating Desktop Central with ServiceDesk Plus is to generate an authentication Key to authenticate the integration. Authentication Key is also called as API Key. Authentication keys should be generated in both the servers, that is Desktop Central and ServiceDesk Plus. The key which is generated in Desktop Central should be entered in ServiceDesk Plus server, and the key which is generated in ServiceDesk Plus, should be updated in the Desktop Central server. All communications between the Desktop Central and the ServiceDesk Plus server will be validated based on these authentication keys.

Authentication Key is mandatory to secure all communications between the Desktop Central and ServiceDesk Plus. Authentication Keys are used to perform the below mentioned operations:

1. Authentication Key generated in Desktop Central and updated in ServiceDesk Plus is used to:
    - Authenticate all communications from Desktop Central server to ServiceDesk Plus will be authenticated only using the authentication key.
2. Authentication Key generated in ServiceDesk Plus and updated in Desktop Central Plus is used to:
    - Install/uninstall software applications
    - Log help desk requests as tickets in ServiceDesk Plus
    - Add work log to remote connections.

Generating Authentication Key in Desktop Central

Note : The following steps are applicable only for customers who are running Desktop Central build # 90109 or later versions and ServiceDesk Plus build # 9033. If you are using Desktop Central running on build number lesser than 90109, or ServiceDesk Plus build number lesser than 9033, then upgrade to the latest version and follow the steps mentioned below.

Authentication key can be created only for the logged on user and the user should have Administrator privilege. To generate an authentication key, You need to login to Desktop Central web console as the user, with administrator privilege and follow the steps mentioned below:

1. Click **Admin** tab on Desktop Central web console
2. Under **Integration,** select **API Key Generation**
3. Against the user name, under **Action**, click **Generate** to generate authentication key
4. Copy the generated key and click **Save** to complete the process

You can now update the copied authentication key in the ServiceDesk Plus server, for the integration to work. The API Key that you have generated should be pasted on the SeriveDesk Plus server in the below mentioned location :

1. Click **Admin**, tab on ServiceDesk Plus
2. Under **General**, choose **ME Integrations**
3. Choose **Desktop Central** and specify the **API Key** under **Server Configuration**.
4. Click **Test Connection and Save** to verify the API key is authentication and communication has been established.

You have successfully generated the API key and established communication with the ServiceDesk Plus server.

Generating Authentication Key in ServiceDesk Plus

To generate an authentication key for ServiceDesk Plus, you should login as a user, with administrator privilege. Follow the steps mentioned below to generate authentication key for a new user.

1. Go to **Admin** tab in **ServiceDesk** Plus
2. Under **Users,** select **Technician**
3. Click **Add New** to create a new technician and fill in the required details.
    1. Enter the name
    2. Enter the required description and specify the privileges required for the technician like, contact information, cost details, department details, assigning the group to technician and select permission.
    3. Check the **Enable login for this technician** checkbox. Enter the following details for the technician:
        i. Login Name
        ii. Password
        iii. Re-type Password
        iv. Domain
    4. Select **Enable Administrator Privileges (SDAdmin)** option

5. Under **API Key Details,** click **Generate/Regenerate** to generate the authentication Key

You have successfully generated the authentication key, which should be copied and pasted in Desktop Central Server -> Admin tab -> Integrations -> ServiceDesk Plus settings -> API key details. You can also generate authentication key for the existing user by editing the **Technician** details, and click **Generate** under **API Key details**. If you wanted to generate authentication key for logged in user, you can click **Personalize** and generate API key.

Integrating Asset Data

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

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

Prerequisites

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

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

Integrating Desktop Central with ServiceDesk Plus

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

1. Click the **Admin** tab
2. In the **Integration Settings** section, click **ServiceDesk Plus Settings**
3. In the **ServiceDesk Plus Settings** section, check the **Enable ServiceDesk Plus Integration** checkbox
4. In the **Service Desk Server Plus Details** section, specify the following details about the **ServiceDesk** Plus Server:
    a. IP address/DNS name
    b. Port number
    c. Required communication protocol
5. In the **Features to Integrate** section, select IT Asset Data checkbox for Desktops & Mobile Devices. If you wanted to integrate asset data of only mobile device, or desktop then you can check the appropriate check box.
6. Specify the settings to post details on the asset data

a. Configure the settings on what action needs to be performed on ServiceDesk Plus, when a comptuer/mobile device is removed from Desktop Central. You can choose to mark the asset as "Disposed" or completely remove the asset details on ServiceDesk Plus. However, this change will not happen vice-versa, no changes made in ServiceDesk Plus will impact the asset details in Desktop Central.

b. You can choose to assign an owner for computers/mobile devices. This data will be posted based on logged-on user for desktops and the user, to whom the device is associated. This data will be posted during every schedule for desktops and every scan for mobile devices.

7. Click **Save**

ℹ If you have chosen the communication protocol as HTTPS, restart your computer for the changes to reflect.

Logging Help Desk Requests as Tickets

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

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

Benefits

The benefits include the following:

1. Submit requests without logging in
2. Send requests using predefined templates and can even attach screenshots automatically.
3. Use customizable subject lines to configure the HelpDesk application and enable automatic assignment of tickets
4. Configure settings in Desktop Central to log the following asset-related alerts as tickets in ServiceDesk Plus. These include alerts related to:
    a. Recently added hardware
    b. Commercial software applications that have recently been installed or uninstalled
    c. Prohibited software applications that have recently been installed
    d. Software compliance issues related to expired licenses or under licensed software applications

Prerequisites

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

1. Ensure that the build numbers conform to the details given below:
    a. Desktop Central: Professional Edition, Build number 70133 or later versions

   a. ServiceDesk Plus: Version 8.0 or later versions
2. Run both Desktop Central and ServiceDesk Plus in your network
3. Manage all the computers in your network using Desktop Central

Logging Help Desk Requests & Alerts as Tickets in ServiceDesk Plus

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

1. Click the **Admin** tab
2. In the **Integration Settings** section, click **ServiceDesk Plus Settings**
3. In the **ServiceDesk Plus Settings** section, check the **Enable ServiceDesk Plus Integration** checkbox
4. In the **Service Desk Server Plus Details** section, specify the following details about the ServiceDesk Plus Server:
   a. IP address/DNS name
   b. Port number
   c. Required communication protocol
5. In the **Features to Integrate** section, select Log Help Desk Requests as Tickets checkbox
6. Click **Save**

If you have chosen the communication protocol as HTTPS, restart your computer for the changes to reflect.

Deploying Software Applications

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

Prerequisites

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

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

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

If you have chosen the communication protocol as HTTPS, restart your computer for the changes to reflect.

Configure Desktop Central Settings in ServiceDesk Plus

- To configure DesktopCentral Settings in ServiceDesk Plus, follow the below given steps
  - Click Admin --> Desktop Central Server Settings
  - Specify the details of the Desktop Central installation like Server Name/IP, Port and the communication details.
  - Click **Save**
- Enable the option to display the install or uninstall software applications option in the Actions menu option in ServiceDesk Plus. You can enable this option in the **Service Catalog** in the Help Desk section in ServiceDesk Plus.

Complete UI Integration with ServiceDesk Plus

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

Prerequisites

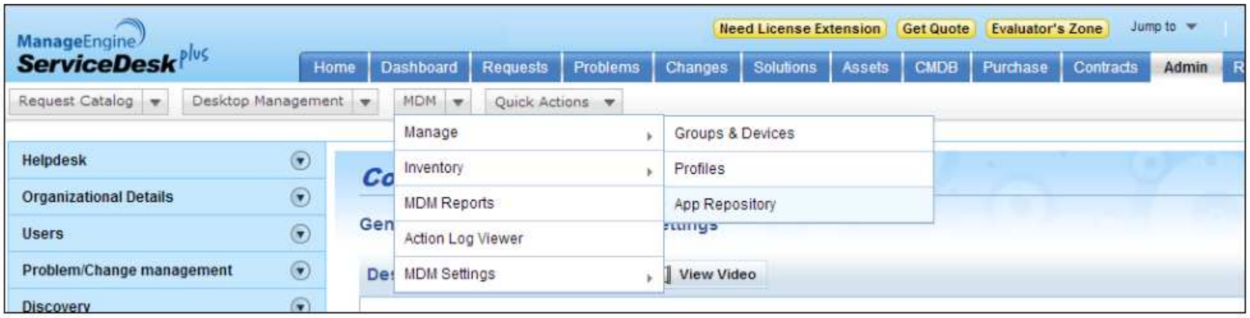
1. Ensure that the build numbers conform to the details given below:
    a. Desktop Central: Professional Edition, Build number 70242 or later versions
    a. ServiceDesk Plus: Build Number 8017 or later versions
2. Run both Desktop Central and ServiceDesk Plus in your network
3. Manage all the computers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

Steps to Integrate Desktop Central UI with ServiceDesk Plus

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

a. Click Admin --> Other ME Products --> Desktop Central
b. Specify the details of the Desktop Central installation like Server Name/IP, Port and the communication details.
c. Select the Enable Desktop Management Menu option.
d. Click **Save**

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



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

Enabling Desktop Management Menu for ServiceDesk Plus Users

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

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

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

1. From the ServiceDesk Plus Web console, select Admin --> Technicians
2. Click the user to whom you should enable Desktop Management menu.
3. Under the Login Details of the user, select "Enable to access Desktop Management Functionality" option
4. Choose what privileges should the user have in Desktop Central:

   a. Admin privilege will have access to all the features
   b. Guest privilege will only have read-only access to Desktop Management functions.
5. Select the required privilege and click Save.
6. Repeat the above steps for every user to whom the Desktop Management menu has to be enabled.

