ManageEngine

GETTING STARTED WITH **DESKTOP CENTRAL CLOUD**

THIS GUIDE COVERS THE FOLLOWING TOPICS

01 System requirements

02 Account creation

03 Define the Scope of Management (SoM)

04 Agent installation

05 Creating a remote office

06 Configuring the AD connector

SYSTEM **REQUIREMENTS**

The system requirements for using Desktop Central Cloud include the following:

- Hardware requirements for distribution servers
- Hardware requirements for Desktop Central agents
- Software requirements for distribution servers
- Supported browsers

Minimum hardware requirements for distribution servers

Number of computers managed using the distribution server	Processor information	RAM size	Hard disk space
1 to 500	Intel Core i3 (2 core/4 thread) 2.0Ghz 3MB cache	4GB	6GB*
501 to 1,000	Intel Core i3 (2 core/4 thread) 2.9Ghz 3MB cache	4GB	12GB*
1,001 to 3,000	Intel Core i5 (4 core/8 thread) 2.3GHz	8GB	16GB*
3,001 to 5,000	Intel Core i7 (6 core/12 thread) 3.2GHz	8GB	20GB*

*This amount may increase depending on the number of software applications and patches that are deployed from each server.

Minimum hardware requirements for Desktop Central agents

Hardware	Requirement
Processors	Intel Pentium
Processor Speed	1.0GHz
RAM Size	512MB
Hard Disk Space	3GB*

*This amount may increase depending on the number of software applications and patches that are deployed from each server.

Minimum software requirements for distribution servers

The supported operating systems (OSs) for distribution servers and Desktop Central agents include the following:

Distribution servers

You can install distribution servers on any of the following Windows operating system versions:

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

* Recommended for managing 5,000 or more endpoints

DESKTOP CENTRAL **AGENTS**

You can use desktop Central to manage the computers running on the following operating systems:

Windows OS	Windows Server OS	Mac OS	Linux OS*
Windows 10	Windows Server 2019	10.15 Catalina	Ubuntu 10.04 and later versions
Windows 8.1	Windows Server 2016	10.14 Mojave	Debian 7 and later versions
Windows 8	Windows Server 2012	10.13 High	Red Hat Enterprise
	R2	Sierra	Linux 6 and later versions
Windows 7	Windows Server 2012	10.12 Sierra	CentOS 5 and later versions
	Windows Server 2008 R2	10.11El Capitan	Fedora 19 and later versions
		10.10 Yosemite	Mandriva 2010 and later versions
*Conditional support		10.9 Mavericks	Linux Mint 13 and later versions
	*Conditional support	10.8 Mountain lion	OpenSuSE 11 and later
		10.7 Lion	SuSE Enterprise Linux 11 and later versions
			Pardus 17 and 19
			*We support kernel versions above 2.6.33

FOR MANAGING **MOBILE DEVICES**

- Android: Android devices running on version 4.0 or above
- iOS (including iPhones, iPads, and iPods): iOS devices running on version 4.0 or above
- Windows smartphones: Devices running on version Windows Phone 8.1 or above
- Windows laptops (including Surface Hubs and Surface Pros): Devices running on Windows 10
- Chrome OS: Devices running on version 57.0 or later
- tvOS: Devices running on version 7.0 or above
- macOS: Devices running on version 10.7 or later

Note:

A TLS version of 1.2 and above is required for the legacy devices to be managed using Desktop Central Cloud.

SUPPORTED **BROWSERS**

Any of the following browsers can access the Desktop Central Cloud console:

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

Note:

The screen resolution should be 1280 x 1024 pixels or higher.

ACCOUNT **CREATION**

1. The first step in getting started with Desktop Central Cloud is to create an account with Zoho Corp., which is ManageEngine Desktop Central's parent company. This account will be used to access Desktop Central Cloud.

IF YOU HAVE AN EXISTING ZOHO ACCOUNT:

If you are an existing user of any of Zoho or ManageEngine's cloud services, you will be logged in automatically, using your existing account.

IF YOU DO NOT HAVE AN ACCOUNT WITH ZOHO:

If this is the first time you are accessing one of Zoho's cloud products, you'll have to create an account and provide the following details:

- Name
- Email address
- Organization
- Phone number (Optional)

Note:

The organization details specified here are confidential. The account created here becomes the super admin.

1. A confirmation email will be sent to the address provided. Upon successful verification, your account will be created.

2. You will be redirected to the Desktop Central console automatically. In the future, you can visit https://desktopcentral.manageengine.com, and log in using your Zoho account to access Desktop Central as needed.

3. To empower more technicians to use Desktop Central based on your organization's needs, an invitation can be sent to them via email.