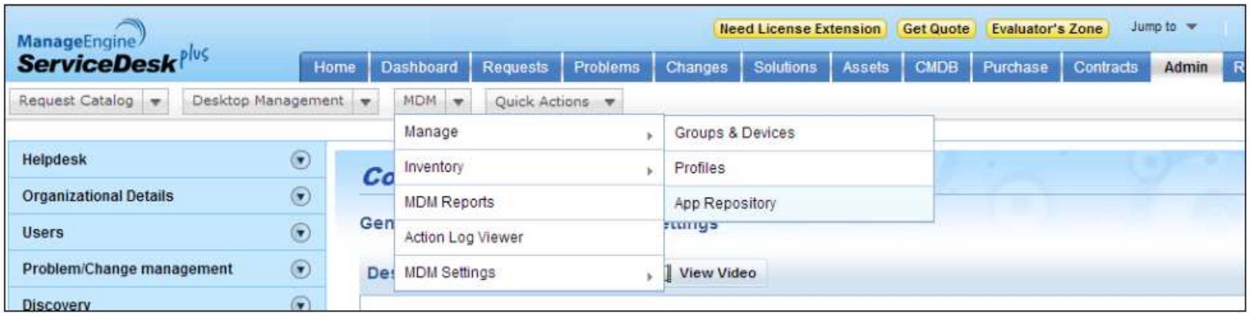
You cannot enable the Desktop Management menu for yourself. You should ask a fellow administrator to enable it for you.

Steps to Integrate Desktop Central MDM UI with ServiceDesk Plus

To integrate Desktop Central MDM UI with ServiceDesk Plus, follow the steps mentioned below;

1. Click **Admin** and select other ME Products and choose **Desktop Central**
2. Click **Enable MDM Menu**.
3. Click **Save**

After enabling the MDM menu, ServiceDesk Plus users, will be able to see a MDM Menu in the ServiceDesk Plus UI



Integrating with ServiceDesk Plus On-Demand

If you are currently using Desktop Central and ServiceDesk Plus On-Demand, you can integrate them and reap the following benefits:

- Procure updated IT asset data from Desktop Central to ServiceDesk Plus On-Demand
- Log help desk requests from the Desktop Central's agent tray icon as tickets in ServiceDesk Plus On-Demand

For the above mentioned features to work, you will have to integrate Desktop Central with the ServiceDesk Plus On-Demand server. There are two stages in integrating Desktop Central with ServiceDesk Plus On-Demand, namely :

- Generate Authentication Key
- Configure Integration Settings

Generate Authentication Key

Authentication key is required for secured data transfer between Desktop Central and ServiceDesk Plus On-Demand. Login to your ServiceDesk Plus On-Demand account as the administrator and access this url: **https://accounts.zoho.com/apiauthtoken/create?SCOPE=SDPOnDemand/sdpodapi**, you can see that the authentication key has been auto-generated. This key does not have any expiry date. You can see a sample key below:

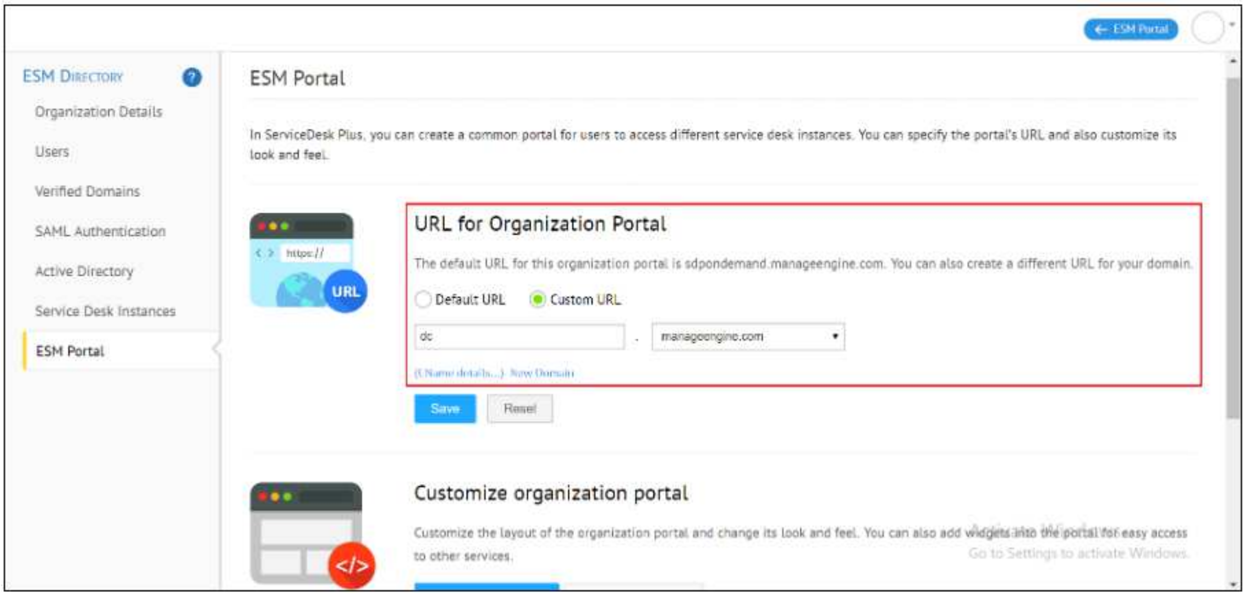
```
# #Tue Jul 08 05:41:29 PDT 2014
AUTHTOKEN=e3d7627cdaba53a6be6aa41e792db648
RESULT=TRUE
```

You have successfully created an authentication key. This can be used while configuring the integration settings.

Configure Integration Settings

To configure the ServiceDesk Plus On-Demand settings, follow the steps mentioned below:

1. From your Desktop Central web console, navigate to **Admin** tab -> Integration Settings -> ServiceDesk Plus Settings -> Select **ServiceDesk Plus On-demand.**
2. Enter the server name. You have the following options:
    a. Choose either "https://sdpondemand.manageengine.com", "https://sdpondemand.manageengine.en" or "https://sdpondemand.manageengine.in", according to the domain your SDP server is hosted in. To find out the exact URL, go to ServiceDesk Plus console and navigate to ESM Directory >> ESM portal >> URL for Organization Portal, as shown below:



ESM Portal

In ServiceDesk Plus, you can create a common portal for users to access different service desk instances. You can specify the portal's URL and also customize its look and feel.

URL for Organization Portal

The default URL for this organization portal is sdpondemand.manageengine.com. You can also create a different URL for your domain.

○ Default URL ● Custom URL

dc . manageengine.com ▾

(CName details...) New Domain

Save Reset

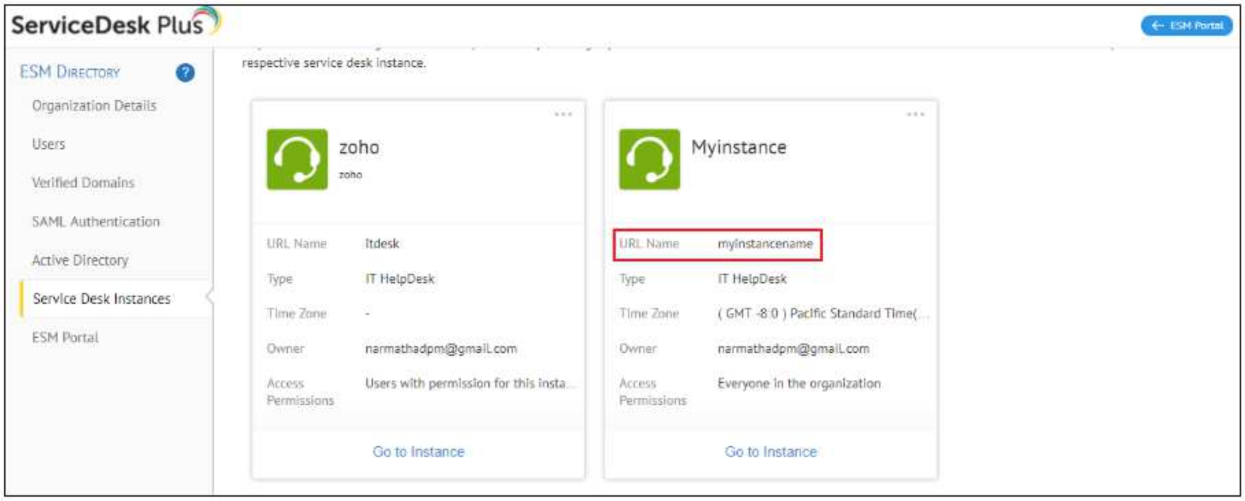
Customize organization portal

Customize the layout of the organization portal and change its look and feel. You can also add widgets into the portal for easy access to other services.

Go to Settings to activate Windows.

    b. Choose "Portal" if you've set up a customized domain for accessing ServiceDesk Plus cloud and enter the exact URL.

Note: All the helpdesk tickets and assets are posted to this URL. To post the DC - SDP integration tickets to a specific instance, provide the complete portal URL along with the instance name e.g.: https://dc.manageengine.com/app/myinstancename. If an instance is not specified in the URL, the **tickets will be raised to the default instance**. You can create and check instance names in ServiceDesk Plus console by navigationg to ESM Directory >> Service Desk Instances, as shown below:



respective service desk instance.

zoho
zoho

URL Name: Itdesk
Type: IT HelpDesk
Time Zone: -
Owner: narmathadpm@gmail.com
Access Permissions: Users with permission for this insta...

Myinstance

URL Name: myinstancename
Type: IT HelpDesk
Time Zone: (GMT -8:0) Pacific Standard Time(...
Owner: narmathadpm@gmail.com
Access Permissions: Everyone in the organization

3. Provide the generated API key. To know more, refer generating API key document.
4. Under **Features to be Integrated**, you can select the required features "**IT Asset Data**" and "**Log Help Desk Requests as Tickets**".
5. If you have integrated IT asset data, you can define the action to be performed on ServiceDesk Plus, when computers are removed from SoM and you can enable the option for assigning workstation owners automatically.
6. Click **Save** to save the changes.

You can see that Desktop Central has been successfully integrated with ServiceDesk Plus On-Demand.

IT Asset Data

Asset data will be posted to the Desktop Central server during the following scenarios:

- System Start Up
- User Logon
- After manual or scheduled scan
- When a new Software Application is installed/Uninstalled
- During the 90 minutes refresh cycle

The asset data, which is posted in Desktop Central will be updated to the ServiceDesk Plus On-Demand.

Log Help Desk Requests as Tickets

Users will be able to raise help desk tickets from the Desktop Central agent tray icon. These help desk tickets will be updated in the ServiceDesk Plus On-Demand server. **Proxy** and **Help Desk Settings**, under **Admin** tab, need to be configured for this feature to work. The benefits of logging help desk tickets as requests in ServiceDesk Plus On-Demand are:

- Submit requests without logging in
- Send requests using predefined templates and can even attach screenshots automatically
- Use customizable subject lines to configure the HelpDesk application and enable automatic assignment of tickets
- Configure settings in Desktop Central to log the following asset-related alerts as tickets in ServiceDesk Plus. These include alerts related to:
- Recently added hardware
- Commercial software applications that have recently been installed or uninstalled
- Prohibited software applications that have recently been installed
- Software compliance issues related to expired licenses or under licensed software applications

Features to be integrated

The following features can be integrated:

- Asset Management
- Configuration
- Remote Control
- Help Desk Ticketing

Asset Management

Under Asset Management, the following can be integrated:

- Asset data of computers : Define the action to be performed in ServiceDesk Plus when a computer is removed from SoM. You can either mark the asset state as disposed or remove the asset. Additionally, you can automatically assign owners for workstation.
- Asset data of mobile devices
- Send requests for approval to use prohibited software
- Log inventory alerts as ServiceDesk Plus requests

Configuration

Under Configuration, the following can be integrated:

- Deploy software from ServiceDesk Plus tickets
- Publish user-defined configuration templates

Remote Control

Whenever a remote connection is established using Desktop Central to resolve a ServiceDesk Plus ticket, update the worklog details to ServiceDesk Plus.

Help desk ticketing

You can enable the option to log help desk requests from agent tray icon as ServiceDesk Plus tickets.

Integrating with AssetExplorer

AssetExplorer is a web based software that is widely used for asset management. If you are currently using AssetExplorer to manage your assets, then integrating with Desktop Central will provide you the following benefits:

- Gain more accuracy with the asset information
- Immediate information when there is a change in status of the asset
- Fetch asset data of desktops and mobile Devices
- Fetch accurate details of all the hardware and software/app details

Integrating Desktop Central with AssetExplorer, optimizes the results of AssetExplorer. Since Desktop Central is an agent based solution, the data fetched from Desktop Central is more accurate and timely than AssetExplorer. Desktop Central will periodically update the asset information to the AssetExplorer. Desktop Central will post the inventory details immediately to AssetExplorer in the following scenarios :

- During every system startup
- User Logon
- After ever successful scan (manual & scheduled)
- Whenever a new software application is installed/uninstalled
- During the 90 minutes refresh interval

Steps to Integrate AssetExplorer

You will have to perform the steps mentioned below on the Desktop Central web console to integrate it with AssetExplorer:

1. Click **Admin** tab on the Desktop Central web console
2. Under **Integration** and Choose **ServiceDesk Plus Settings**
3. Under products to be integrated choose **AssetExplorer**
4. Specify the Server Name/ IP Address/DNS Name
5. Specify the port number
6. Select the Communication type as HTTP or HTTPS
7. Click to enable the features that you wanted to be integrated such as mobile devices and computers
8. Click **Save** to save the changes.

You have successfully integrated Desktop Central with AssetExplorer.

Desktop Central Reports

Reports are the best tool any IT administrator would like to lay their hands upon. These reports not only give quick and easy access to the details, but also help them keep a variety of risks at bay. Desktop Central comes with an integrated reporting bundle that showcases a comprehensive and exhaustive list of reports. Right from the information relating to user logon details to the inventory associated with the network, Desktop Central helps IT administrators derive a whole lot of information even from their enterprise's Active Directory in just a few clicks. Desktop Management can be simplified by using the scheduling options of the software. These reports extract the information and display them in a well formatted manner. Options to convert the extracted report to other file formats like PDF and CSV is just a click away.

The following reports are offered by Desktop Central:

1. Scheduled Reports
2. Custom Reports
3. Query Reports
4. Active Directory Reports
5. User Logon Reports
6. Power Management Reports
7. Configuration Reports
8. USB Reports

Report Settings

By configuring report settings, one can enable user logon reports and specify the time period for maintenance of user logon history. Additionally, power management reports can be enabled as well.

Export Settings

Exporting or scheduling reports in formats such as PDF, CSV, XLSX may include personal information such as user name, computer name or IP address. You can configure your export and scheduled report settings by masking, removing or retaining Personally Identifiable Information (PII).

Scheduled Reports

The Schedule Reports feature enables you to receive query reports, custom reports and predefined reports in specific formats such as CSV, XLS and PDF. By using this feature, you do not have to view the individual reports, instead you can schedule them to be sent to you by E-mail at the specified times. These reports are automatically generated and compiled. In addition to this, you can configure the settings so that the reports can be sent to more than one person.

You receive scheduled reports in the following formats :

1. Attachment : You can receive the scheduled reports as an attachment to your E-mail ID.
2. Zipped file : In case you have selected a lot of reports to be received as a scheduled report, you can choose to receive these as a zipped file to you mail.
3. URL : If the size of the report exceeds the permissible size by your mail server, you can choose this option to publish the reports that you have selected on Desktop Central server and the path will be sent to you mail ID.

A code, mapped to the file path of the report in the server, is sent along with the download URL for the report so that the end user can download just the report with the help of the URL.

Creating a Scheduled Report

To create a scheduled report, follow the steps given below :

a. Click on **Reports** tab and click on **Add Schedule Report**.
b. After providing a scheduler name and description, choose the required reports from the **reports category**.
c. Specify the **report format** and the **delivery format**.
d. Provide **e-mail ID of the recipient(s)**.
e. Configure the **scheduler** to set the frequency at which the reports need to be generated and when it needs to be generated.
f. Click on **Save** and you have now created a schedule report which will be sent to you according to the delivery schedule that you have set.

If you want the reports to be **generated immediately**, click on **Execute Now** under actions column against the report you have created. You will now receive the report immediately, as well as at the scheduled time.

Custom Reports

While Desktop Central provides various canned reports on different modules like Patch Management, Asset Management, and so on, it is also possible to create customized reports to meet your specific requirement. Follow the links to learn more

- Wizard Based Custom Report
- Custom Query Report

Follow the steps for creation of a custom report.

Creating Custom Reports

In addition to the out-of-the-box reports, Desktop Central allows you to create custom reports by specifying the criteria and selecting the required parameters. Follow the steps below to create a custom report using Desktop Central:

1. Select the **Reports** tab from the Desktop Central Client.
2. Click on **Custom Reports**. This opens the Custom Report page.
3. Specify the name for the report.
4. Select the Module. This is currently available only for the Asset Management module and will be extended for other modules in our subsequent updates.
5. Select the Sub Module as Computer, Hardware or Software.
6. Specify the criteria for generating the report. You can specify multiple criteria by clicking the "+" icon
7. Select the Columns to view in the report. You can change the position of the columns by using the up and down arrow icons.
8. Click on **Run & Save** button to save the report permanently. (or) Click **Run Report** if just a temporary report is needed.

Note: If you choose the **Run Report** option, you can edit the report and later on save the same. Likewise if you intend to make any changes to a saved report, you can make use of the Edit option in the **Custom Report** Page.

9. You have an option to save this report in PDF and CSV formats.

Custom Query Report

Desktop Central provides the following types of reports:

- Canned reports on various modules like Patch Management, Asset Management, Active Directory, and so on.
- Wizard-based Custom Reports to retrieve any specific information

In addition to the above report types, it also provides an ability to retrieve the required information from the database using the Query Report. This might be useful in cases where you are not able to get the required information from the Canned or the Custom Reports.

The Query Report can be created using the **Query Report** button available under **Reports tab.**. You may have to provide the SQL Query and create the report. The report can be saved for future reference and / or exported to CSV format for further processing.

From where can I get the Query?

Contact desktopcentral-support@manageengine.com with the details of your requirement. Alternatively, you can also submit your request online.

Our support team will process your requirement and send you the query.

Built-in Date Functions

Date is stored in the Long format in the database. You will not be able to interpret the date on seeing this long format. In order to convert this to readable date format, two built-n functions are included:

- LONG_TO_DATE() - for displaying the date in the results
- DATE_TO_LONG() - for using the date within the query

LONG_TO_DATE()

This function can be used to convert the date from the long value to the date format. Consider the following example:

You wish to retrieve software details along with the date and time at which the software was detected. The query you would normally use is:

```
Select SOFTWARE_NAME, DETECTED_TIME from invsoftware


SOFTWARE_NAME         DETECTED_TIME

Adobe Reader          1234558984892

Skype                 8945934747893
```

In the above result, you will see the Detected Time in long format, which is not readable. Now, modifying the query as below will give you the desired output

```
Select SOFTWARE_NAME, LONG_TO_DATE(DETECTED_TIME) from invsoftware


SOFTWARE_NAME         DETECTED_TIME_DATE_FORMAT

Adobe Reader           09/12/2009 15:35

Skype                  07/13/2009  13.25
```

DATE_TO_LONG()

This function can be used to convert the Date format to Long value. Consider the example where you wish to retrieve the details of the software detected between two specific dates. You should use the query as below:

```
select * from invsoftware where DETECTED_TIME between
DATE_TO_LONG(08/01/2009 00:00:00) and

DATE_TO_LONG(08/31/2009 00:00:00)
```

The date should be specified in the following format: mm/dd/yyyy hh:mm:ss

Date Templates

For retrieving the data between some predefined dates, you can make use of the date templates. The following date templates are supported:

- Today - <from_today> - <to_today>
- Yesterday - <from_yesterday> - <to_yesterday>
- This Week - <from_thisweek> - <to_thisweek>
- Last Week - <from_lastweek> - <to_lastweek>
- This Month - <from_thismonth> - <to_thismonth>
- Last Month - <from_lastmonth> - <to_lastmonth>
- This Quarter - <from_thisquarter> - <to_thisquarter>
- Last Quarter - <from_lastquarter> - <to_lastquarter>

Active Directory Reports

Desktop Central gives you an insight into the Active Directory by providing reports on various Active Directory components. The reports can be accessed by selecting the Reports tab from the client window. The following reports about the Active Directory are shown:

- Active Directory User Reports
- Active Directory Computer Reports
- Active Directory Group Reports
- Active Directory Organization Unit Reports
- Active Directory Domain Reports
- Active Directory GPO Reports

More granular reports are provided for each of the above components.

Active Directory Report Features

- Ability to generate reports for custom inputs for granularity.
- Customizable columns in all the reports.
- Columnar sorting of reports
- Export reports in PDF and CSV formats.
- Ability to synchronize report data with Active Directory at regular intervals.