DEFINE THE **SCOPE OF MANAGEMENT** (SoM)

After logging in to the Desktop Central console, the first thing you'll have to do is define your SoM by determining the target domain(s) and/or workgroup(s). To add the necessary domain or workgroup, follow the steps below:

1. Navigate to the **Agent tab**. Select **Domain** from the left pane > **Add domain.**

Note:

When adding a domain or workgroup, it is mandatory to provide credentials with **administrative privileges,** as this super admin account will be used to deploy Desktop Central agents across your network.

2. To **add a domain**, provide the following details:

Parameter	Description
Domain Name	The name of the domain.
Network Type	For adding a domain, choose the network type as Active Directory.
Domain Username	The username with domain admin privileges. It is recommended to have a dedicated domain admin user account for Desktop Central whose password policy is set to "Never Expire."
Password	The password of the domain admin user.
AD Domain Name	The fully qualified domain name (FQDN) of the Active Directory domain.
Domain Controller Name	If you have multiple domain controllers (DCs), provide the name of the DC nearest to the computer where the server is installed.

3. To **add a workgroup,** provide the following details:

Parameter	Description
Domain Name	The name of the workgroup.
Network Type	For adding a workgroup, choose the network type as Workgroup.
Admin Username	The username that 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."
Password	The password of the admin user.
DNS Suffix	This is required to identify a computer within a workgroup uniquely. For example, if you have a computer with the same name in two different workgroups, the DNS suffix is used to identify it uniquely.

AGENT **INSTALLATION**

After creating either a domain or a workgroup and defining the scope of management, the next step is to install Desktop Central agents on all the machines that you want to manage.

For further insights on the various methods and steps of installing agents, refer our document on agent installation.

CREATING A **REMOTE OFFICE**

As more companies branch out across the globe, managing and securing all the endpoints located in both local and branch offices becomes a cumbersome process for IT administrators. In addition, these admins are tasked with managing roaming users, which becomes a herculean task.

A remote office can be either a physical local office or a distributed network across different places in the world. With Desktop Central by your side, managing your local and remote network becomes a walk in the park. All you have to do is create a remote office, which can communicate with the Desktop Central server in two ways:

1. Direct communication
2. Through a distribution server (DS)

REMOTE OFFICE CREATION **WITH A DS**

A distribution server acts as a communication layer sandwiched between the endpoints in your remote office and the Desktop Central server. It replicates patch and software binaries from the Desktop Central server, and as the name indicates, distributes them across the remote office endpoints as opposed to each endpoint contacting the Desktop Central server individually to download patch and software binary. This drastically reduces bandwidth bottleneck issues and optimizes your network bandwidth.

Note:

It is recommended to have a dedicated computer for your distribution server, and this machine should have a static IP address to ensure hassle-free communication.

1. Navigate to the **Agent tab**. From the left pane, select **Remote Offices > Add Remote Office.**

2. Specify a name for the remote office.

3. By default, the chosen **Communication Type** will be **Through Distribution Server.**

4. Provide the requested details, including the Domain NETBIOS name, Name of the computer in which the DS will be installed, the IP address, and the FQDN/DNS name.

5. Configure the **Replication Policy** to associate it with the remote office. You can create a new replication policy that is tailor-made for the needs of your organization and the available bandwidth. To learn more about the significance of a replication policy, refer to this document.

6. Configure the proxy settings, and add the computers that are part of the remote office.

REMOTE OFFICE CREATION **FOR DIRECT COMMUNICATION**

1. Navigate to the **Agent tab**. From the left pane, select **Remote Offices > Add Remote Office.**

2. Specify a name for the remote office.

3. Choose the **Communication Type** as **Direct Communication.**

4. Configure the **Replication Policy** to associate it with the remote office. You can create a new replication policy that is tailor-made for the needs of your organization and the available bandwidth. To learn more about the significance of a replication policy, refer to this document.

5. Configure the proxy settings, and add the computers that are part of the remote office.

CONFIGURING THE **AD CONNECTOR**

Desktop Central Cloud eliminates the need for a server-installed machine, reducing the time and cost spent on setting up and maintaining a hardware infrastructure. Since the Desktop Central server will be hosted in one of our data centers, it's not possible for the server to communicate with your network's Active Directory (AD).

This is where Desktop Central's AD Connector comes to the rescue. AD Connector is a component that acts as a communicator between the Desktop Central server and the domain controller of your organization. One of your distribution servers can be configured as an AD Connector. Ensure that your domain controller is accessible by the chosen distribution server.

1. Navigate to the **Agent tab > Domain.**

2. From the AD Connector drop-down menu, choose a distribution server that will act as the AD Connector.

Note:

Once you configure the AD Connector, it cannot be removed. However, for the convenience of retiring machines that act as AD Connectors (or deleting the remote office that contains it), you can change the AD Connector to another machine by following the steps outlined above. Uninstallation of a distribution server or deletion of the remote office can only be done after changing the AD Connector.