Active Directory User Report

To access the User Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Select the User Logon Reports under Active Directory Reports to view the reports.

Follow the links to learn more about the various User Reports provided by Desktop Central

- Active Directory General User Reports
- User Account Status Reports
- Password Based User Reports
- Privileged User Reports
- Logon Based User Reports

Active Directory General User Reports

All User Accounts

Provides the details of all the users of the domain that the system/user running the Desktop Central belongs to.

To view the report, click the **All User Accounts** link available under the General Reports category. Clicking a user from the report displays the complete user information of that user.

Recently Created User Accounts

Provides the details of the user accounts that are created recently. This is determined based on the value contained in the *createTimeStamp* attribute of the Active Directory.

To view the report, click the **Recently Created User Accounts** link available under the General Reports category.

By default, the users created for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a user from the report displays the complete information of that user.

Recently Modified User Accounts

Provides the details of the user accounts modified recently. This is determined based on the value contained in the *modifyTimeStamp* attribute of the Active Directory.

To view the report, click the **Recently Modified User Accounts** link available under the General

Reports category.

By default, the user accounts modified for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a user from the report displays the complete information of that user.

User Accounts without Logon Scripts

Provides the details of the users who do not have any scripts executed during their logon to the domain. This is determined based on the value contained in the *scriptPath* attribute of the Active Directory.

To view the report, click the **User Accounts without Logon Scripts** link available under the General Reports category. Clicking a user from the report displays the complete information of that user.

User Accounts in Multiple Groups

Provides the details of the user accounts that are in more than one groups. This also includes the nested groups i.e., groups that contain other groups as its members in the domain.

To view the report, click the **User Accounts in Multiple Groups** link available under the General Reports category.

User Accounts that Never Expires

Provides the list of user accounts that never expires. This is determined based on the value contained in the *userAccountControl* of the Active Directory.

To view the report, click the **User Accounts that Never Expires** link available under the General Reports category.

User Account Status Reports

Active User Accounts

Provides the list of users who have logged on to the domain in the past 30/60/90/180 days. This is determined based on the value contained in the *lastLogon* attribute of the Active Directory.

To view the report, click the **Active User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Inactive User Accounts

Provides the list of users who have not logged on to the domain in the past 30/60/90/180 days. This is determined based on the value contained in the *lastLogon* attribute of the Active Directory.

To view the report, click the **Inactive User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Disabled User Accounts

Provides the list of user accounts that are disabled by the administrator. This is determined based on the value contained in the *userAccountControl*attribute of the Active Directory.

To view the report, click the **Disabled User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Locked User Accounts

Provides the details of the user accounts that have been locked out. The user account will get locked on frequent bad login attempts. The Account Lock Out Policy specifies the allowed number of bad login attempts after which the account will be locked. The account will be automatically unlocked after sometime. The locked user accounts are determined based on the value contained in the *lockoutTime* attribute of the Active Directory.

To view the report, click the **Locked User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Expired User Accounts

Provides the details of the user accounts that have expired. This is determined based on the value contained in the *accountExpires* attribute of the Active Directory.

To view the report, click the **Expired User Accounts** link available under the Account Status Reports category. Clicking a user from the report displays the complete information of that user.

Password Based User Reports

Soon-to-Expire User Passwords

Provides the details of the users whose password will expire within the specified number of days. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Soon-to-Expire User Passwords** link available under the Password Based Reports category.

By default, the users whose passwords will expire in another seven days is shown. You can select a different period to view the report. Clicking a user from the report displays the complete information of that user.

Password Expired User Accounts

Provides the details of the users whose password has expired. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Password Expired User Accounts** link available under the Password Based Reports category. Clicking a user from the report displays the complete information of that user.

Password Never Expiring User Accounts

Provides the list of users whose password never expires. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **Password Never Expiring User Accounts** link available under the Password Based Reports category. Clicking a user from the report displays the complete information of that user.

User Accounts Password that cannot be Changed

Provides the list of users who cannot change their password. This is determined based on the value contained in the *userAccountControl* attribute of the Active Directory.

To view the report, click the **User Accounts Password that cannot be Changed** link available under the Password Based Reports category. Clicking a user from the report displays the complete information of that user.

Privileged User Accounts

Domain Admin User Accounts

Provides the list of users who have domain administrative privileges.

To view the report, click the **Domain Admin User Accounts** link available under the Accounts with Privileged User Accounts category.

User Accounts with Dial-in Permissions

Provides the list of users who have dial-in permissions to access the domain. This is determined based on the value contained in the *msNPAllowDialinattribute* of the Active Directory.

To view the report, click the **User Accounts with Dial-in Permissions** link available under the Privileged User Accounts category.

Logon Based User Reports

- Unused User Accounts
- Recently Logged On User Accounts
- Last Logon Failed User Accounts

Unused User Accounts

Provides the list of users who have not logged on to the domain since creation of the account. This is determined based on the value contained in the *lastLogon* of the Active Directory.

To view the report, click the **Unused User Accounts** link available under the Logon Based Reports category. Clicking a user from the report displays the complete information of that user.

Recently Logged On User Accounts

Provides the details of the users who have logged on in the past n days. The recently logged on users are determined based on their last logon time.

To view the report, click the **Recently Logged On User Accounts** link available under the Logon Based Reports category.

By default, the users logged on for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a user from the report displays the complete information of that user.

Last Logon Failed User Accounts

Provides the list of users whose last logon has failed. This is determined based on the value contained in the *badPasswordTime* and *badPwdCount* attributes of the Active Directory.

Active Directory Computer Report

To access the Computer Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **Computer Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various Computer Reports provided by Desktop Central

- General Computer Reports
- Server Based Reports
- Computer OS Based Reports

General Computer Reports

All Computers

Provides the list of all the computer accounts available in the domain.

To view the report, click the **All Computers** link available under the General Reports category. Clicking a computer account from the report displays the complete information of that account.

Windows Workstation

Provides the details of the workstations in the domain. All the computers except Servers and Domain Controllers are termed as workstations.

To view the report, click the **Windows Workstation** link available under the General Reports category. Clicking a computer account from the report displays the complete information of that account.

Recently Added Computers

Provides the details of the computer objects that are created recently. This is determined based on the value contained in the *createTimeStamp*attribute.

To view the report, click the **Workstations** link available under the General Reports category.

By default, the report displays the computer accounts that are created in the last one week. You have an option to choose a different period or to generate a report for a custom period.

Clicking a computer account from the report displays the complete information of that account.

Recently Logged On Computers

Provides the list of computer accounts through which an user has logged on to the domain. This is determined based on the value contained in the*lastLogon* attribute.

To view the report, click the **Recently Logged On Computers** link available under the General Reports category.

By default, the report displays the computer accounts through which an user has logged on to the domain in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a computer account from the report displays the complete information of that account.

Recently Modified Computer Accounts

Provides the details of the computer objects that are modified recently. This is determined based on the value contained in the *ModifyTimeStamp*attribute.

To view the report, click the **Recently Modified Computer Accounts** link available under the General Reports category.

By default, the report displays the computer accounts that are modified in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a computer account from the report displays the complete information of that account.

Disabled Computer Accounts

Provides the list of computer accounts that are disabled in the domain. This is determined based on the value contained in the *userAccountControl* of the Active Directory.

To view the report, click the **Disabled Computer Accounts** available under General Reports category. Clicking a computer account from the report displays the complete information of that account.

Computer Accounts by OU

Provides the list of computer accounts filtered by the OU it belongs to.

To view the report, click the **Computers Accounts by OU** available under General Reports category.

By default, the computer accounts of all the OUs in the domain are listed. Browse to select a specific OU and click **Generate** to view the computer accounts of that OU. Clicking a computer account from the report displays the complete information of that account.

Server Based Reports

Windows Servers

Provides the list of Windows Servers in the domain. This is determined based on the value contained in the *operatingSystem* attribute of the Active Directory.

To view the report, click the **Windows Servers** link available under the Server Based Reports category. Clicking a computer account from the report displays the complete information of that account.

Member Servers

Provides the details of the member servers in the domain.

To view the report, click the **Member Servers** link available under the Server Based Reports category. Clicking a computer account from the report displays the complete information of that account.

Domain Controllers

Provides the details of the domain controllers in the domain.

To view the report, click the **Domain Controllers** link available under the Server Based Reports category. Clicking a computer account from the report displays the complete information of that account.

Computers by OS Service Pack

Computers by OS Service Pack

Provides the details of the computers based on the operating system and service pack versions.

To view the report, click the **Computers by OS Service Pack** available under OS Based Reports category. Select the Operating System and the Service Packs to filter the view. Clicking a computer account from the report displays the complete information of that account.

Active Directory Group Report

To access the Group Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **Group Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various Group Reports provided by Desktop Central

- General Group Reports
- Group Type Reports
- Group Member Based Reports

Active Directory General Group Reports

- All Groups
- Recently Created Groups
- Recently Modified Groups
- Groups by OU

All Groups

Provides the details of all the groups of the domain.

To view the report, click the **All Groups** link available under the General Reports category. Clicking a group from the report displays the complete information of that group.

Recently Created Groups

Provides the details of all the groups that are recently created. This is determined based on the value contained in the *createTimeStamp* of the Active Directory.

To view the report, click the **Recently Created Groups** link available under the General Reports category.

By default, the groups created for the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a group from the report displays the complete information of that group.

Recently Modified Groups

Provides the details of all the groups that are recently modified. This is determined based on the value contained in the *modifyTimeStamp* of the Active Directory.

To view the report, click the **Recently Modified Groups** link available under the General Reports category.

By default, the groups modified in the last one week is shown. You have an option to choose a different period or to generate a report for a custom period. Clicking a group from the report displays the complete information of that group.

Groups by OU

Provides the list of groups filtered by the OU it belongs to.

To view the report, click the **Groups by OU** link available under the General Reports category.

By default, the groups of all the OUs in the domain are listed. Browse to select a specific OU and click **Generate** to view the groups of that OU. Clicking a group from the report displays the complete information of that group.

Active Directory Group Type Reports

- Security Groups
- Distribution Groups

Security Groups

Provides the details of the security groups available in the domain. This is determined based on the value contained in the *groupType* attribute of the Active Directory.

To view the report, click the **Security Groups** link available under the Group Type Based Reports category. Clicking a group from the report displays the complete information of that group.

Distribution Groups

Provides the details of the distribution groups available in the domain. This is determined based on the value contained in the *groupType* attribute of the Active Directory.

To view the report, click the **Distribution Groups** link available under the Group Type Based Reports category. Clicking a group from the report displays the complete information of that group.

Member Based Reports

Groups with Member Details

Provides the details of the groups with its member count, such as no. of users, computers, groups, etc.

To view the report, click the **Groups with Member Details** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Groups with Maximum Members

Provides the details of the large groups in the domain based on its members count.

To view the report, click the **Groups with Maximum Members** link available under the Member Based Reports category. You can customize the report by selecting the member count. Clicking a group from the report displays the complete information of that group.

Groups without Members

Provides the list of groups that do not have any members.

To view the report, click the **Groups without Members** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

User-only Groups

Provides the list of groups that have only users as its members.

To view the report, click the **User-only Groups link** available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Computer-only Groups

Provides the list of groups that have only computers as its members.

To view the report, click the **Computer-only Groups** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Nested groups

Provides the list of nested groups (groups within groups) in the domain.

To view the report, click the **Nested groups** link available under the Member Based Reports category. Clicking a group from the report displays the complete information of that group.

Active Directory Organizational Unit Report

To access the Organizational Unit Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **OU Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various OU Reports provided by Desktop Central

- Active Directory General OU Reports
- OU Child Based Reports

Active Directory General OU Reports

- All OUs
- Recently Created OUs
- Recently Modified OUs

All OUs

Provides the list of all the OUs of the domain.

To view the report, click the **All OUs** link available under the General Reports category. Clicking an OU from the report displays the complete information about that OU.

Recently Created OUs

Provides the list of OUs that are recently created. This is determined based on the value contained in the *createTimeStamp* attribute.

To view the report, click the **Recently Created OUs** link available under the General Reports category.

By default, the report displays the OUs created in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking an OU from the report displays the complete information about that OU.

Recently Modified OUs

Provides the list of OUs that are recently modified. This is determined based on the value contained in the *ModifyTimeStamp* attribute.

To view the report, click the **Recently Modified OUs** link available under the General Reports category.

By default, the report displays the OUs modified in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking an OU from the report displays the complete information about that OU.

OU Child Based Reports

- OUs with Child Details
- OUs without Children
- User-only OUs
- Computer-only OUs
- Nested OUs

OUs with Child Details

Provides the list of OUs with its child details, like no. of users, computers, groups, and OUs.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

OUs without Children

Provides the list of OUs that do not have any children.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

User-only OUs

Provides the list of OUs that have only users as their children.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

Computer-only OUs

Provides the list of OUs that have only computers as their children.

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

Nested OUs

Provides the list of OUs that nested (OUs within OUs).

To view the report, click the **OUs with Child Details** link available under the OU Children Based Reports category. Clicking an OU from the report displays the complete information about that OU.

Active Directory Domain Reports

To access the Domain Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **Domain Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various Domain Reports provided by Desktop Central

- Active Directory General Domain Reports
- Active Directory Container Reports

General Domain Reports

- Active Directory Sites
- Active Directory Domains
- Active Directory Printers
- Group Policy Creator Owners

Active Directory Sites

Active Directory Site Report provides the list of Sites with their attributes, such as Site name, subnet, netmask, and domain controller. Clicking a site from the report provides more details, such as the number of computers in each subnet, creation time, modified time, and so on.

To view the report, Click the **Active Directory Sites** link available under the General Reports category.

Active Directory Domains

Active Directory Domain Report provides the complete information of domain with the fully qualified Domain name, creation time, modified time, location, and its members.

To view the report, Click the **Active Directory Domains** link available under the General Reports category.

Active Directory Printers

Active Directory Printer Report provides the list of printers with their attributes such as name, host server name, model of printer, physical location and share name. Clicking the printer from the report gives details, such as Domain name, Active Directory URL, Model, Physical location, Share name, Modified time, Creation time, Printer Hosted Server name, Driver name, and Port name.

To view the report, Click the **Active Directory Printers** link available under the General Reports category.

Group Policy Creator Owners

Provides the members of Group Policy Creator Owners (GPCO) group. The members of this group can modify group policy for the domain.

To view the report, click the **Group Policy Creator Owners** link available under the General Reports category.

Container Based Reports

Users In "Users" Container

Provides the list of users in the "users" container of the domain.

To view the report, click the **Users In "Users" Container** link available under the Container Based Reports category.

Groups In "Users" Container

Provides the list of groups in the "users" container of the domain.

To view the report, click the **Groups In "Users" Container** link available under the Container Based Reports category.

Computers In "Computer" Container

Provides the list of computers in the "computer" container of the domain.

To view the report, click the **Computers In "Computer" Container** link available under the Container Based Reports category.

Groups In "Builtin" Container

Provides the list of groups in the "Builtin" container of the domain.

To view the report, click the **Groups In "Builtin" Container** link available under the Container Based Reports category.

Active Directory GPO Reports

To access the GPO Reports, follow the steps below:

1. Click the **Reports** tab to invoke the Reports page.
2. Click the **GPO Reports** from the left pane.
3. Select the required link to view the reports.

Follow the links to learn more about the various GPO Reports provided by Desktop Central

- General GPO Reports
- GPO Link Based Reports
- Inheritance Based Reports
- GPO Status Based Reports
- Special GPO Reports

General GPO Reports

All GPOs

Provides the list of GPOs that are created in the domain.

To view the report, click the **All GPOs** link available under the General Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Recently Created GPOs

Provides the list of GPOs that are recently created in the domain.

To view the report, click the **Recently Created GPOs** link available under the General Reports category. This is determined based on the value contained in the *createTimeStamp* attribute.

By default, the report displays the GPOs created in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a GPO from the report displays the complete information about that GPO.

Recently Modified GPOs

Provides the list of GPOs that are recently modified in the domain. This is determined based on the value contained in the *ModifyTimeStamp*attribute.

To view the report, click the **Recently Modified GPOs** link available under the General Reports category.

By default, the report displays the GPOs modified in the last one week. You have an option to choose a different period or to generate a report for a custom period. Clicking a GPO from the report displays the complete information about that GPO.

GPOs by OUs

Provides the list of OUs and their linked GPOs.

To view the report, click the **GPOs by OUs** link available under the General Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPO Link Based Reports

- GPOs Linked To OUs
- GPOs Linked To Domains
- GPOs Linked To Sites

GPOs Linked To OUs

Provides the list of GPOs that are linked to OUs in the domain. This is determined based on the value contained in the *gPLink* attribute of the Active Directory.

To view the report, click the **GPOs Linked To OUs** link available under the GPO Link Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs Linked To Domains

Provides the list of GPOs that are linked to domains. This is determined based on the value contained in the *gPLink* attribute of the Active Directory.

To view the report, click the **GPOs Linked To Domains** link available under the GPO Link Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs Linked To Sites

Provides the list of GPOs that are linked to sites. This is determined based on the value contained in the *gPLink* attribute of the Active Directory.

To view the report, click the **GPOs Linked To Sites** link available under the GPO Link Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Inheritance Based Reports

- Block Inheritance enabled OUs
- Block Inheritance enabled Domains
- Enforced GPOs

Block Inheritance enabled OUs

Provides the list of OUs that are prevented from inheriting GPOs from any of its parent container. This is determined based on the value contained in the *gPOptions* attribute of the Active Directory.

To view the report, click the **Block Inheritance enabled OUs** link available under the Inheritance Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Block Inheritance enabled Domains

Provides the list of domains that are prevented from inheriting GPOs from any of its parent container. This is determined based on the value contained in the *gPOptions* attribute of the Active Directory.

To view the report, click the **Block Inheritance enabled Domains** link available under the Inheritance Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Enforced GPOs

Provides the list of GPOs that have the enforced flag set. Enforced GPOs when applied to OUs are also applied to their children irrespective of whether Block Inheritance is set or not.

To view the report, click the **Enforced GPOs** link available under the Inheritance Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPO Status Based Reports

- User Settings Enabled GPOs
- Computer Settings Enabled GPOs
- User and Computer Settings Enabled GPOs
- Disabled GPOs
- Unused GPOs

User Settings Enabled GPOs

Provides the list of GPOs that have Computer Settings disabled. These GPOs can be used to make the user settings.

To view the report, click the **User Settings Enabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Computer Settings Enabled GPOs

Provides the list of GPOs that have User Settings disabled. These GPOs can be used to make the computer settings.

To view the report, click the **Computer Settings Enabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

User and Computer Settings Enabled GPOs

Provides the list of GPOs that can be used to perform both user and computer settings.

To view the report, click the **User and Computer Settings Enabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Disabled GPOs

Provides the list of GPOs that have both User and Computer Settings disabled.

To view the report, click the **Disabled GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Unused GPOs

Provides the list of GPOs that are not used since creation.

To view the report, click the **Unused GPOs** link available under the GPO Status Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Special GPO Reports

GPOs with Most Modified User Settings

Provides the list of GPOs that have user versions greater than 5. You have an option to select a different version number.

To view the report, click the **GPOs with Most Modified User Settings** link available under the GPO Version Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs with Most Modified Computer Settings

Provides the list of GPOs that have computer versions greater than 5. You have an option to select a different version number.

To view the report, click the **GPOs with Most Modified Computer Settings** link available under the GPO Version Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

GPOs with Most Modified User & Computer Settings

Provides the list of GPOs that have user or computer versions greater than 5. You have an option to select a different version number.

To view the report, click the **GPOs with Most Modified User & Computer Settings** link available under the GPO Version Based Reports category. Clicking a GPO from the report displays the complete information about that GPO.

Viewing User Logon Reports

To view the **User Logon Reports**, select the **Reports** tab and click the **User Logon Reports** link from the left pane. The User Logon Reports are classified under the following headings; click the links to learn more:

- General Reports
- Usage Reports
- History Reports

General Reports

Currently Logged on Users

Provides the list of users who are currently logged on to the domain.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Currently Logged on Users** link available under the General Reports category.

Currently Logged on Computers

Provides the list of computers from where users have logged on to the domain.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Currently Logged on Computers** link available under the General Reports category.

Usage Reports

Table of contents

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane.

Users Frequently Logged On to the Domain

Provides the list of users who logs on to the domain frequently. It is arrived when the average user logon to the domain is more than 1.5 times the normal.

To view the report, select the **Reports** tab, click the User Logon Tracking Reports from the left pane, and click the **Users Frequently Logged On to the Domain** link available under the Usage Reports category.

Users Rarely Logged On the Domain

Provides the list of users who logs on to the domain rarely. It is arrived when the average user logon to the domain is less than 0.6 times the normal.

To view the report, select the **Reports** tab, click the User Logon Tracking Reports from the left pane, and click the Users **Rarely Logged On the Domain** link available under the Usage Reports category.

Inactive Users

Provides the list of users who have not logged on to the domain in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Tracking Reports from the left pane, and click the **Inactive Users** link available under the Usage Reports category.

Computers with Frequent User Logon

Provides the list of computers with more user logon to the domain. It is arrived when the average user logon from the computer is more than 1.5 than normal.

To view the report, select the **Reports** tab, click the User Logon Tracking Reports from the left pane, and click the **Computers with Frequent User Logon** link available under the Usage Reports category.

Computers with Rare User Logon

Provides the list of computers with few user logon to the domain. It is arrived when the average user logon from the computer is less than 0.6 than normal.

To view the report, select the **Reports** tab, click the User Logon Tracking Reports from the left pane, and click the **Computers with Rare User Logon**link available under the Usage Reports category.

Computers with No User Logon

Provides the list of computers where no user have logged on.

To view the report, select the **Reports** tab, click the User Logon Tracking Reports from the left pane, and click the **Computers with No User Logon**link available under the Usage Reports category.

History Reports

Table of contents

User Logon History

Provides the list of history of users who have logged on to the domain in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **User Logon History** link available under the History Reports category.

User Logon History by Computers

Provides the list of computers and their corresponding user logon history in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **User Logon History by Computers** link available under the History Reports category.

Domain Controllers with Reported Users

Provides the list of users and their corresponding Domain Controllers (logon servers) in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **Domain Controllers with Reported Users**link available under the History Reports category.

User Logon History on Domain Controller

Provides the list of domain controllers and their corresponding user logon history in the specified number of days. This is configurable from the Report Settings.

To view the report, select the **Reports** tab, click the User Logon Reports from the left pane, and click the **User Logon History by Domain Controllers**link available under the History Reports category.

Setting Up User Logon Reports

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

To Maintain User Logon History:

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

Viewing System Uptime Report

- Configuring Data Storage Period
- Viewing Report for a Specified Period
- Viewing Detailed Uptime Report
- Exporting the Report

Provides the total uptime and downtime of the computers in the network for a given period. The report can be filtered to view computers in a specific domain and period. To view the report, select **Reports --> Power Management Reports --> System Uptime Report**

Configuring Data Storage Period

Desktop Central, by default, stored the uptime/downtime details of all the computers for a period of 30 days. This can be configured to suit your need. To specify the period,

1. Click **Edit Settings** link. This is open the Power Report Settings dialog.
2. Specify the number of days you wish to store the data and click **Apply**.

Viewing Report for a Specified Period

1. Select the **Domain** or select **All Domains** to view the uptime of all the computers.
2. Select a period from the list. To specify a custom period, click **Select Custom Date** and specify the start and end dates.
3. Specify the start and end time for which the report has to be displayed. If you wish to see the complete details, specify the start and end time as 00:00 and 23:59 respectively.
4. Selecting the "**Consider hibernate/standby as shutdown**" option will show the hibernate/standby periods as downtime.
5. Click **Apply Filter** to view the report based on the specified criteria.

Viewing Detailed Uptime Report

Desktop Central will display the summary view of the total uptime and downtime of the computers based on the selected criteria. Selecting the Detail Report option will display the start and shutdowm times of the computers for the given period. You can also click the computer name to view its detailed and summary reports.

Exporting the Report

The System Uptime Report can be exported to a PDF or a CSV format by clicking the respective options from the top-right. The current report that is being displayed will be exported to the selected format.

Viewing Configuration Reports

The Configuration reports helps the administrators to view the details of the configurations that are applied on users, computers, and based on the configuration type. To view the reports, follow the steps given below:

1. Click the **Reports** tab to invoke the **Reports** page.
2. Click the desired report from the Configuration Reports.

The Configuration Reports includes the following reports:

- Configuration by User
- Configuration by Computer
- Configurations by Type

Configuration by User

This report provides a list of users for whom configurations were applied using Desktop Central. It also provides details about the total number of configurations applied for a particular user and the last configuration and time at which it was applied. Clicking the user name will list the details of the configurations applied for that user.

You also have an option to filter your view based on the time at which the configuration was applied or by the configuration type.

Configuration by Computer

This report provides a list of computers for which configurations were applied using Desktop Central. It also provides details about the total number of configurations applied for that computer and the last configuration and time at which it was applied. Clicking the computer name will list the details of the configurations applied for that machine.

You also have an option to filter your view based on the time at which the configuration was applied or by the configuration type.

Configurations by Type

This report provides you the list of configurations that have been applied on users and computers based on the configuration type. It also provides you the total number of configurations that have been applied for a particular type and the last configuration, and time at which it was applied.

USB - Audit

USB devices have been a vital threat to data security. Almost every enterprise has a need to monitor the usage of USB devices within the network. In addition to securing the USB access, Desktop Central also helps you to track the usage of USB devices. Administrators can now audit the USB usage details and configure USB Alert using Desktop Central. This document will explain you about the steps involved in configuring the following:

- Viewing USB Usage Reports
- Configuring USB Audit Settings
- Configuring USB Alert Settings

Note: This feature is currently supported only for computers using windows operating system.

Viewing USB Usage Reports

Follow the steps mentioned below to view the usage of the USB devices in the managed computers:

1. Click **Reports** tab
2. From the left panel find **Reports Category**
3. Select **USB Reports**
4. Under **USB Audit Reports** Click **USB usage Report**

You will have the reports listed, from which you can choose to see the summary and detailed view.

USB Audit Settings

USB audit settings will be enabled by default. Users can disable if required. Follow the steps mentioned below to configure USB Audit settings;

1. Click **Admin** Tab
2. Under **Configuration Settings,** select **USB Settings** and choose **Audit settings**
3. **Enable** USB audit settings
4. Specify the number of days you wanted the USB usage history to be maintained.

5. Specify how often should the report be generated.
6. Click **Save Changes**

USB audit settings will be saved and the reports will be generated accordingly.

USB Alert Settings

Administrators can configure the USB alert settings. Every time a user tries to plug-in a restricted USB device, they will be notified with an alert message stating that the usage of USB device is restricted and will be asked to contact the system administrator. Follow the steps mentioned below to configure the USB alert settings:

1. Click **Admin** Tab
2. Under **Configuration Settings,** select **USB Settings** and choose **Audit settings**
3. **Enable** USB alert settings
4. Specify the title and the message that needs to be displayed to the end user while a restricted USB device is plugged in.
5. You can specify, if the message should be displayed only for the first time or every time a restricted USB device is plugged in.
6. Click **Save Changes** to store the settings.

You have successfully configured the USB alert settings.

Appendix

This section includes the following topics:

- Interpreting Error Messages
- Knowledge Base
- FAQs
- Security Policies
- Windows System Tools
- Data Backup and Restore
- Dynamic Variables
- Limitations
- Glossary

Interpreting Error Messages

1001: Storage Error Occurred

The configurations defined using Desktop Central are stored in the database. If we are unable to store the configuration details, this error message is shown. The reasons could be any of the following:

- Could not establish connection with the database.
- Violations in data definitions.

1002: Unknown error

This error is shown when any runtime error occurs, which is not defined in Desktop Central. Please contact desktop central support with the details of the error.

1003: DB Error

This error is shown when the database connection is lost.

1004: DB Error

This error message is shown when you try to access the data, which has been deleted from the database.

1010: Invalid User

While defining the scope of management, if the user name provided is invalid, this error message is shown.

Top

1011: User is already Inactive

When you try to add an user which is already present in the Inactive User list, this error message is shown.

1101: Invalid Container name

While defining targets for the configuration or while defining the scope of management, if an invalid / nonexistent container name is given this error occurs. The error message is shown, when you click Add more targets button or during deployment.

1103: Group Policy Object (GPO) creation failed

For every configuration a Group Policy Object (GPOs) will be created. When the GPO could not be created due to some access restrictions, etc., this error is shown.

1104: Group Policy Object (GPO) deletion failed

When an already defined configuration is deleted, the corresponding GPO is also deleted. This error is shown, when the GPO could not be deleted.

1105: Group Policy Object (GPO) linking failed

When a configuration defined, a GPO will be created and linked with the targets specified. This error is shown, when the linking fails.

1106: Group Policy Object (GPO) unlinking failed

When an already defined configuration is suspended, respective GPO will be unlinked from the targets. This error is shown, when the unlinking fails.

Top

1107: WMI query failed

Desktop Central fetches the computer details through WMI. The WMI query may fail in the following cases:

1. Authentication failure
2. When the machine is shutdown
3. When the RPC server is not running.

1108: Active Directory error occurred

Pertains to the Active Directory related error. Please create a support file by clicking the **Support File** link available under the **Support** tab and send it to support@desktopcentral.com. Our support team will be able to assist you on this.

1109: Unable to Extract Information from the given Msi Package

The possible reason for this error could be that the MSI package is corrupted.

1110: Access is Denied

The Active Directory credentials are taken while you define the scope of management. This credential is stored in Desktop Central, which will be used for deploying configurations. When this credential becomes invalid or if it does not have necessary privileges, this error is shown.

One possible reason is that the credential is modified outside the Desktop Central.

1111: File Copy Failed

This error message is shown, when the user do not have necessary privileges to copy a file. Check whether the credentials supplied while defining the Scope of Management has necessary privileges.

Top

1112: Folder Copy Failed

This error message is shown, when the user do not have necessary privileges to copy a folder. Check whether the credentials supplied while defining the Scope of Management has necessary privileges.

1113: The Given User Account is not a valid Domain Administrator

When the user account provided in the Scope of Management does not belong to a Domain Administrator group.

1114: The Given Password is wrong

The password provided in the Scope of Management is not valid.

1115: Active Directory/Domain Controller not Found

This error message is shown when no Active Directory/Domain Controller is found in your network. Desktop Central requires either of the two to perform the configurations.

1222: The network is not present or not started

This error message is shown when Desktop Central is unable to discover any domain. To fix this, start the Workstation service in the machine where Desktop Central is installed.

Top

Knowledge Base

1. Is Windows 9x series supported by Desktop Central?

No. Windows 9x series are not currently supported.

Questions

2. How will I know whether Desktop Central is currently running or not?

When the desktop Central is running, you can see the Desktop Central icon in the system tray. Alternatively, you can check for the following processes in the task manager:

- java.exe - pertaining to the Desktop Central Server
- mysqld-nt.exe - pertaining to the MySql database
- wrapper.exe - pertaining to the system tray operations

Questions

3. How to change the port number of the Web server?

During installation, you can specify an alternate port for the Web server, the default being 8020.

If you wish to change the port after installation, select **Admin --> Settings** and change the Web Server Port from the Port Settings. This change will take effect when you restart Desktop Central.

Questions

4. Why my computer is not listed in the managed computers list?

This happens when

1. The computer is not within the defined scope
2. When the agent or the Client Side Extension (CSE) is not installed in the computer. Try rebooting the computer.

Questions

5. How do I know the status of the applied configurations?

You can view the status of the deployed configurations in the Desktop Central client by clicking the **View Configuration** link.

For details on various states, refer to the Managing Configurations and Collections topic.

Questions

6. What types of scripts are supported in Custom Script configuration?

In addition to the configurations that are supported by Desktop Central, administrators can also write their own scripts that could be run on the user machines for accomplishing specific configurations. The scripts could be any of the following:

- Batch file (.bat or .cmd)

- In any other language hosted by Windows Script Host (WSH), such as VB Script, JScript, Perl, REXX, and Python.

The script engines for languages like Perl, REXX, and Python, must be registered with Windows.

Questions

7. Can any executables be installed using Desktop Central?

Any application in Microsoft Software Installer format (.MSI files) or in an EXE format can be installed using Desktop Central.

Questions

8. Can I use Desktop Central in a multi-domain, multi-domain controller environment?

Yes, you can use a single installation of Desktop Central to manage multiple domains in the same LAN.

Questions

9. Why the status of the configuration never change to Executed though the configurations have been applied on all the targets?

There is a possibility that there are some inactive users within the defined target. Add them to the inactive users list to get the accurate status of the configurations.

Questions

10. When a Site is given as a target, the status always shows as In Progress. Why?

There is no way to determine the user count in a given site. Without this it is not possible to verify whether the configuration is applied to all the users or not. Hence, the status is always shown as In Progress.

Questions

11. I am using the free version, but I see DesktopCentral folder in other machines which are not managed by Desktop Central. Why?

Desktop Central installs an agent or Client Side Extension (CSE) in the machines that are managed using the product. There is a possibility that during evaluation, you might have defined a scope that included more that 10 desktops. Since you can manage only up to ten desktops with the free version, you are still seeing the Desktop Central folders in the other machines that were managed during evaluation.

These agents will be removed when you uninstall Desktop Central.

Questions

12. I have different types of Windows Os-es in my domain, such as Windows XP, Windows 2000, Windows 2003, and so on. Is it possible to manage only the Windows XP machines in my network?

No. it is not possible to include the machines to be managed based on the OS type. When you select the Domain or the Organization Unit, all the machines under it will be included in the scope. However, you can exclude the machines from the target list based on the OS type while defining the configuration.

Refer to the Defining Targets topic for more details.

Questions

13. I have defined a set of security policies and the status is shown as executed. However, the policies defined does not seem to have been applied.

Desktop Central applies the configurations as per the Microsoft guidelines beyond which we do not have any control.

Questions

14. What does "Not Applicable" in the Execution Status view indicate?

When a configuration is applied using Desktop Central, the total target count, irrespective of whether the exclude criteria is defined or not, is shown as Total Target Computers in the Execution Status view . This is because, the number of desktops that falls under the exclude category can only be determined at the time of deployment in the client machines. This count is later included in the Not Applicable category to match the count.

For configurations that do not have an exclude criteria, the Not Applicable count will be zero.

Questions

15. What is the significance of the "Update Now" button shown in Report page?

The details about the Active Directory are periodically fetched and stored in the database. Any modifications in the Active Directory will not be reflected in the report immediately as the update is only periodic. To synchronize the data, click the Update Now button.

Questions

16. Will the inactive users be refreshed automatically?

Inactive user entries will be refreshed automatically whenever the Active Directory contents are getting updated in Desktop Central's local database. Also the inactive user state will be made as active if any configuration, excluding Windows Installer, Alert, and Custom Script configurations, is applied for an inactive user.

Questions

17. I have uninstalled the Product, but the agents installed by Desktop Central are not uninstalled. How to uninstall all the agents now?

When Desktop Central is uninstalled, Uninstall GPO will be automatically created to remove all the agents during the next client systems reboot. If that has not happened, Uninstall GPO has to be created natively to uninstall agents of Desktop Central from client machines. The GPO has to be created in the Domain Controller. The procedure to create the GPO is given below.

The batch file required for creating the GPO can be downloaded as a zip file from here.

For Windows 2000 Domain Controller

1. Go to Start -->Administrative Tools -->Active Directory Users and Computers.
2. Right Click Domain name. Click "Properties". Click "Group Policy" Tab.
3. Click "Create and Link a GPO here", give the name, and Click "OK".
4. Under the Domain name right-click on the GPO and select "Edit".
5. In the screen that opens, double-click on "Windows settings" under Computer configuration and select Scripts (Startup/shutdown)
6. Double-click Startup in the right window and click "Show files" from the Startup properties dialog.
7. Copy the *Agentuninstall.bat* file in the new screen and close.
8. Click "Add", select the *Agentuninstall.bat* file from the list and click OK.

For 2003 Domain Controller

1. Go to **Start** --> **Administrative Tools** --> **Active Directory Users and Computers**.
2. Right Click Domain name. Click "**Properties**". Click "**Group Policy**" Tab.
3. Click Open in the "**Group Policy management**" dialog. This opens Group Policy management Console.
4. Right-click on the Domain name and select "**Create and Link a GPO here**" option
5. Give a name and Click "**OK**".
6. Under the Domain name right-click on the GPO and select "**Edit**".
7. In the screen that opens, double-click on "**Windows settings**" under Computer configuration and select Scripts (Startup/shutdown)
8. Double-click Startup in the right window and click "**Show files**" from the Startup

properties dialog.

9. Copy the ***Agentuninstall.bat*** file in the new screen and close.
10. Click "**Add**", select the ***Agentuninstall.bat*** file from the list and click OK.

After creating the GPO, the agents will be completely uninstalled upon rebooting the client machines.

Questions

18. When I install the agents using the Install Agent button from the SoM page, I get the error as "Retrieval of WMI data on remote m/c has failed".

This could happen in any of the following cases:

1. When the domain credentials specified in SoM page has been changed.
2. Firewall settings in the client machines is not configured.

Solution

Case 1: Specify the correct domain credentials in the SoM Page by clicking the Edit button.

Case 2: Either disable the firewall or modify the firewall settings to enable remote administration as given below:

Open the command prompt in the client machine, type "*netsh firewall service type=remoteadmin mode=enable scope=all*" and press enter.

Questions

19. Inventory scanning has failed. Why?

This could happen in the following cases:

- When the Desktop Central Agents is not installed in the client computers. Check the Agent Installation knowledge base for the possible reasons.
- When the firewall in the machine running Desktop Central blocks the status reaching the Desktop Central server. Configure firewall and add TCP port 8021 to the exceptions list.

When the firewall is enabled in the client systems. Configure firewall and add TCP port 8021 to the exceptions list.

20. I have set up inventory alerts, but I do not receive any alerts?

To receive email alerts, you should have configured the Mail Server settings in the Desktop Central Server. Refer to the Mail Server Configurations in the online help documentation.

Dynamic Variables

Dynamic Variables are those that are replaced dynamically by Desktop Central while applying the configurations. As the name implies, the value of these variables are not the same for all the users/computers.

For example, to redirect the shortcuts of the start menu that are common for all the users to the system drive, you can use the dynamic variable**$SystemDrive**. This will be replaced by the corresponding system drive of that computer (like C, D, etc.) while deploying the configuration.

The table below lists the dynamic variable supported by Desktop Central:

Dynamic Variable	Description	Example Value of the Variable
$ComSpec	Specifies the path to the command interpretor	C:\WINNT\system32\cmd.exe
$HomePath	Refers to the home directory as defined in UMD/AD	\\JOHNSMITH\
$NtType	Role of NT/2000/XP computer	Server, Workstation
$OS	Short name of currently installed operating system	Windows_NT
$OSVersion	2000 & XP will report back as NT	Windows 2000
$OStype	2000 & XP will report back as NT	NT
$OsBuildNumber	Refers to the build number of the currently installed operating system	1381, 2195

$OsCsdVersion	Refers to the service pack of the currently installed operating system	Service Pack 4
$ProfileDirDU	Will be replaced by the full path of the "Default User" profile	C:\Documents and Settings\Default User
$ProfilesDir	Will be replaced by the full path of where user profiles are stored	C:\Documents and Settings
$ShellCache	Will be replaced by the path to current user's Temporary Internet Files shell folder	C:\Documents and Settings\JohnSmith\Local Settings\Temporary Internet Files
$ShellCookies	Will be replaced by the path to current user's Internet Cookies shell folder	C:\Documents and Settings\JohnSmith\Cookies
$ShellDesktop	Will be replaced by the path to current user's Desktop shell folder	C:\Documents and Settings\JohnSmith\Desktop
$ShellFavorites	Will be replaced by the path to current user's Favorites shell folder (also referred to as "IE Bookmarks").	C:\Documents and Settings\JohnSmith\Favorites
$ShellHistory	Will be replaced by the path to current user's History shell folder	C:\Documents and Settings\JohnSmith\Local Settings\History
$ShellMyPictures	Will be replaced by the path to current user's My Pictures shell folder	C:\Documents and Settings\JohnSmith\My Documents\My Pictures

$ShellNetHood	Will be replaced by the path to current user's Network Neighborhood shell folder	C:\Documents and Settings\JohnSmith\NetHood
$ShellPersonal	Will be replaced by the path to current user's Personal shell folder (also referred to as "My Documents")	C:\Documents and Settings\JohnSmith\My Documents
$ShellPrintHood	Will be replaced by the path to current user's Printer Neighborhood shell folder	C:\Documents and Settings\JohnSmith\PrintHood
$ShellPrograms	Will be replaced by the path to current user's Start Menu Programs shell folder	C:\Documents and Settings\JohnSmith\Start Menu\Programs
$ShellRecent	Will be replaced by the path to current user's Recent Documents shell folder	C:\Documents and Settings\JohnSmith\Recent
$ShellSendTo	Will be replaced by the path to current user's Send To shell folder	C:\Documents and Settings\JohnSmith\SendTo
$ShellStartMenu	Will be replaced by the path to current user's Start-Menu shell folder	C:\Documents and Settings\JohnSmith\Start Menu
$ShellStartup	Will be replaced by the path to current user's Start Menu Startup shell folder	C:\Documents and Settings\JohnSmith\Start Menu\Programs\Startup
$ShellTemplates	Will be replaced by the path to current user's Templates shell folder	C:\Documents and Settings\JohnSmith\Templates

$SystemDrive	Refers to the drive where OS files are located	C:
$SystemRoot	Will be replaced by the path to operating system folder	C:\WINNT
$TempDir	Will be replaced by the path to the temporary directory on the client	C:\Documents and Settings\JohnSmith\Local Settings\Temp
$WinDir	Will be replaced by the path to user's Windows folder (usually same as SystemRoot, exception would be a terminal server)	C:\WINNT

Limitations

1. When a site is chosen as the target for a user configuration, the status of the configuration will always be In Progress. This is because, it is not possible to get the exact user counts of individual sites.
2. When a user login to different computers in a domain, the status of the configurations defined for that user will reflect the status of the latest deployment.
3. When an already defined configuration is modified and re-deployed, the previous data will be overwritten and will not be shown in history reports.
4. Remote Shutdown Tool will not work for Windows 2000 computers.
5. Disk Defragmentation is not supported in Windows 2000 computers.

Known Issues

1. Printers shared in a Domain cannot be shared to computers in a Workgroup or vice-versa.
2. Redirecting folders between computers of different Domains or between a Workgroup and a Domain computer is not supported.
3. Software Installation will not work in the following cases:
   a. Package is in computer share of one Domain and you are trying to install it to a computer in another Domain.

   b. Package is in computer share of a Domain and you are trying to install it to a computer in a Workgroup or vice-versa.
   c. Package is in computer share of one Workgroup and you are trying to install it to a computer in another Workgroup.
4. In Custom Script configuration, Logoff and shutdown scripts cannot be executed.

Known Issues in deploying Configuration to Windows Vista Client Machines

1. When Security Policies are deployed to Windows Vista machines, the status will be shown as successful, but, the policies will not be applied.

Known Issues in Desktop Sharing

1. If the remote computer is shutdown using Remote Desktop Sharing, the viewer will not close by itself and has to be closed manually. It will display a blue screen showing a message "Meeting has stopped".
2. When connecting from Firefox/Flock browsers, Desktop Central Add-on (xpi) will be installed every time you access a remote computer using the Active X viewer. If you do not accept to install the xpi within 20 seconds, the remote service will be killed and you will not be able to access it. You have to close the viewer and have to connect again.
3. In Java viewer, Zoom In, Zoom Out, and Full Screen icons in the toolbar will not work.
4. When a remote connection is established, a message "You are now controlling the desktop" will appear. If you do not click OK within 20 seconds, the connection will close automatically. You have to close the viewer and have to connect again.

Glossary

This section provides the description or definitions of the terms used in Desktop Central.

Site

One or more well connected (highly reliable and fast) TCP/IP subnets. A site allows administrators to configure Active Directory access and replication topology quickly and easily to take advantage of the physical network. When users log on, Active Directory clients locate Active Directory servers in the same site as the user.

Domain

Domain is a group of computers that are part of a network and share a common directory database. A domain is administered as a unit with common rules and procedures. Each domain has a unique name.

Organizational Unit (OU)

An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain. An organizational unit is the smallest scope to which a Group Policy object can be linked, or over which administrative authority can be delegated.

Top

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.

🡅Top

Some definitions are adapted from Microsoft Help Documentation.

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.
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.

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.
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.
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 settings	Prevents users from changing automatic configuration settings. Automatic configuration is a process that administrators can use to update browser settings periodically.
Restrict changing proxy settings	Prevents users from changing proxy settings.
Restrict changing Messaging settings	Prevents users from changing the default programs for messaging tasks.

Restrict changing Calendar and Contact settings	Prevents users from changing the default programs for managing schedules and contacts.
Restrict Reset Web Settings feature	Prevents users from restoring default settings for home and search pages.
Restrict changing Check if Default Browser setting	Prevents Microsoft Internet Explorer from checking to see whether it is the default browser.
Restrict changing any Advanced settings	Prevents users from changing settings on the Advanced tab in the Internet Options dialog box.
Restrict changing Automatic Install of IE components	Prevents Internet Explorer from automatically installing components.
Restrict changing automatic check for software updates	Prevents Internet Explorer from checking whether a new version of the browser is available.
Restrict changing showing the splash screen	Prevents the Internet Explorer splash screen from appearing when users start the browser.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Network

Desktop Central supports configuring the following security policies in Network category:

Security Policy	Description
Hide 'Entire Network' from Network Neighborhood	Removes all computers outside of the user's workgroup or local domain from lists of network resources in Windows Explorer and My Network Places.
AlphaNumeric password	Windows by default will accept anything as a password, including nothing. This setting controls whether Windows will require a alphanumeric password, i.e. a password made from a combination of alpha (A, B, C...) and numeric (1, 2 ,3 ...) characters.
Enable access to properties of RAS connections available to all users	Determines whether a user can view and change the properties of remote access connections that are available to all users of the computer.
Ability to delete all user remote access connection	Determines whether users can delete all user remote access connections.
Ability to enable/Disable LAN connections	Determines whether users can enable/disable LAN connections.
Ability to rename LAN	Determines whether users can rename LAN or all user remote access connections.
Prohibit access to properties of LAN	Determines whether users can change the properties of a LAN connection.
Prohibit access to properties of components of LAN	Determines whether Administrators and Network Configuration Operators can change the properties of components used by a LAN connection.

Prohibit access to the advanced settings item on the advanced menu	Determines whether the Advanced Settings item on the Advanced menu in Network Connections is enabled for administrators.
Prohibit access to the dial-up preferences item on the advanced menu	Determines whether the Dial-up Preferences item on the Advanced menu in Network Connections folder is enabled.
Allow configuration of connection sharing (User)	Determines whether users can use the New Connection Wizard, which creates new network connections.
Prohibit adding and removing components for a LAN or RA connection	Determines whether administrators can add and remove network components for a LAN or remote access connection. This setting has no effect on non-administrators. If you enable this setting the Install and Uninstall buttons for components of connections are disabled, and administrators are not permitted to access network components in the Windows Components Wizard.
Prohibit TCP/IP advanced configuration	Determines whether users can configure advanced TCP/IP settings. If you enable this setting, the Advanced button on the Internet Protocol Properties dialog box is disabled for all users (including administrators).
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 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.
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 de-fragmentation snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Event viewer snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Fax services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Indexing services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Internet Information Services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

Restrict/permit Local users and groups snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Performance logs and alerts snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Shared folders snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit System information snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Telephony snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

Restrict/permit WMI control snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit System properties snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Group policy snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Group policy tab for active directory tool snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Administrative templates (computer) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Administrative templates (users) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

Restrict/permit Folder redirection snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Internet explorer maintenance snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Remote installation services snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Scripts (logon/logoff) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Scripts(startup/shutdown) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Security settings snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

Restrict/permit Software installation (computer) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.
Restrict/permit Software installation (user) snap-in	If the setting is enabled, the snap-in is permitted. If the setting is disabled, the snap-in is prohibited. If this setting is not configured, the setting of the "Restrict users to the explicitly permitted list of snap-ins" setting determines whether this snap-in is permitted or prohibited.

The policy descriptions are taken from Microsoft Help Documentation

Security Policies - Computer

Desktop Central supports configuring the following security policies in Computer category:

Security Policy	Description
Disable ctrl+alt+del requirement for logon	Determines whether pressing CTRL+ALT+DEL is required before a user can log on.
Restrict CD-ROM access to locally logged-on user only	Determines whether a CD-ROM is accessible to both local and remote users simultaneously.
Restrict Floppy access to locally logged-on user only	Determines whether removable floppy media is accessible to both local and remote users simultaneously.
Prevent users from installing printer drivers	It prevents users from installing printer drivers on the local machine.
Prevent user from changing file type association	Disables the buttons on the File Types tab. As a result, users can view file type associations, but they cannot add, delete, or change them.

The policy descriptions are taken from Microsoft Help Documentation

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.

Disk Cleanup Tool

The Disk Cleanup utility helps to cleanup the unwanted filed in the disk to increase the free space.

Desktop Central cleans the windows system for the following:

- Remove Active Setup Temp Folders
- Compress old files
- Remove content indexer
- Remove downloaded Program Files
- Remove internet cache files
- Remove memory dump files
- Remove Office setup files
- Remove offline files
- Remove web pages
- Remove old check disk files
- Empty recycle bin
- Remove remote desktop cache files
- Remove setup log files
- Remove old system restore positions.
- Remove Temporary files
- Remove temporary offline files
- Remove uninstall backup images
- Remove webclient and web publisher cache files

Disk Defragmenter Tool

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.

For more information, visit the following web pages on our website:

How To's:
https://www .manageengine.com/products/desktop-central/how-to.html

Knowledge Base:
https://www.manageengine.com/products/desktop-central/knowledge-base.ht ml

FAQs:
https://www .manageengine.com/products/desktop-central/faq.html

Training/Feature Videos:
https://www .manageengine.com/products/desktop-central/videos.html

Online Help:
https://www .manageengine.com/products/desktop-central/help/index.html